UN Comprehensive Study on Cybercrime

Organized Crime and Illicit Trafficking Branch
Division for Treaty Affairs

Why is cybercrime a particular challenge?
Analogy with ‘conventional crime’

The Act
The Victim/Target

The Modus Operandi

UNODC
United Nations Office on Drugs and Crime
The Perpetrator

The Response?
Criminal Justice - Legislation

Criminal Justice - Evidence
Criminal Justice- Investigation

International cooperation

Prevention
A Cybercrime Response: The Core Elements

1) Legislation
   • Criminalization
   • Procedural powers and electronic evidence
   • Jurisdiction
   • Responsibility and liability of the private sector
   • International cooperation

2) Law enforcement, prosecution and court capacity
3) International cooperation mechanisms
4) Prevention: public-private partnerships and awareness raising
5) In line with human rights and the rule of law

The UN Cybercrime Study

• Mandated by General Assembly Resolution 65/230 and conducted by an open-ended intergovernmental expert group
• Aims to present a comprehensive global picture of:
  • the problem of cybercrime
  • responses to it by Member States, the international community and the private sector
• Will examine options for strengthening existing and proposing new national and international legal or other responses to cybercrime
### What is Cybercrime Anyway?

#### Acts against the confidentiality, integrity and availability of computer systems and data
- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data
- Illegal data interference or system interference
- Production, distribution or possession of computer misuse tools
- Breach of privacy or data protection measures

#### Computer-related acts for personal or financial gain
- Computer-related fraud or forgery
- Computer-related identity offences
- Computer-related copyright and trademark offences
- Sending or controlling sending of SPAM

**UNODC**

### What is Cybercrime Anyway?

#### Specific computer-related acts
- Computer-related acts causing personal harm
- Computer-related acts involving racism or xenophobia
- Computer-related production, distribution, or possession of child pornography
- Computer-related solicitation or ‘grooming’ of children
- Computer-related acts in support of terrorism offences

**UNODC**
The Study Topics

- The phenomenon of cybercrime
- Cybercrime legislation
- Criminalization
- Law enforcement investigation and procedure
- Electronic evidence
- Criminal justice response and capacity
- International cooperation
- Cybercrime prevention
- Cybercrime and human rights

The UN Cybercrime Study

Member state questionnaire

Private sector questionnaire

Intergovernmental organizations and academia questionnaire

Comprehensive study

Other material and consultations
Study Timeline

**February 2012:** Finalization of the questionnaire and dissemination to Member States, the private sector, IGOs and academia

**April 2012:** Regional workshops to support countries in completing the questionnaire. Chair of expert group makes informal presentation to Crime Commission

**End May 2012:** Deadline for receipt of responses to the questionnaire

**November 2012:** Second meeting of the Expert Group and presentation of preliminary results

**December 2012 – March 2013:** Drafting and finalization with a view to presentation of the study to the Crime Commission in April 2013
The Study Questionnaire

- Covers the **core elements** needed for a cybercrime response (legislation, capacity, international cooperation, prevention and human rights)
- Includes ‘**act descriptions**’ as a common basis for discussion
- Divided into different tabs for **different institutions**:
  - General section (1 tab)
  - Legislators (2 tabs)
  - Police (2 tabs)
  - Prosecution (2 tabs)
  - Courts (1 tab)
  - International cooperation authorities (3 tabs)

This Workshop

- Provides an opportunity to contribute to a piece of global research that will **inform the future cybercrime agenda** at international level
- Provides an opportunity to **exchange experience** on challenges and good practices in preventing and combating cybercrime in the region
- Offers support to the ongoing process of **national self-assessment** in the area of cybercrime by providing a **framework** for core elements of the cybercrime response
- Will focus on **legislation**, police and criminal justice **capacities** and **international cooperation**
# Agenda

## This Morning
- Introduction to country cybercrime situations
- First look at the study questionnaire

## This Afternoon
- Working session on cybercrime legislation
- Working session on police, prosecution and court capacities, challenges and good practices

## Tomorrow Morning
- Working session on police, prosecution and court capacities, challenges and good practices (continued)
- Working session on international cooperation

## Tomorrow Afternoon
- Exchange of experience on process of national cybercrime assessment
- Workshop conclusions
Thank you

cybercrime.study@unodc.org
steven.malby@unodc.org