CHAPTER – VI
INTERNATIONAL INITIATIVES TO COMBAT
CYBER CRIME

Cyber crime is not a national problem but an international one. International access to information and the mobility of data are fundamental to the working of our economic systems. Distance, time and space have ceased to be obstacles in commercial transactions. However, the rapid transnational expansion of large-scale computer networks and the ability to access these systems through regular telephone lines increases the vulnerability of these systems and the opportunity for their misuse of criminal activity. This menace of crime in cyberspace has the potential for limiting the development of cyber based international trade and commerce, apart from shying away the ordinary people who's privacy and security gets adversely affected by the onslaught of information crimes.

The international element of the commission of cybercrime creates new problems and challenges for the law. Systems may be accessed in one country, the data manipulated in another country and the consequences felt in a third country. The result of this ability is that different sovereignties, jurisdictions, laws and rules will come into play. More than in any other transnational crime, the speed, mobility, flexibility, significance and value of electronic transactions profoundly challenge the existing rules of international crime law.

It goes without saying that any national legal response will have only limited utility in combating this international menace of cyber crimes.

In the light of above discussion on the need for international efforts in combating cybercrimes let us now look into some of the efforts in this direction, initiated by international organizations:-


435
1. COUNCIL OF EUROPE

The first international initiative on computer crime in Europe was the Council of Europe\textsuperscript{1} Conference on Criminological Aspects of Economic Crime in Strasbourg in 1976. Several categories of computer crime were introduced.

In 1985, the Council of Europe appointed another expert committee, in order to discuss the legal issues of computer-related crime. A summary of the guidelines for national legislatures, with liability for international acts only, was presented in the Recommendation of 1989.\textsuperscript{2} It included a minimum list of computer fraud, computer forgery, damage to computer data or computer programmes, computer sabotage, unauthorized access, unauthorized interception, unauthorized reproduction of a protected computer programme and unauthorized reproduction of topography. The Recommendation included an optional list for consideration when planning new legislation.

On 11 September, 1995 the Council of Europe adopted another Recommendation\textsuperscript{3} concerning problems of procedural law connected with Information Technology. This Recommendation introduces 18 principles, categorized in seven chapters: search and seizure; technical surveillance; obligation to co-operate with the investigating authorities; electronic evidence; use of encryption; research; statistics and training; international co-operation.\textsuperscript{4}

In 1997, another committee of Experts on crime in cyber-space was appointed by the council of Europe to identify and define new crimes, jurisdictional rights and criminal liabilities due to communication on the Internet. Apart from the members of the council, United States, Japan, Canada and South

\textsuperscript{1} The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 member states in the European region. The Council of Europe is not to be confused with the Council of European Union and the European Council, as the Council of Europe is not part of the European Union, but a separate organization.

\textsuperscript{2} The Council of Europe adopted this Recommendation [No. R (89) 9] on September 13, 1989 at the 428th Meeting of the Ministers Deputies.

\textsuperscript{3} Recommendation No. R (95) 13 at the 543rd Meeting of the Ministers Deputies, http://www.usdoj.gov/criminal/cybercrime/crycoe.htm

Africa were made invitees to the meetings and they also participated in the negotiations. The committee produced a draft convention, which was adopted by the Ministers of Foreign Affairs on November 8, 2001. Minister or their representative from 26 member countries together with United States, Japan, Canada and South Africa signed the treaty. By April 2009, 46 states have signed and 25 states have ratified the convention on cybercrime. Countries such as Argentina, Pakistan, Philippines, Egypt, Botswana and Nigeria have already drafted parts of their legislation in accordance with the convention. Although those countries have not yet signed the convention, they are supporting the harmonization and standardization process intended by the drafters of the convention. The convention is today recognized as an important international instrument in the fight against cybercrime and is supported by different international organizations.

2. CONVENTIONS OF COUNCIL OF EUROPE

The council has adopted many conventions towards this end. These conventions aims at harmonizing the legislative responses to combat increasing incidence of cybercrimes, among the member countries of European Union as well as those other countries that are willing to adopt them. These conventions are as follows:

1 The need for a ratification is laid down in Article 36 of the convention:

Article 36-Signature and entry into force-

(1) This convention shall be open for signature by the member states of the council of Europe and by non-member states which have participated in its elaboration.

(2) This convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the secretary General of the Council of Europe.


3 Interpol highlighted the importance of the convention on cybercrime in the Resolution of the 6th International Conference on Cyber Crime, Cairo—"That the convention on cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cybercrime. Countries shall be encouraged to consider joining it. The convention shall be distributed to all Interpol member countries in the four official languages", http://www.interpol.com/Public/Technologycrime/conference/6thIntConf/Resolution.asp.

437
2.1 Convention for Protection of Individuals with Regard to Automatic Processing of Personal Data

This convention was arrived at by the member states of the Council of Europe of 28 Jan 1981, at Strasbourg, recognizing the necessity to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples and considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing.\(^1\) The Convention, while accepting the importance of the privacy, also reaffirms their commitment to freedom of information regardless of frontiers.

The purpose of the Convention is to secure in the territory of each Party, for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him. Towards this end the Convention imposes upon the parties a duty to ensure necessary measures in its domestic law to give effect to the basic principles for data protection, set out in the convention including appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection.\(^2\) It also requires that personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life or criminal convictions, may not be processed automatically unless domestic law provides appropriate safeguards.\(^3\)

The Convention requires that adequate security measures have to be ensured for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.\(^4\) The Convention stipulates the

\(^1\) Preamble to the Convention.
\(^2\) Articles 4 and 10.
\(^3\) Articles 6.
\(^4\) Article 7.
quality for automatic processing of any personal data in Article 5 by stating that personal data undergoing automatic processing shall be: (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date and (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

Article 8 of the Convention provides some additional safeguards to the data subjects by stating that:

'Any person shall be enabled:

(a) to establish the existence of an automated personal data file, its main purposes; as well as the identity and habitual residence or principal place of business of the controller of the file;

(b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

(c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

(d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs (b) and (c) of this article is not complied with.

Further, Article 14 provides that 'Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party'.

1 The term 'Data Subject' means an identified or identifiable individual whose personal data is subjected to automatic processing.
Article 12 deals with the trans-border flow of personal data. The Article mandates that a Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorization trans border flows of personal data going to the territory of another Party, thereby protecting the free flow of information across the borders. However, in order to ensure protection of the privacy of the data subjects, a country is permitted to bring in legislative controls that includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection. Such restrictions are also permitted where the transfer is made from its territory to the territory of a non-signing State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party.

Convention requires the parties to provide mutual assistance in implementation of the provisions thereof. Each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe for coordinating the mutual assistance between the parties, at lateral level.

Article 23 of the Convention permits the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee. This provision facilitates adoption of same standards by non-member countries for the mutual benefits.¹

2.2. **Convention on Cyber Crime, Budapest, 23 Nov. 2001**

The council of Europe Convention on Cyber Crime was opened for signatures at a conference in Budapest, Hungary, on November 23, 2001. This convention is a historic milestone in the combat against cybercrime, and entered

¹ [http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm](http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm);
into force on July 1, 2004. The number of signatures not followed by ratifications are 23 States and the number of ratifications/accessions are 23 states (December 2008). An Additional Protocol on the criminalization of Acts of a Racist and Xenophobic Nature Committed through computer systems of January 2003 has also been adopted. This convention is quite comprehensive in dealing with various aspects of prevention and detection of cybercrimes. The major features of the convention are discussed in the following paragraphs:-

**Chapter I.** includes use of terms (computer system,\(^1\) computer data, service provider and traffic data).

**Chapter II.** of the Convention lists out the measures that are to be taken at the national level, by the parties to the Convention. Firstly, parties are required to take legislative and other measures, in their substantive criminal laws, necessary to establish criminal liability for the following offences:

**Article-2 Illegal Access:** The access to the whole or any part of a computer system without right, when committed intentionally. A Party may require that the offence be committed by infringing security measures, with the intent to obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article-3 Illegal Interception:** The interception without right when committed intentionally and made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. However, a Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

**Article-4 Data Interference:** The damaging, deletion, deterioration, alteration or suppression of computer data without right, when committed intentionally. However, a Party may reserve the right to require that for such conduct to become an offence must result in serious harm.

---

\(^1\) The definition is sufficiently flexible to address technology that go beyond traditional computer systems. It includes mobile telephones that have the capability to produce, process and transmit data, such as accessing Internet, sending e-mail, and transmitting attachments.
**Article-5 System Interference:** The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data, when committed intentionally.

**Article-6 Misuse of Devices:** The production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences mentioned above, or a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of such offences, when committed intentionally and without right. These provisions will not bring criminal liability where the production, procurement etc is not for committing an offence but for authorized testing or protection of a computer system. Similarly, the a Party is free to reserve the right not to apply this provision, except in the case of production, procurement etc of a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing an offence.

**Article-7 Computer-related Forgery:** The input, alteration, deletion, or suppression of computer data, when committed intentionally and without right, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

**Article-8 Computer-related Fraud:** The causing of a loss of property to another person, when committed intentionally and without right, by any input, alteration, deletion or suppression of computer data or by any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

**Article-9 Offences Related to Child Pornography:** The following conducts, when committed intentionally and without right:
• Producing child pornography for the purpose of its distribution through a computer system
• Offering or making available child pornography through a computer system
• Distributing or transmitting child pornography through a computer system
• Procuring child pornography through a computer system for oneself or for another person
• Possessing child pornography in a computer system or on a computer data storage medium.

The term "child pornography" shall include pornographic material that visually depicts, a minor engaged in sexually explicit conduct, a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a minor engaged in sexually explicit conduct.

**Article-10 Infringements of Copyright and Related Rights:** Infringement of copyright and infringement of related rights, as defined under the law of the Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed willfully, on a commercial scale and by means of a computer system.

A Party may reserve the right not to impose criminal liability on infringement of copyright and infringement of related rights as stated above, in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred above.

**Article-11 Attempt and Aiding or Abetting:** Intentional aiding or abetting the commission of any of the offences established in accordance with the Convention with intent that such offence be committed and an attempt to commit any of those offences.
The Convention also establishes corporate liability on any legal persons for any offences committed by a natural person for its benefit. It also requires the members to establish effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions against the persons committing, abetting, aiding or attempting any of those offences listed above.

Apart from establishing criminal liabilities for the 'cyber crimes' in their domestic laws, the Convention also requires that the parties adopt legislative and other measures as may be necessary to establish certain powers and procedures required for the purpose of specific criminal investigations or proceedings, subject to necessary conditions and safeguards for protecting the human rights and liberties. These powers and procedures shall apply to the criminal offences established under the Convention, other criminal offences committed by means of a computer system and collection of evidence in electronic form of a criminal offence. The parties are also required to provide for in their domestic laws for the following:

**Article-16 Expedited Preservation of Stored Computer Data:** Each Party is required to adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. Party shall also adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

**Article-17 Expedited Preservation and Partial Disclosure of Traffic Data:** Each party shall adopt necessary measures to ensure that expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication and ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to
identify the service providers and the path through which the communication was transmitted.

**Article-18 Production Order:** Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

**Article-19 Search and Seizure of Stored Computer Data:** Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access a computer system or part of it and computer data stored therein; and a computer-data storage medium in which computer data may be stored in its territory. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed. These measures shall include the power to seize or similarly secure a computer system or part of it or a computer-data storage medium, make and retain a copy of those computer data, maintain the integrity of the relevant stored computer data and render inaccessible or remove those computer data in the accessed computer system.

**Article-20 Real-time Collection and Interception of Traffic Data:** Parties are required to adopt legislative and other measures necessary to empower its competent authorities to collect or record or intercept through the application of technical means on the territory of that Party, and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party; or to cooperate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communication in its territory transmitted by means of a computer system. Party shall also adopt legislative and other measures necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
Article-22 Jurisdiction: The convention mandates that the parties are to establish jurisdiction over any offence under the Convention, committed in its territory, or on board of ship flying its flag, or an aircraft registered under its laws, or committed by one of its nationals outside its territorial jurisdiction, is the offence is punishable under criminal law where it was committed.

International Co-operation: The Convention in its Chapter III provides the principles relating to international co-operation in dealing with cyber crimes. It provides that the Parties shall co-operate with each other, in accordance with the provisions of the Convention and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. It also provides specific principles with regard to co-operation in following fields that are to be followed by the parties:

Article-24 Extradition
Article-25 Mutual Assistance
Article-26 Sharing of Disclosure of spontaneous Information
Article-28 Confidentiality and limitation on use of the shared data, for investigations or proceedings other than those stated in the request.
Article-31 Mutual assistance regarding accessing of stored computer data
Article-33 Mutual assistance in real-time collection of traffic data
Article-34 Mutual assistance regarding the interception of content data

The Convention also requires the parties to designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision immediate assistance for the purpose of investigations or proceedings concern-criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. A Party's point of contact shall have the capacity to carry out communications with the point of
2.3 Convention on the Prevention of Terrorism

On terrorism, 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, and entered into force on June 1, 2007. In this convention a terrorist offence is merely defined as meaning any of the offences as defined in the attached list of 10 treaties in the Appendix.

The purpose of the present convention is to enhance the efforts of parties in preventing terrorism and its negative effects on the full enjoyment of human rights, in particular the right to life, both by measures to be taken at national level and through international cooperation, with due regard to the existing applicable multilateral or bilateral treaties or agreements between the parties.

According to the 2005 Council of Europe Convention on the Prevention of Terrorism, [CETS No.196] Articles 5-7, parties to the Convention are required to adopt certain preparatory conducts that have a potential to lead to terrorist acts as criminal offences.

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

---


2 Explanatory Report note 98.
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 the skills or "know-how" and intended to be used for the carrying out of the terrorist offence or for a contribution to it.1 The training must be unlawfully and intentionally.2

2.4 Convention on the Protection of Children against sexual Exploitation and Sexual Abuse

Sexual exploitation and sexual abuse of children are among the worst forms of violence against children and have long-lasting damaging consequences for the young victims.

Protecting children from violence has been a top priority at the council of Europe for many years. On 25 October 2007 the Council of Europe convention on the Protection of Children against Sexual Exploitation and sexual Abuse (CETS No. 201) was adopted and opened for signature on the occasion of the 28th Conference of European Ministers of Justice in Lanzorote, Spain.3 On the first day the convention on the protection of children opened for signature 23 states4

1 Explanatory Report note 122.
3 http://www.coe.int/t/e/legal_affairs/legal_co_operation/fight_against_sexual_exploitation_of_children/
4 Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Ireland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Turkey, Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).
signed the convention. The major features of the convention are discussed in the following paragraphs:

Article 1-Purposes

1. The purpose of this Convention are to:
   a. prevent and combat sexual exploitation and sexual abuse of children;
   b. protect the rights of child victims of sexual exploitation and sexual abuse;
   c. promote national and international co-operation against sexual exploitation and sexual abuse of children.

2. In order to ensure effective implementation of its provisions by the Parties, this Convention sets up a specific monitoring mechanism.

Article 11 - Principles

1. Each Party shall establish effective social programmes and set up multidisciplinary structures to provide the necessary support for victims, their close relatives and for any person who is responsible for their care.

2. Each Party shall take the necessary legislative or other measures to ensure that when the age of the victim is uncertain and there are reasons to believe that the victim is a child, the protection and assistance measures provided for children shall be accorded to him or her pending verification of his or her age.

Article 12 - Reporting suspicion of sexual exploitation or sexual abuse

1. Each Party shall take the necessary legislative or other measures to ensure that the confidentiality rules imposed by internal law on certain professionals called upon to work in contact with children do not constitute an obstacle to the possibility, for those professionals, of their reporting to the services responsible for child protection any situation where they have reasonable grounds for believing that a child is the victim of sexual exploitation or sexual abuse.

2. Each Party shall take the necessary legislative or other measures to encourage any person who knows about or suspects, in good faith, sexual exploitation or sexual abuse of children to report these facts to the competent services.
Article 13 - Helplines

Each Party shall take the necessary legislative or other measures to encourage and support the setting up of information services, such as telephone or Internet helplines, to provide advice to callers, even confidentially or with due regard for their anonymity.

Article 14 - Assistance to victims

1 Each Party shall take the necessary legislative or other measures to assist victims, in the short and long term, in their physical and psycho-social recovery. Measures taken pursuant to this paragraph shall take due account of the child's views, needs and concerns.

2 Each Party shall take measures, under the conditions provided for by its internal law, to co-operate with non-governmental organizations, other relevant organizations or other elements of civil society engaged in assistance to victims.

3 When the parents or persons who have care of the child are involved in his or her sexual exploitation or sexual abuse, the intervention procedures taken in application of Article 11, paragraph 1, shall include:

- the possibility of removing the alleged perpetrator;
- the possibility of removing the victim from his or her family environment. The conditions and duration of such removal shall be determined in accordance with the best interests of the child.

4 Each Party shall take the necessary legislative or other measures to ensure that the persons who are close to the victim may benefit, where appropriate, from therapeutic assistance, notably emergency psychological care.

Article 18 - Sexual abuse

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalized:

a. engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities;
b. engaging in sexual activities with a child where:
   - use is made of coercion, force or threats; or
   - abuse is made of a recognized position of trust, authority or influence over the child, including within the family; or
   - abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.

2 For the purpose of paragraph 1 above, each Party shall decide the age below which it is prohibited to engage in sexual activities with a child.

3 The provisions of paragraph 1.a are not intended to govern consensual sexual activities between minors.

Article 19 - Offences concerning child prostitution

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalized:
   a. recruiting a child into prostitution or causing a child to participate in prostitution;
   b. coercing a child into prostitution or profiting from or otherwise exploiting a child for such purposes;
   c. having recourse to child prostitution.

2 For the purpose of the present article, the term "child prostitution" shall mean the fact of using a child for sexual activities where money or any other form of remuneration or consideration is given or promised as payment, regardless if this payment, promise or consideration is made to the child or to a third person.

Article 20 - Offences concerning child pornography

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalized:
a. producing child pornography;
b. offering or making available child pornography;
c. distributing or transmitting child pornography;
d. procuring child pornography for oneself or for another person;
e. possessing child pornography;
f. knowingly obtaining access, through information and communication technologies, to child pornography.

2 For the purpose of the present article, the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction or a child's Sexual organs for primarily sexual purposes.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material:
   - consisting exclusively of simulated representations or realistic images of a non-existent child;
   - involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

4 Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

Article 21 - Offences concerning the participation of a child in pornographic performances

1 Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct is criminalized:
   a. recruiting a child into participating in pornographic performances or causing a child to participate in such performances;
   b. coercing a child into participating in pornographic performances or profiting from or otherwise exploiting a child for such purposes;
e. knowingly attending pornographic performances involving the participation of children.

2 Each Party may reserve the right to limit the application of paragraph l.c to cases where children have been recruited or coerced in conformity with paragraph l.a or b.

**Article 22 - Corruption of children**

Each Party shall take the necessary legislative or other measures to criminalize the intentional causing, for sexual purposes, of a child who has not reached the age set in application of Article 18, paragraph 2, to witness sexual abuse or sexual activities, even without having to participate.

**Article 23 - Solicitation of children for sexual purposes**

Each Party shall take the necessary legislative or other measures to criminalize the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph l.a, or Article 20, paragraph l.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.¹

**3. THE EUROPEAN UNION (EU)**

The European Union² has only limited powers with regard to the legislation in the field of criminal law. It has the ability to harmonize the national criminal law only is special areas such as the protection of financial interests of the European Union and Cyber Crime.

---


² The European Union is a supranational and intergovernmental union of today 27 member states from the European continent.
In 1999, the European Union launched the initiative "eEurope", by adopting the European Commission’s communication "eEurope: An Information Society for all". In 2000, the European Council adopted a comprehensive "eEurope Action Plan" and called for its implementation before the end of 2002.

In 2001, the European commission published a communication titled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and combating computer-related crime." In this communication, the commission analyzed and addressed the problem of cybercrime and pointed out the need for effective action to deal with threats to the integrity, availability and dependability of information systems and networks.

In addition, the commission published a communication on "Network and Information Security" in 2001 that analyzed the problems in network security and drafted a strategic outline for action in this area.

Both these commission communications emphasized the need for approximation of substantive criminal law within the European Union especially with regard to attacks against information systems. The harmonization of the substantive criminal law within the European Union in the fight against cybercrime is recognized as a key element of all initiatives at the EU-level. Following this strategy, the commission in 2002 presented a proposal for a "Framework Decision on Attacks against Information System". The proposal by the Commission was partly modified and finally adopted by the Council and it entered into force in 2005.

The Framework Decision takes note of the Council of Europe Convention on Cybercrime but concentrates on the harmonization of substantive criminal law provisions that are designed to protect infrastructure elements.

---

5 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
Article 2- Illegal access to information system:-
(1) Each Member state shall take the necessary measures to ensure that the international access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

(2) Each member state may decide that the conduct referred to in paragraph-1 is incriminated only where the offence is committed by infringing a security measures punishable by effective, proportional and dissuasive criminal penalties.

Article 3- Illegal system interference

Each member state shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 4- Illegal data interference

Each member state shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alternation, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

States shall, according to Article 6, ensure that illegal system interference and illegal data interference is punishable of a maximum at least between 1 and 3 years of imprisonment. But aggravating circumstances included in Article 7 may result in a maximum of at least between 2 and 5 years.

States shall establish Jurisdiction described in Article 10. According to Article 10.3 a state which under its laws does not extradite its own nationals, shall establish Jurisdiction over and prosecute conducts referred to in Article 2-4, when it is committed by one of its nationals outside its territory.
In the latest development, the EU Commission Considered an initiative in May 2007 regarding to European legislation against identity theft, called *Towards a general policy on the fight against cyber crime.*

The commission organized an European Union Expert Meeting on Cybercrime in November 2007. The meeting represented a next step for the EU in implementing the general policy outlined by the commission.

A Framework Decision amending the Framework Decision 2002/475JHA on combating Terrorism has been prepared in 2008 in the European Union. It will include three new crimes in the EU legislation: public provocation to commit terrorist offences, recruitment for terrorism and training for terrorism.¹

On 10 March 2009, Microsoft academia and law enforcement organizations have appealed to the European Commission to support an initiative to establish a network of university Centres of Excellence to train law enforcement agencies on cyber crime investigation techniques.

Speaking at the council of Europe Octopus Interface 2009 Conference, Tim Cranton, Associate General Counsel of Worldwide Internet Safety Programs at Microsoft, released a study produced with the support of INTERPOL and Europol which calls for the creation of the ‘Cybercrime Centers of Excellence Network for Training, Research and Education’ (2 CENTRE). He also revealed that Microsoft will support submissions by universities for funding seeking to join the 2 CENTRE programme made to the European Union.

Cybercrime is also of concern to the European commission, which has advised on the creation of the 2 CENTRE initiative. The initiative is in keeping with the commission's overarching policy objective of setting up an EU cybercrime investigation training platform.

The first 2 CENTRE scheduled to go operational in 2010 will be located in University College Dublin (UCD), Ireland and Universite Technologique de Troyes, France.¹

4. OECD INITIATIVES

The first international effort in harmonizing the legal responses towards cybercrime was appointment of an expert committee by the Organization for Economic Co-operation and Development (OECD), in 1983, in Paris, to discuss computer-related crime and the need for changes in the Penal Codes of the member countries.² Based on the proposals put forth by the committee, the OECD recommended member countries to bring in changes in their penal legislations to cover certain types of cybercrime. The proposals listed the acts, which could constitute a common denominator between the different approaches taken by the member countries. Though not binding in nature, these proposals are crucial in the sense that they are the first truly international effort in this direction.

The OECD also developed Guidelines to provide a foundation on which countries and the private sector acting separately as well as in concert may construct a framework towards the security of information systems. These guidelines are intended to serve as a benchmark against which all the stakeholders may measure their progress. These guidelines are addressed to information systems and aims to achieve:-

(a) Promote cooperation between the public and private sectors in the development and implementation of such measures, practices and procedures.

(b) Foster confidence in information systems and the manner in which they are produced and used.

(c) Facilitate development and use of information systems, nationally and internationally.


(d) Promote international cooperation in achieving security of information systems.

The OECD Guidelines are based on the following nine principles:-

(1) **Accountability Principle**: The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.

(2) **Awareness Principle**: In order to foster confidence in information systems, owners, providers and users and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the exercise and general extent of measures, practices and procedures for the security of information systems.

(3) **Ethics Principle**: Information systems and the security systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.

(4) **Multidisciplinary Principle**: Measures, practices and procedures for the security of information systems should take into account of and address all relevant considerations and viewpoints, including technical, administrative, organizational, operational, commercial, educational and legal considerations and view points.

(5) **Proportionality Principle**: Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information system and to be severity, probability and extent of potential harm, as the requirement for security vary depending on the information system.

(6) **Integration Principle**: Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practice and procedures of the organization so as to create a coherent system of security.

(7) **Timeliness Principle**: Public and private parties, at both the national and international levels, should act in a timely and coordinated manner to prevent and to respond to branches to security of information systems.
(8) **Reassessment Principle**: The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.

(9) **Democracy Principle**: The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.

Even before this, as early as in 1977, OECD has began to elaborate guidelines governing protection of privacy and the transborder flow of personal data. The council of OECD adopted these guidelines on 23 Sept. 1980, as a recommendation to member states. The main points of the guidelines concerns the following principles related to:-

(1) **Collection Limitation**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(2) **Data Quality**: Personal data should be relevant to the purpose for which they are to be used, and, to the extent necessary for those purpose, should be accurate, complete and kept up-to-date.

(3) **Purpose Specification**: The purpose for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purpose or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

(4) **Use Limitation**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with paragraph (3) except:-

(a) With the consent of the data subject; or

(b) by the authority of law.

(5) **Security Safeguards**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
(6) Openness:- There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

(7) Individual Participation:- An individual should have the right:-

(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

(b) to have communicated to him, data relating to him-
   ■ with a reasonable time;
   ■ at a charge, if any, that is not excessive;
   ■ in a reasonable manner; and
   ■ in a form that is readily intelligible to him

(c) to be given reasons if a request made under sub paragraphs(a) and (b) is denied, and to be able to challenge such denial; and

(d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

(8) Accountability:- A data controller should be accountable for complying with measures which give effect to the principles stated above.¹

Though these guidelines are not binding on the members, they act as a recommendation of the general principles set forward for implementation by them. All the members of OECD have endorsed the guidelines.

OECD is currently involved in a Workshop on Spam. The first workshop was conducted in Brussels, on 2-3Feb, 2004² and the second workshop is

---

¹ OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1851861_1_1_1,00.html; http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1,00.html; http://www5.cao.go.jp/seikatsu/kojin/houseika/daiil/1/siryou5.html;
scheduled to be held in Busan, Korea on 8-9 September 2004.¹ The objectives of these workshops include the following:-

- consider the next steps in developing and "OECD Anti-spam Toolkit".
- Examine network management solutions to reduce spam.
- Examine the use of authentication and technical tools to reduce spam.
- Consider best practice and technical tools to reduce mobile spam and instant messaging spam.

The OECD, has launched an Anit-spam "Toolkit" as the first step in a broader initiative to help policy makers, regulators and industry players orient their policies relating to spam solutions and restore trust in the Internet and e-mail.²

OECD has also undertaken many other initiatives in the field of Information Technology that have indirect bearing on fighting cybercrimes. OECD Guidelines on Cryptography Policy is an example of such initiatives.

The OECD Draft Cryptography Policy Guidelines Nov. 1996.³ The Guidelines were adopted as a recommendation of the council of the OECD on 27 March, 1997.⁴ The OECD Guidelines are as follows:-

1. **Trust in Cryptographic Methods**: Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communication systems.

2. **Choice of Cryptographic Methods**: Users should have a right to choose any cryptographic method, subject to applicable law.

3. **Market Driven Development of Cryptographic Method**: Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

---

³ http://ezines.onb.ac.at:8080/quint/pub/97-01-30/Netzeil/OECD/index_2.html
(4) **Standards for Cryptographic Methods:** Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

(5) **Protection of Privacy and Personal Data:** The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

(6) **Lawful Access:** National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.

(7) **Liability:** Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

(8) **International Cooperation:** Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

A Joint APEC-OECD Workshop in Security of information was held in Seoul on 5-6 September 2005. Several topics were discussed, including promoting global governmental incidents response.

In 22 and 23 April 2007 and APEC-OECD Workshop was held in Manila. A Joint APEC-OECD workshop on initiatives among member economies promoting safer internet environment for children was held in Japan on 13 October 2008.

---


The OECD was the first international organization that initiated guidelines for computer crime, but does not today work directly on cybercrime *per se*. The organization focuses more on cyber security, and promotes a global coordinated policy approach building trust and confidence. The OECD Working Party on Information and Privacy (WPISP) develops international guidelines.¹

5. **THE G-8 GROUP OF STATES**

The G-8 Group of states² countries established in 1997 the subgroup of High-Tech Crime (the Leon Group). During their meeting in Washington D.C., United States, the G8 Justice and Interior Ministers adopted Ten principles and a Ten-Point Action Plan to fight high-Tech crimes. The Heads of the G8 endorsed these principles later, which include:-

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be coordinated among all concerned states, regardless of where harm has occurred.
- Law enforcement personal must be trained and equipped to address high-tech crimes.

In 1999, the G8 specified their plans regarding the fight against high-tech crimes at a Ministerial Conference on Combating Transnational Organized Crimes in Moscow, Russia Federation. They expressed their concerns about crimes (such as child pornography), as well as traceability of transactions and transborder access to stored data. Their communique contains a number of principles in the


² The G8 Consists of eight countries (states): Canada, France, Italy, Japan, Russia, United Kingdom, Germany and USA; http://www.g7.utoronto.ca; http://www.usdoj.gov/criminal/cybercrime/g82004/g8_background.html.
fight against cybercrime that are today found in a number of international strategies.1

14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems, which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders.

We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex I to this Communiqué. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes - including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions - so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.
One of the practical achievements of the work done by expert groups has been the development of an international 24/7-network of contacts requiring participating countries to establish points of contact for transnational investigations that are accessible 24 hours a day, 7 days a week.

At the G8 Conference in Paris, France in 2000, the G8 addressed the topic of cybercrime with a call to prevent lawless digital havens. Already at that time, the G8 connected its attempts for international solutions to the council of Europe's Convention on Cybercrime. In 2001, the G8 discussed procedural instruments in the fight against cybercrime at a workshop held in Tokyo, focusing on whether data retention obligations should be implemented or whether data preservation was an alternative solution.

At the meeting of G8 Justice and Home Affairs Ministers in Washington D.C., on May 10-11, 2004, a Joint communiqué stated that with the council of Europe Convention of Cybercrime coming into force the states should take steps to encourage the adoption of the legal standards it contains on a broad basis.

At the Moscow Meeting in 2006 for the G8 Justice and Home Affairs Ministers discussed cybercrime and issues of cyber space. In a statement it was emphasized:

We also discussed issues related to sharing accumulated international experience in combating terrorism, as well as comparative analysis of relevant pieces of legislation on that score. "We discussed the necessity of improving effective counter measures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that it is necessary to device a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an

international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors.¹

The G8 Summit in 2006 was held in St. Petersburg and a Summit Declaration on Counter-Terrorism included as follow:

We reaffirm our commitment to collaborative work, with our international partners to combat the terrorist threat, including:

Implementing and improving the international legal framework on counter-terrorism;

Effectively countering attempts to misuse cyber space for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists.²

At the meeting of G8 Justice and Interior Minister in Munich, Germany on May 23-25, 2007, the delegates also agreed "to work towards criminalizing, within national legal frameworks, specific forms of misusing the Internet for terrorist purposes".

The G8 Group had their last meeting at the Hokkaido Tokyako Summit on July, 7-9, 2008. A report to the G8 Summit leaders from the G8 experts on International Terrorism and Transnational Organized Crime was presented.³

6. EFFORTS OF UNITED NATIONS (UN)

Following the seventh UN Congress on the Prevention of Crime and the Treatment of offenders, which took place in 1985, the Secretary-General prepared a report entitled "Proposals for concerted International Action Against forms of Crime Identified in Milan Plan of Action". Computer crime was discussed in paragraphs 42-44 of that report.

¹ http://www.g7.utoronto.ca/justice/justice2006.htm.
² http://www.g8russia.ru/docs/17.html
At the 8th Congress on the Prevention of Crime and the Treatment of Offenders (held in Havana, Cuba, 27 August-7 September 1990), the UN General Assembly adopted a resolution dealing with computer crime legislation.\(^1\) Based on its resolution 45/121(1990), the UN published a manual in 1994 on the prevention and control of computer related crime.\(^2\)

On Dec. 8, 1999, the UN General Assembly adopted the Anti-Terrorism Financing Convention that grew out of G8 nation endeavours to combat terrorist financing.\(^3\) The United Nations General Assembly has adopted a number of resolutions. General Assembly Resolution 55/63 of 4 December 2000 and 56/121 of 19 December 2001 on "Combating the Criminal misuse of information technologies", are most important.

The Resolution 55/63 includes as follows:-

(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.

(b) Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized.\(^4\)

The Resolution 56/121 invites Member States, when developing national laws, policy and practices to combat the criminal misuse of information technologies, to take into account, inter alia, the work and achievements of the Commission on Crime Prevention and Criminal Justice.\(^5\)

In 2004, the UN created a working group dealing with spam, cybercrime and other Internet-related topics, emphasizing the interest of the UN in participating in ongoing international discussions on cybercrime threats.\(^6\)

---

At the 11th UN Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand in 2005, a Declaration was adopted that highlighted the need for harmonization in the fight against cyber crime. The Bangkok Declaration no. 16 reads as follows:-

We note that, in the current period of globalization, information technology and the rapid development of new telecommunication and computer network systems have been accompanied by the abuse of those technologies for criminal purposes. We therefore welcome efforts to enhance and supplement existing cooperation to prevent investigate and prosecute high-technology and computer related crime including by developing partnerships with the private sector. We recognize the important contribution of the United Nations to regional and other international forums in the fight against cybercrime and invite the Commission on Crime Prevention and Criminal Justice, taking into account that experience, to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations.

In addition, a number of United Nations system Decisions, Resolutions and Recommendations address issues related to cybercrime. The most important ones are:

- The United Nations Office for Drugs and Crime (UNODC) Commission on Crime Prevention and Criminal Justice\(^1\) adopted a Resolution on effective crime prevention and criminal justice responses to combat sexual exploitation of children.\(^2\)

- In 2004 the United Nations Economic and Social Council\(^3\) adopted a resolution on international cooperation in the prevention, investigation, 

---

1 The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up 1991. It is a subsidiary body of the Economic and social council.
3 The United Nations Economics and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues, http://www.un.org/ecosco/.
prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.¹

In 2004 the council adopted a resolution on the sale of licit drugs via the Internet that was explicitly taking regard to a phenomenon related to a computer crime.²

In 2007 the council adopted a resolution in international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.³ Both resolutions do not explicitly address the challenges of Internet related crimes but is applicable with regard to these offences as well.

7. INTERNATIONAL TELECOMMUNICATIONS UNION (ITU)

The International Telecommunication Union (ITU),⁴ as a specialized agency within the United Nations, plays a leading role in the standardization and development of telecommunication as well as cyber security issues. Among other activities, the ITU was the lead agency of the World Summit on the Information Society (WSIS) that took place in two phases is Geneva, Switzerland (Dec.2003) and in Tunis, Tunisia (2005). Governments, Policy-makers and experts from around the world shared ideas and experiences about how best to address the emerging issues associated with the development of a global information society, including the development compatible standards and laws. The outputs of the Summit are contained in the Geneva Declaration of principles, the Geneva plan of Action; the Tunis Commitment and the Tunis Agenda for the Information Society.

The Geneva plan of Action highlights the importance of measures in the fight against cybercrime:

⁴ The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialized agency of the United Nations. The ITU has 191 Members States and more than 700 Sector Members and Associates, http://www.itu.int.

469
C5. **Building Confidence and security in the use of ICTs**

12. **Confidence and security are among the main pillars of the Information Society.**

(b) Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness.

Cyber crime was also addressed at the second phase of WSIS in Tunis in 2005. The Tunis Agenda for the Information Society highlights the need for international cooperation in the fight against cybercrime and refers to the existing legislative approaches such as the UN General Assembly Resolution and the Council of Europe Convention on Cybercrime:

*We affirm that measures undertaken to ensure Internet stability and security, to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and the Geneva Declaration of Principles (paragraph 42).*

*We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's convention on Cybercrime (paragraph 40).*

As an outcome of the WSIS, ITU was nominated as the sole Facilitator for Action Line C5 dedicated to building of confidence and security in the use of information and communication technology. At the second Facilitation Meeting.

for WSIS Action Line C5 in 2007, the ITU Secretary-General highlighted the importance of international cooperation in the fight against cybercrime and announced the launch of the *ITU Global Cyber security Agenda (GCA)*. The GCA is made up of seven main strategic goals, including the main strategic goal for the legislative measures: the elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures.¹

In order to assist the ITU's Secretary-General in developing strategic proposals to Member States, a High Level Experts Group (HLEG) was established in October 2007. This global expert group of more than 100 experts, has in June 2008 made the advices on strategies in the following five work areas: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building and International Cooperation.²

The role of ITU is to seek consensus on a framework for international cooperation in cyber security, in order to reach for a common understanding of cyber security threats among countries at all stages of economic development, that includes developing and putting into action solutions aimed at addressing the global challenges to cyber security and cybercrime.³

8. **INTERPOL**

INTERPOL is the world's largest international police organization, with 187 member countries. Created in 1923, it facilitates cross-border police cooperation, and supports and assists all organizations, authorities and services whose mission is to prevent or combat international crime.⁴

Interpol's objectives are as follows:-

- continue with and enhance its regional expert group approach to be truly international.

---

• Create, develop, and contribute to establishing international, uniform standards relating to policy, legislative, investigate, and exchange of information issues.

• Build effective partnerships to strengthen law enforcement’s efficacy and ability in responding to this criminal threat.¹

Interpol has been actively involved in combating cybercrime.² Interpol held its first Interpol Training Seminar for Investigators of computer crime, in Paris, Dec. 7-11, 1981.³ Interpol has organized its International Conference on Computer Crime in 1995, 1996, 2000, 2003, 13 to 15 April, 2005,⁴ and 12 Sept. 2007.⁵ The single most important contribution of Interpol in combating cyber crime has been the setting up 'working parties' or a group of experts at regional level. The working party consists of the heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas and in Africa. The major achievements of these working parties are briefly listed below:-

(A) **European Working Party of Information Technology Crime**

This was formed in 1990. Its noted achievement include:-


• Conducting numerous training courses in order to share its expertise with other members, presented by law enforcement experts for the benefit of law enforcement and aimed at different levels of expertise and subject areas, ranging from introductory courses to courses specializing in Internet investigations, including the Train the trainers programme.

---

² http://www.interpol.int/Public/Technologycrime/default.asp.
³ The conference was organized by Interpol in co-operation with Stein Schjolberg. It was attended by 66 delegates from 26 countries. The keynote speaker at the conference was Donn B. Parker, SRI International, Menlo Park, California, USA, the "founder" of the combat against computer crime.
⁵ http://www.intrpol.int/Public/ICPO/speeches/india20070912.asp.
Setting up of a rapid information exchange system which essentially consists of two elements: an international 24-hours response system, the National Central Reference Points (listing responsible experts within more than 100 countries currently listed this is now being expanded and has been endorsed by the High Tech Crime sub-group of the G8) and a formatted computer crime message format to ensure that all the essential information is transmitted.

The working party also recognized the necessity to complement its expertise the additional outside expertise; in order to not make the working party too cumbersome, this additional expertise (which is not restricted to law enforcement) was incorporated into so-called 'Project groups' and is selected by studying the curriculum vitae received in response to a general invitation to European member countries; these project groups are specific task motivated groups led up working party members who within the framework of a specific set period have to complete their project (the meetings are merely used to co-ordinate and streamline the efforts of the individuals, the real work is done on their own time-this has proven to be a very successful and time efficient methods).

(B) Latin American Working party on Information Technology Crime

This was formed in 2005. The aims of this working party are:

- To improve the cooperation, sharing of knowledge and practical experience INTERPOL member countries and other International Organization dealing with high-Tech Crime.
- To promote the standardization of methods and working proceedings to combat efficiently cyber crime.
- To establish a good practice guidelines.

The practical activities are:

- To coordinate with the rest of INTERPOL working parties an Information Technology crime

• To promote international police cooperation among Latin American countries.
• To share expertise on Information Technology crime investigations.
• To create and supervise the work done by the sub-groups coping with the specific necessities of the specialized units dealing with high-tech crime in Latin America.

(C) **African Regional Working Party on Information Technology Crime**

The group agreed unanimously on following objectives for the African working party on Information Technology crime:-

• Developing and making expertise available for combating information technology crime in the region and inter-regional.
• Develop and enhance partnerships with organizations which deal with information technology crime.
• Establish, co-ordinate and promote the use of best practices in investigation and prevention of information technology crime.
• Increase information flow within the regional computer crime units.
• Promotion of operating procedures standardization in the African region.

The group agreed unanimously on following project for the Interpol Working Party on Information Technology Crime Africa:-

To run an awareness program for the top management level for African countries and regional police organizations and to start targeting all African countries with information on information technology crime on a regular basis. The Head of CID should be invited to the next meeting of the group to formulate a plan of action to deploy cyber crime units.

(D) **Asia-South Pacific Working Party on Information Technology Crime**

The delegates the 10th INTERPOL Working Party on Information Technology Crime for Asia and South Pacific (Seaul 14 Nov., 2008) recommend:-
That member states should seek close cooperation between regional entities such as ASEANAPOL and to develop partnerships with public and private based in the Asia South Pacific Region;

That the Asia-South Pacific Working Party shall keep giving our assistance to Latin America working Party in order to help them to develop their own training materials;

That members states should empower INTERPOL to organize ad-hoc meetings when specific cyber crime issues are identified;

That the existing working party projects (Intelligence Scooping Project, Information Sharing Project, Training Project and Forensic Project) shall be continued effectively. In particular Country Reports shall be updated continuously in order to share that latest information among the Member states under the Intelligence Scoping Project;

That the National Central Reference Points (NCRPs) network list shall be kept fully updated; especially members states should make effort to contact to the Asia-South Pacific Countries who are not on the NCRP list to be affiliated;

The NCRP should be used appropriately as a tool of operational Assistance;

That member states shall take part in our Training Party from the Trainers and Trainees point of view to develop capability Building.

To coordinate the efforts of regional working parties, Interpol has also set up a steering committee for Information Technology Crime. The task of this committee is to streamline the individual efforts of the member countries by avoiding unnecessary duplication and the resultant waste of human and financial resources. The SC has now gone a step further by contacting organizations outside of Interpol and involving them in their initiatives. To date, they have thus achieved success, most notably with the High Tech Crime Sub-group of the G8, the International Chamber of Commerce, UNAFEI (the United Nations Asia Institute
for the Prevention of Crime and the Treatment of Offenders), as well as with several academic institutions.¹

8.1 7th International Conference

Interpol's 7th international conference on cyber crime kicked off in New Delhi on 12 to 14 Sept., 2007.²

Interpol proposed on 12 Sept, 2007 the creation of global and Regional anti-crime centres to fight criminal activity online and respond quickly to emergency cybercrime alerts. During on international cyber crimes conference in New Delhi, Interpol Secretary-General Ronald K. Noble said that "the Internet should not be allowed to become a place where criminals have the upper hand and can escape punishment". Officials from 37 countries discussed identity theft online bank fraud, Internet gaming and the risks of online terrorist activity during the two-day conference organized by Interpol.³

8.2 Global Security Initiative

In 2008 INTERPOL launched its Global Security Initiative for the 21st Century (GSI). Outlining a strategic vision to guide the Organization's developing and strengthen its support of global policing.

Transnational crime networks including terrorist groups, have adopted quickly to the opportunities brought by globalization. Such networks cross geographical borders and use the internet to perpetrate cybercrime, illicit trade and terrorism. Combating these crimes requires a new, collective and global approach to the role of international law enforcement and the funding to support it.

The GSI aims to tackle these international security challenges by providing the framework for a comprehensive strategy involving governments, international organizations and the private sector.

Five Pillars for Security:

The GSI sets out a new approach to address the challenges of 21st century security, focusing on five pillars that are vital to INTERPOL’s role in enhancing the safety of citizens globally. These build on the organization’s current priorities and underpin a framework of far-reaching future activities. These five pillars are:

1. **Global Security through Enhanced information sharing and Connectivity:** INTERPOL’s communications systems, databases and analysis have consistently proven their value in addressing our most pressing global threats. We now need to extend the quantity and availability of information to the law enforcement community, and develop programmes and tools that focus on securing physical and virtual borders.

2. **Secure Global Infrastructure:** Advances in information and communications technology have brought huge personal and economic benefits, but a crucial commitment to online security must be met: the commitment to protect citizens and businesses online to the same extent as we protect them in their communities and on the streets. Countering the misuse of technology will require the involvement and expertise of the companies and individuals who intended it. INTERPOL will serve as the strategic link between public and private interests committed to developing ways to combat the cyber-security threat.

3. **Global Law Enforcement Capacity:** There is a pressing need to help countries that lack the financial, technical and human resources needed to address today’s law enforcement challenges. INTERPOL’s aim is to provide the right training and tools to law enforcement bodies around the world. We need to empower our National Central Bureaus as the focus for international police co-operation within their countries and tailor our services to the needs of member countries.

4. **Strategic Global Partnerships:** Today’s security challenges require significant funding if they are to be tackled effectively. INTERPOL cannot rely on member country contributions alone to meet the growing global
security need. Public and private partnerships and investments are essential if our strategic vision is to be realized.

(5) **Innovation:** We must actively involve our global membership, academic and strategic thinkers in the world to law enforcement in shaping our future. By encouraging innovative thinking we can create an environment for success, conducive to delivering cutting-edge crime-fighting tools, technology, and a strategy to combat 21st century crime.1

8.3 **Cofee Agreement**

Under Computer Online Forensic Evidence Extractor (COFEE) agreement, Microsoft will make available to INTERPOL's 187 member countries its COFEE software tool to aid law enforcement investigators in incident response investigation access live computer system data.

Since volatile data collection is a paramount concern in live incident response situations, investigators often used to create a record of existing system files and folders without compromising its evidentiary value. COFEE will assist police in INTERPOL's member countries gather information that might otherwise be lost if the target system was shut down, by allowing investigator's to configure and use a set of programmes designed to gather content from a running system.

"Law enforcement organizations face an evolving and increasingly complex set of challenges, in the information age", said Linda K. Zecher, corporate Vice President of the Worldwide Public Sector at Microsoft. "It is essential that they are equipped with the right technologies to meet these challenges and we are pleased to partner with INTERPOL to support that cause through free distribution of the COFEE tool to frontline investigators across the world".

"The COFEE agreement and training programme will help establish a recognized international standard for digital forensics and cyber crime investigators and will therefore help law enforcement to develop internally, the expertise which it requires in the long-term", said Professor Joe Carthy of University College Dublin's (UCD) centre for cyber Crime Investigations, which

is partnering INTERPOL to develop training programmes to enable forensic experts to use COFEE.¹

INTERPOL’s 2008 General Assembly (meeting in St. Petersburg, Russia, from 7 to 10 October, 2008 at its 77th session)² in Russia approved the creation of an INTERPOL Computer Forensic Analysis Unit. Working with partners, its services to member countries will include training, impartial and independent assistance with computer forensics examination on missions, and the development of international standards for the search, seizure and investigation of electronic evidence.³

9. ASSOCIATION OF SOUTHEAST ASIAN NATIONS (ASEAN)

The Association of Southeast Asian Nations (ASEAN)⁴ has established high level Ministerial Meeting on Transnational Crime (AMMTC). At the meeting in Bangkok, January 8, 2004, a statement included cyber crime was recognized and the need for an effective legal cooperation to enhance the fight against transnational crime.

A plan of Action to Implement the joint Declaration on ASEAN-China Strategic Partnership for peace and prosperity, was signed on October 8, 2003, in Bali, Indonesia. ASEAN and China will pursue the following joint actions and measures:-

- Formulate cooperative and emergency response procedures for purpose of maintaining and enhancing cyber security, and preventing and combating cybercrime.

In a statement from ASEAN Regional Forum (ARF) on July 2006 it was emphasized that:-

---


² Creating and INTERPOL Computer forensic Analysis Unit, http://www.interpol.int/Public/ICPO/GeneralAssembly/AGN77/resolutions/AGN77 RES08.asp.


⁴ ASEAN Group consists of 10 states: Brunei Darussalam, Cambodia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Viet Nam; http://www.aseansec.org
Believing that an effective fight against cyber attacks and terrorist misuse of cyber space requires increased, rapid and well functioning legal and other forms of cooperation.

1. ARF participating states and organization endeavour to enact, if they have not yet done so, and implement cybercrime and cyber security laws in accordance with their national conditions and by referring to relevant international instruments and recommendations/guidelines for the prevention, detection, reduction, and mitigation of attacks to which they are party, including the ten recommendations in the UN General Assembly Resolution 55/63 on combating the Criminal Misuse of Information Technologies.

2. ARF participating countries and organization acknowledge the importance of a national framework for cooperation and collaboration in addressing criminal, including terrorist, misuse of cyber space and encourage the formulation of such a framework that they include...."

Ministers of ASEAN member countries and China with responsibility for cooperation in combating transnational crime met in Brunei Darussalam in November 2007. It was agreed that with the emerging challenges and increasing scope of transnational crime cooperation, the ASEAN-China Memorandum of Understanding (MoU) needed to be reviewed and revised accordingly. In a joint communiqué, including China, Japan and the Republic of Korea, a statement was adopted as follows:-

We held a retreat to exchange views on strengthening ASEAN+3 cooperation in combating transnational crime focusing on the emerging challenges of cyber-crime and its strong linkages to other transnational crime for example terrorism and trafficking in persons.

A Joint communiqué from the ASEAN chiefs of Police Conference in Brunei Darussalam in May 2008 included the adoption of resolutions on cybercrime. A joint communiqué from the ASEAN Chief of Police Conference in
Hanoi, Socialist Republic of Viet Nam on 13-15 May 2009 included the adoption of resolutions on cyber crime.¹

10. THE COMMONWEALTH

In an effort to harmonize computer related criminal law in the commonwealth countries, experts gathered together and presented a model law to the conference of ministers in 2002. That law, titled the Computer and Computer Related Crimes Act,² shares the same framework as the Convention on Cybercrime to limit conflicting guidance. The model law serves as an example to common principles each country can use to adopt framework legislation compatible with other commonwealth countries.

A Meeting of Senior Officials of Commonwealth Law Ministers was held in October 2007. The meeting addressed laws to combat terrorism and money laundering.³

11. NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO has organized a Science for Peace and Security Advanced Research Workshop in Sofia, Bulgaria, in October 2006. The workshop focused on Cyber Terrorism- a serious threat to peace and security in the 21st century.⁴

NATO has in 2008 opened a centre of excellence on cyber defence in Tallinn, Estonia, in order to conduct research and training on cyber warfare.⁵

Experts from Israel, Italy and several other NATO countries will attend the science for Peace and Security-sponsored workshop "Operational Network Intelligence: Today and Tomorrow to be held on 6-7 February 2009 in Venice, Italy. The overall purpose of the workshop is to rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber attacks.⁶

¹ http://www.aseansec.org/21619.htm.
² Legal and Constitutional Affairs Division, Commonwealth Secretariat.
⁵ http://www.nato.int/docu/update/2008/05-may/e0514a.html
⁶ http://www.nato.int/docu/update/2009/02-february/e0zo6a.html.
A workshop in Kyiv, Ukraine, on 14 and 15 May 2009, provided a valuable opportunity to share information and experience on tackling the financing of terrorism. It was well attended by participants from Allied and partner countries, as well as experts from the OSCE, academic institutions and the private sector.

The main areas of discussion were:

(1) new development in the funding sources and methods of terrorist groups;
(2) relationships between the financing of terrorism and international organized crime;
(3) the economic and financial dimension of terrorist actions directed toward critical infrastructures;
(4) national and international measures against terrorist financing.¹

NATO Advanced Networking Workshop entitled "Cyber terrorism: Prevention and Protection" is to be held in Moldova, Chisinau, May 21-23, 2009. The workshop purpose is to gather regional research teams (especially from the region of Moldova, Belarus and Ukraine) cooperated with the international experts to examine ways to develop an actionable, sustained national awareness campaign and prevention program (concrete activities and recommendations) to alert and inform widely- intraregional, federal, state and local governments, educational institutions, small business and home users about cyber security risks. Concurrent purpose is to help organizations and individuals to protect key resources critical infrastructure, and their own personal sensitive information and identities from man-made and natural threats as well as to provide knowledge transfer and utilization of appropriate advanced IT-based technologies.²

12. ASIAN PACIFIC ECONOMIC COOPERATION (APEC)

The Asian Pacific Economic Cooperation (APEC)³ has at a meeting a Mexico in October 2002 leaders collectively committed to:

³ APEC consists of 21 States: Australia, Brunei, Darussalam, Canada, Chile, People's Republic of China, Hong Kong China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papa New Guinea, Peru, Philippines, Russia, Singapore, Chinese Taipei, Thailand, United States, Viet Nam; http://www.apecsec.org.
Endeavour to enact a comprehensive set of laws relating to cyber security and cybercrime that are consistent with the provisions of international legal instruments, including United Nations General Assembly Resolution 55/63 (2000) and the convention on Cybercrime (2001), by October 2003.

In a Joint statement at the Ministerial Meeting in Santiago, Chile, November 17-18, 2004, APEC leaders agreed to strengthen the respective economies ability to combat cybercrime by enacting domestic legislation consistent with the provisions of international legal instruments, including the Convention on Cybercrime (2001), and relevant United Nations General Assembly Resolutions.

At the APEC Telecommunications and Information Working Group Meeting on September 5-9, 2005, in Seoul, Korea, a statement reads as follows:

Economies are currently implementing and enacting cyber security laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws.

At the ministerial meeting in November 2005, APEC Ministers approved an APEC Strategy to ensure a trusted, secure, and sustainable online environment. Member States was urged to:

Address the threat posed by the misuse, malicious use and criminal use of the online environment by ensuring that legal and policy framework;
Address substantive, procedural and mutual legal assistance arrangements.

The ministers renewed their commitment in the Lima Declaration, stating that they:

Encourage all economies to study the Convention on Cybercrime (2001) and endeavour to enact a comprehensive set of laws relating to cyber security and cyber crime that are consistent with international legal

---


A joint APEC-OECD Workshop on Security of Information was held in Seoul on 5-6 September, 2005. Several topics were discussed, including promoting global governmental incidents response.\(^1\) In April 2007 an APEC-OECD Workshop was held in Manila.\(^2\) A Joint APEC-OECD Workshop on initiatives among member economies promoting safer internet environment for children was held in Japan on 13 October, 2008.\(^3\)

The 39\(^{th}\) meeting of the Telecommunications and Information Working Group was held in Singapore from 13-18 April, 2009. The meeting discussed recent policy and regulatory development.\(^4\)

A chair’s Report of the Telecommunications and Information Working Group was presented to the Seventh APEC Ministerial Meeting in Bangkok on 23 April, 2008.\(^5\)

13. WORLD TRADE ORGANIZATION (WTO)

Trade related aspects of the intellectual property rights were specifically dealt by the WTO. The WTO agreements like General Agreement on Trade and Tariff (GATT) and Agreement on Trade Related Intellectual Property Rights (TRIPS) deal with piracy. Section 5 of Article 61 of the TRIPS Agreement obliges member states to provide criminal procedures with respect to prosecution of Intellectual Property Rights. It states; “Members shall provide for criminal procedures and penalties to be applied at least in case of willful trade mark, counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monitory fines sufficient to...

---

2 http://www.cybercrimelaw.net/content/Global/oecd.html
3 http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.
4 http://www.mtc.gob.pe/portal/apec/2016/10/18/Tel38_Hod.pdf
provide a deterrent consistently with the level of penalties applied for crimes of corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements, the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed willfully and on a commercial scale.¹

The WTO has discussed privacy issues with respect to the free flow of data. In the GATT agreement, WTO accepted privacy issues as a justification for limiting international data flows.

14. WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO)

This body, whose objective is furthering protection of intellectual property throughout the world, has taken some initiatives towards controlling piracy in the cyber world. WIPO has published model provisions for protecting computer programs similar to, but more comprehensive than, copyright protection, as early as in 1978. Later on it was recommended by a committee of experts in WIPO, in 1983, that neither a special protection structure nor treaties should be considered at that time, but if necessary the same may be considered at some later point. However, during a joint meeting of WIPO and UNESCO held in Geneva in 1985, majority of the participants regarded computer programs as works which deserve protection by copyright laws and only a small number of participants voted for immediate sui generis protection.

In Dec. 1996, a WIPO diplomatic conference adopted the WIPO Copyright Treaty (WCT) and the WIPO Performance and Phonograms Treaty (WPPT). These treaties contain provisions for copyright protection of copyrightable contents disseminated through global networks. The treaty obliges the contracting parties to provide legal remedies against the circumvention of

technological measures such as encryption used by authors in connection with
the exercise of their rights and against the removal of altering information, such
as certain that identify the work of their authors, necessary for the management of
their rights.

15. ORGANIZATION OF AMERICAN STATES (OAS)

The Ministers of Justice or Ministers or Attorneys General of the Americas
in the Organization of American States (OAS) recommended in Peru in 1999 the
establishment of a group of governmental experts on cybercrime. At a Meeting in
Trinidad and Tobago in 2002 recommendations were adopted giving the Group of
Experts the following mandate:

To consider the preparation of pertinent inter-American legal instruments
and model legislation for the purpose of strengthening hemispheric
cooperation in combating cybercrime, considering standards relating to
privacy, the protection of information, procedural aspects, and crime
prevention.

The Fifth Meeting of Ministers of Justice or of Ministers or Attorneys
General of the Americas in Washington D.C. on April 28-30, 2004,¹ approved
conclusions and recommendations. The recommendations included as follows:

that Member States should evaluate the advisability of implementing the
principles of the Council of Europe Convention on Cybercrime (2001), and
consider the possibility of acceding to that convention.

The General Assembly of the Organization of American States requested at
the Meeting on June 7, 2005, the Permanent Council to convene the meeting of the
Group of Governmental Experts on Cybercrime.

The Organization of American States, in cooperation with the Council of
Europe and Spain, organised a conference in Madrid on December 12-13, 2005.
This conference was titled: 
Among the conclusions was adopted:

¹ http://www.oas.org/juridico/english/cyber_meet.html
Acknowledge the importance of the only international treaty in this field: the Convention on Cybercrime which is open to all States as well as the importance of strengthening the international legal framework;

Strongly encourage States to consider the possibility of becoming Parties to this Convention in order to make use of effective and compatible laws and tools to fight cybercrime, at domestic level and on behalf of international cooperation;

Recognize the need of pursuing cooperation, providing technical assistance and organizing similar events in other regions of the world.

The Permanent Council of the Organization of American States resolved on December 15, 2005, that the Group of Governmental Experts on Cybercrime should meet on February 27-28, 2006 for the purpose of carrying out the mandates referred to in the conclusions and recommendations of the Fifth Meeting of Ministers of Justice of April 28-30, 2004.

The Group of Governmental Experts on Cybercrime met in Washington D.C. February 27-28, 2006. The Agenda included also:

Challenges on accessing, drafting and amending legislation consistent with the principles, substantive and procedural law of the Council of Europe Convention on Cybercrime (2001)

At the Sixth Meeting of Ministers of Justice in June 2006 it was made a statement as follows:

... continue to strengthen cooperation with the Council of Europe so that the OAS member states can give consideration to applying the principles of the Council of Europe's Convention on Cyber-crime and to acceding thereto, and to adopting the legal and other measures required for its implementation. Similarly, that efforts continue to strengthen mechanisms for the exchange of information and cooperation with other international organizations and agencies in the area of cybercrime, such as the United Nations, the European Union, the Asia Pacific Economic Co-operation
Forum, the Organization for Economic Co-operation and Development (OECD), the G-8 the Commonwealth, and Interpol, in order for the OAS member states to take advantage of progress in those forums.

The conclusions and recommendations were followed up at a plenary session in June 2007 and a resolution was adopted (AG/RES. 2266 (XXXVII-0/07)) A Seventh Meeting of Ministers of Justice was held in June 2008. In addition, an OAS- Council of Europe Workshop on cybercrime legislation was held in Bogota, Colombia, in September 2008.

*****