Some Cybersecurity and Cybercrime issues

- Today, we are already facing urgent growing problems of criminal and terrorist use of the Internet
  - Terrorism in cyberspace consists of both cybercrime and terrorism
  - Cyberthreats have blurred the differences between cybercrime and terrorism in cyberspace

- Nowadays Cybersecurity issues should be considered under the perspective of Peace and Security in cyberspace
  - The developments must be discussed by experts where all stakeholders are represented as soon as possible, including a way forward for a process of a global agreement in a Protocol
ITU launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges to cybersecurity could be coordinated. In order to assist the ITU in developing strategic proposals, a global High-Level Experts Group (HLEG) was established in October 2007.

- This global experts group of almost 100 persons delivered the Chairmans Report in August 2008 with recommendations, including those on cyber crime legislations.
- The Global Strategic Report was delivered in November 2008, is composed of:
  - Legal measures
  - Technical and procedural measures
  - Organizational structures
  - Capacity building
  - International cooperation

The ITU Global Cybersecurity Agenda (GCA) should be seen as an important first step towards a global approach to reduce risks and threats in cyberspace and to increase cybersecurity effectiveness.

- To fight against cybercrime, or misuses of the Internet
- That can help to increase resilience regarding the impacts of cyberthreats
- That contribute to define an appropriate cybersecurity culture
Statements

- Recognizing with appreciation the work of the Global Cybersecurity Agenda (GCA) launched by the ITU in 2007 and the strategic proposals from the High Level Experts Group (HLEG)

- Underlining the need for coordination and cooperation among States in the combat against cybercrime, and emphasize the role that can be played by the United Nations and other international and regional organizations

- Noting the work of international and regional organizations, including the work of the Council of Europe in elaborating the Convention on Cybercrime (2001) and those other organizations in promoting dialogue between government and the private sector on security measures in cyberspace, since cyberthreats are global problems and need a global harmonization involving all stakeholders

- Underlining the need for strategies on the development of a Protocol for cybersecurity and cybercrime that may serve as a global model cybersecurity and cybercrime legislation that is applicable and interoperable with existing national and regional legislative measures,

- A need of A GLOBAL PROTOCOL ON CYBERSECURITY AND CYBERCRIME is identified

Needs for a Global Protocol

- The Global Cybersecurity Agenda encourages countries to develop national cybersecurity program and international cooperation

- A “Global Protocol” should commit them to do so
  > It will constitute a reference basis for any future international agreement on cybersecurity issues
A question of global protocol

- Without a strong commitment between all actors and involved stakeholders, at national and international levels, it will be impossible to answer the information society needs.

- Without a common understanding and an international agreement, it will be impossible to set up effective security measures to correctly protect ICT resources, including critical information infrastructures, to fight against cybercrime and to preserve fundamental human rights.

Connecting the world responsibly ...

- Cybersecurity education is a long term approach which is efficient for a sustainable information society.

- Products and services should be designed with security and privacy in mind:
  - Security should be effective and efficient.

- Security - Control - Traceability should not be done by obscurity:
  - Transparency - Third control - Legal framework should exist at national and international levels.
  - Abuse of excessive security and misuse should be taken into balance when considering privacy risks management.
Fostering security and privacy

- By a pro-active and systemic approach
- By implementing technical and procedural measures
- By focalizing the attention not only on the “technical” measures, but also on:
  - Education and Awareness
  - Effective Justice and Police systems
  - Effective cooperation
    - Private / Public levels
    - National & international levels
- With respect of privacy principles or directives as specified by OCDE or Council of Europe for example
- By recognising the fact that Human Rights are not negotiable

A question of responsibility

- All actors are responsible for security and privacy
  - Users should be aware of the need for securing digital information and what can be done to foster privacy
- That will contribute avoiding building security based on fear
  - Fear is a selling argument when dealing with security issues but is not rational and does not lead to the best investments and efficiency in security and in privacy protection
- That will contribute avoiding digital security divide
  - Because in an inclusive information society opportunities should be for all!
Some legal considerations

- The Council of Europe Convention on Cybercrime (2001) is based on criminal cyber conducts in the late 1990s
  - New methods of conducts in cyberspace with criminal intent must be covered by criminal law, such as phishing, botnets, spam, identity theft, crime in virtual worlds, terrorist use of Internet, massive and coordinated cyber attacks against the critical information infrastructures
  - Many countries have adopted or preparing for new laws covering some of those conducts. In addition, the terminology included in the Convention is a late 1990s terminology, and do not necessary be suitable for the 2010s

Some legal considerations (ii)

- Even if the Convention on Cybercrime or the principles and standards it contains are accepted, the discussions at the ITU global High Level Experts Group (HLEG) meetings in 2007-2008, and the recommendations in the Chairman’s Report have revealed that for the most others regions worldwide, it still remains an European convention

- Within a global framework, it is necessary to recommend the accepted standards and principles, with certain important exceptions
  - Some countries do not accept all principles, and must be respected for their opinions
  - The discussions will also focus on the variety of viewpoints on these exceptions in order to achieve a potential for consensus

- Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable under national law.

- Crimes against peace and security in cyberspace should be established as crimes under international law through a Convention or Protocol on the United Nations level.

- A Convention or a Protocol on the United Nations level on cybersecurity and cybercrime should be a global proposal for the 2010s that is based on a potential for consensus.
  - The final draft code may be prepared by the International Law Commission. Mankind will in the future be completely dependent on information and communication technologies. Serious crimes in cyberspace should be established under international law, whether or not they are punishable under national law.

A combined global initiative on the United Nations level by organizations such as United Nations Office on Drugs and Crime (UNODC) and the International Telecommunication Union (ITU) should be established.

- This initiative could have as a final goal a Draft Convention that should be submitted to the International Law Commission for considering a United Nations Convention on Peace and Security in Cyberspace.
Draft proposition

- **Part one** of this draft code of crimes against peace and security in cyberspace, includes general provisions and principles on a Global Protocol on Cybersecurity and Cybercrime

- **Part two** includes a detailed proposal for a preliminary Model Law on Cybercrime Legislation
  - The Model Law on Cybercrime Legislation is based on the recommendations that were adopted in a broad agreement by the global High Level Experts Group (HLEG), and recommendations on additional provisions due to the technological development since 2001
  - In addition, it may be expected that the future will need protection of several new legal interests
    - The HLEG Chairman’s Report in full text is attached in Appendix 1.
    - The Global Strategic Report discussed and delivered by the HLEG is attached in Appendix 2

- **Part three** includes commentaries on the general provisions in part one.
  - Document available at: http://www.cybercrimelaw.net/Cybercrimelaw.html

A recent publication

*Title: A Global Protocol on Cybersecurity and Cybercrime*
An already discussed idea ...

IGF 2009

On the news...

World Class Standards

Thank you for your attention.