Cybercrime – the Global Challenge
Standards for the prevention and elimination of cybercrime
UNODC Cybercrime Mandates

2009: General Assembly Resolution 64/179
   Explore ways and means of addressing cybercrime

2010: General Assembly Resolution 67/189
   Comprehensive study on cybercrime

2011: Commission on Crime Prevention and Criminal Justice Resolution 20/7
   General Assembly Resolution 65/230
   Provide cybercrime technical assistance and training

2011: ECOSOC Resolution 2011/33
   Produce a study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children
   Assess the needs of States for training in investigation of these offences
   Design a technical assistance programme to meet those needs

2013: Continued work on the study and strengthened partnerships
The Global Challenge

Compared to the investigation, prosecution and adjudication of ‘conventional’ crimes (such as homicide or robbery), the involvement of a computer, mobile phone, or computer data in a crime event, presents at least three key challenges:

Access to evidence – Evidence of cybercrime exists in electronic form. The lifetime of such evidence varies enormously. The physical location of evidence also varies. Relevant evidence may be contained within vast quantities of non-relevant data, and that electronic evidence can be subject to encryption.

Handling evidence – Electronic evidence requires careful handling in order to ensure that it meets the necessary standards for use in court.

Identifying the perpetrator – The Identification of the perpetrator(s) can represent a significant challenge.
UNODC Global Programme on Cybercrime Objective: to assist developing countries to prevent and combat cybercrime through a global, sustainable and holistic approach

**UNODC Approach: The Global Programme on Cybercrime**

**Capacity Building:**
- Training for law enforcement investigators, lawyers, prosecutors and judges on investigative techniques
- Delivery of analysis tools

**Prevention:**
- Awareness raising
- Engagement of private sector solutions
- Research and analysis

**Framework Support:**
- Development of national cybercrime coordinating mechanisms
- Review and strengthening of legal frameworks

**Cooperation:**
- Development of public-private partnerships
- Strengthening of informal and formal international cooperation mechanisms

**Technical Assistance Tools:**
- Guides on comprehensive assessment, international cooperation, electronic evidence and trend monitoring

**Underlying Standards:**
- Respect for international human rights law
- Regional and international cyberlaw approaches
Combatting the problem

- **International and regional instruments**
  
  International law increasingly recognizes that children deserve special protection.

- **National laws and policies**
  
  States vary considerably in approaches to addressing forms of child abuse and exploitation. While many States criminalize acts such as production of child sexual abuse material, they may differ with respect to elements of the crime and definitions of “child”.

- **International cooperation**
  
  Tools and mechanisms for international cooperation include mutual legal assistance treaties, direct law enforcement cooperation, multi-agency partnerships, forums for information-sharing and informal direct law enforcement cooperation.
Combatting the problem

- **Investigation of offences**
  Specific tools can be employed for detection and investigation: digital forensic techniques, automated search, image analysis and image databases, data mining and analytics.

- **Private sector responses**
  Electronic service providers may engage in this respect through varying degrees of self-regulation, including by internet service providers, self-monitoring by travel and tourism companies and the creation of financial coalitions.

- **Civil society responses**
  Parents, guardians, child educators and civil society are a further vital component in combating the problem, including in supporting children in understanding and handling online risks, the “flagging” of certain material online, the creation of telephone hotlines for reporting, and contributions towards education and psycho-social methods of prevention.
International Instruments to combating ICT-Facilitated sexual abuse and exploitation of children

2. The Optional Protocol to the CRC on the Sale of Children, Child Prostitution, and Child Pornography
4. The Protocol to Prevent, Suppress, and Punish Trafficking in persons, Especially Women and Children
5. Guidelines on Justice in Matters Involving Child Victims and Witnesses of Crime

Prevention, investigation and prosecution of any “serious crime” - includes the use of ICTs to abuse or exploit children. Develop training for combatting crimes through the use of computers...

It renders irrelevant the consent of any child victim of the practice of trafficking in persons
Regional Instruments to combating ICT-Facilitated sexual abuse and exploitation of children

1. Council of Europe Convention on Cybercrime
   Aims to provide a common criminal policy. Art.9 deals with offences related to child pornography.

2. Council of Europe Convention on the Protection of Children against sexual exploitation and sexual abuse
   Aims to prevent and combat sexual exploitation and sexual abuse of children...

3. African Charter on the rights and welfare of the Child
   Protect children from all forms of sexual exploitation and sexual abuse
Regional Instruments to combating ICT-Facilitated sexual abuse and exploitation of children (Child pornography)

1. Commonwealth Model Law (art.10)

2. EU Directive on Child Exploitation (art.15)

3. ITU/CARICOM/CTU Model Legislative (art.13)

4. League of Arab States Convention (Art.12)

5. Draft African Union Convention (art.9)
Figure 3.1: Cybercrime legislation areas

- Criminalization: Existing legislation (38%) vs. New or planned legislation (27%)
- Investigative measures: Existing legislation (15%) vs. New or planned legislation (17%)
- Jurisdiction: Existing legislation (14%) vs. New or planned legislation (11%)
- Electronic evidence: Existing legislation (9%) vs. New or planned legislation (13%)
- International cooperation: Existing legislation (6%) vs. New or planned legislation (12%)
- Prevention: Existing legislation (9%) vs. New or planned legislation (6%)
- Public-private cooperation: Existing legislation (5%) vs. New or planned legislation (5%)
- Other: Existing legislation (6%) vs. New or planned legislation (5%)

Source: Study cybercrime questionnaire. Q12 and Q14. (n=55,36; r=262,111)
National Law

Figure 4.1: National approaches to criminalization of cybercrime acts

- Illegal access
- Illegal interception
- Illegal interference
- Computer misuse tools
- Breach of privacy
- Fraud or forgery
- Identity offences
- Copyright or trademark offences
- SPAM
- Personal harm
- Racism and xenophobia
- Child pornography
- Solicitation or grooming
- Terrorism support offences

Source: Study cybercrime questionnaire. Q25-38. (n=61)
Figure 4.23: Criminalization of computer-related production, distribution or possession of child pornography

- 18% Yes, cyber-specific offence
- 3% Yes, general offence
- 14% Yes, both
- 65% No, not a criminal offence

Source: Study cybercrime questionnaire. Q36. (n=57)
Figure 4.27: Acts constituting child pornography offences

- Accessing: 37%
- Possession only: 63%
- Distribution: 93%
- Copying: 14%
- Production: 89%

Source: UNODC legislation review. (n=70)
Figure 4.28: Criminalization of computer-related solicitation or 'grooming' of children

- 52% Yes, general offence
- 26% Yes, cyber-specific offence
- 17% Yes, both
- 5% No, not a criminal offence

Source: Study cybercrime questionnaire. Q37. (n=54)
Assessment of the training needs of States

Identification of crimes

- Lack of dedicated staff trained in all aspects of ICT. Facilitated child abuse and exploitation cases.
  - Training for persons may best take place on an inter-agency basis.

- The investigation of ICT-F child abuse tended to be reactive in nature, rather than proactive.

- States require a clear legal framework that regulates undercover operations.

  Less 1% of all polices are specialists in cybercrime.

  El Salvador have only one forensic examiner.
Assessment of the training needs of States

- **Investigative capabilities and electronic evidence**
  - Lack of ability to obtain stores or real-time data on traffic content.
  - Service providers require due legal process for disclosure of customer data.
  - Lack basic sufficient material resources, hardware, software and internet.
  - Specialized training for prosecutors and judges in handling digital evidence is a need.

- **International cooperation**
  - Lack of standard operating procedures for requests involving digital evidence
  - Lack of contacts in requested countries (some use the diplomatic via)

In El Salvador the Internet Services Providers only store data for a maximum of 3 months (they said don't have enough space)
Assessment of the training needs of States

VPin victim assistance and awareness raising

- Absence of standard protocols for supporting victims through the investigative process, techniques for interviewing victims and collection and preservation of victim-related evidence

- Lack of awareness among children, families and society in respect of whether—cyberbullying, sexual harassment—constitutes a criminal offence or not.

- Need to promote awareness

• Policy and coordination

- The development of an overarching national law, policy or strategy against ICT-facilitated child abuse and exploitations with clear priorities and targets can greatly contribute to a sustainable, coordinated effort against such offences.

- Urgent need for senior officials in the criminal justice field to be aware of such problems and the importance of digital evidence in investigations.
UNODC technical assistance programme to prevent and combat technology-facilitated child abuse and exploitation

➢ Law enforcement training

- Training on specialized methods for investigating online crimes (types of crimes, offender and victim profile, international image checking, assistance to victims, and rights of the children.
- Support the authorities in establishing the necessary structures for the effective operation of police.
- Support to strengthening cooperation with internet service providers.
- Training on human rights aspects of law enforcement investigations

➢ International cooperation

- Support to authorities responsible for preparing and sending and receiving and implementing mutual legal assistance requests

➢ Training for prosecutors and judges

- Training for prosecutors and judges on protection considerations where child victims are required to testify
UNODC technical assistance programme to prevent and combat technology-facilitated child abuse and exploitation

- Awareness raising
  - Public awareness-raising campaigns.
  - Develop an awareness raising toolkit.

- Sustainability
  - Mechanism to ensure the sustainability of support may include the accreditation for training courses with national police academies and other relevant institutions.
Thank you

Bertha Nayelly Loya
Officer Research
Bertha.loya@unodc.org
+(503) 22 48 88 25