UNODC
Role in global response to Cybercrime
September 2011
Cybercrime

- Refers to criminal activity where a computer or network is the source, tool, target, or place of crime.
- Poses threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure.
Global Challenge

Internet users (% of population)

World average

Internet users in the world, (in millions)

Number of Secure Internet servers

Source: ITU and World Bank

Only data higher than 100 are represented
Links between Cybercrime and Organized Crime

- Traditional organized criminal groups adopting internet-related activities
- Clear links between the most common cybercrimes and organized crime
- Examples: child pornography, identity-related crime committed online, denial-of-service attacks
Transnational Dimension

- Cybercrime very often has a transnational dimension:
  - Due to: underlying network architecture and global availability of services (e-mail provider / hosting provider)

- Essential to promote effective international cooperation in real time
Solutions are as broad as the topic is diverse.

Ranging from:
- technical solutions
- education of users
- legal measures
- capacity building
- international cooperation
UNODC Mandates

- UN Convention Against Transnational Organized Crime
- Resolutions of the:
  - General Assembly
  - ECOSOC
  - Crime Commission
  - Crime Congress
UN GA adopted a resolution on the Creation of a Global Culture of Cybersecurity

Mandate on strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity

UN GA adopted a Resolution to convene an intergovernmental expert group on international responses to CyberCrime
• Recommended that UNODC should continue to cooperate with relevant organizations to provide technical assistance and capacity building; and

• The development of an action plan for capacity-building at the international level be also considered.
3 new resolutions adopted:

1. Relating to capacity building and technical assistance to counter cybercrime in developing countries (RES 20/8 Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building);

2. Pertaining to countering online child sexual abuse and exploitation (Res 1 Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children);

3. Relating to Technical assistance for implementing the international conventions and protocols related to counter-terrorism (includes a request that UNODC provide assistance to requesting Member States with regard to criminal justice responses to terrorism, including [amongst others] the use of the Internet for terrorist purposes).
Why UNODC?

- Only global intergovernmental body working in crime prevention and criminal justice
- Mandate to implement the UNTOC
- Comparative advantages through specialized technical competence, operational capacity and long term expertise in crime prevention, criminal justice and the rule of law
- Unique position through ability to promote international cooperation, specific focus on the developing world, role as an honest-broker with a multilateral platform and extensive network of field offices
UNODC Objectives

- Focus of efforts on the developing world (in 2005 the number of internet users in developing countries surpassed that in developed countries)
- No attempt to duplicate or re-invent the wheel
- Instead: UNODC will look to use/build on/adapt what currently exists, and involve experts and institutions which have already developed and delivered tools and/or training to combat cybercrime
- Ensure partnerships with other stakeholders such as ITU, Interpol, OSCE, EU, Europol, CoE and UN Member states, and, equally, members of the private sector (such as software companies, and Internet service providers - ISPs)
UNODC/ITU Cooperation

- In 2011 UNODC and ITU signed an MoU
- Focus is to join efforts in capacity building related to Cybercrime
  - Combination of the existing training material and courses gives countries access to a wider range of knowledge and tools
  - UNODC/ITU has access to region-specific experiences of two broad networks of field offices in all regions
  - Comprehensive approach combining crime prevention and Cybersecurity and thereby covering legal and technical standards
Proposed Program on Cybercrime

Objective - to assist developing countries to combat cybercrime

Proposed framework:

- **Legislative assistance**: Assist Member States in legislative drafting and adoption of adequate legislation based on country-specific demands and applicable instruments;

- **Capacity building** (longer-term and sustainable): Build operational and institutional capacity of law enforcement and judicial bodies in relation to investigation, prosecution, and adjudication of serious crimes, provide training, and improve international cooperation and exchange between law enforcement authorities, including mutual legal assistance;

- **International cooperation** mechanisms;

- Broad-based policy & **strategy development** including internet-based private sector companies and civil society.

- A particular component to target the **misuse of ICTs for child sexual abuse** and exploitation in developing countries.

- Mobilize and raise awareness of **civil society**.
For further information:

United Nations Office on Drugs and Crime
Vienna International Centre
PO Box 500, A-1400 Vienna, Austria
Tel: +43-1-26060-4084
Fax: +43-1-26060-7-4084
gillian.murray@unodc.org

THANK YOU