CYS 2310
Policy, Legal, Ethics and Compliance

Lecture # 5
International legal frameworks for combating cybercrime

Learning Objectives

In this chapter, we will cover the following topics:

- ✓ Cybercrime: Identifying the challenge
- ✓ UNODC Cybercrime Study (draft)
- ✓ Criminal justice responses to cybercrime
- ✓ Substantive provisions: criminalization
- ✓ Identity-related crime (committed online)

Cybercrime: Identifying the challenge

- Efforts to define cybercrime: an aggregate term?
- Acts constituting cybercrime:
  - Acts against the confidentiality, integrity and availability of computer data or systems;
  - Computer-related acts for personal or financial gain or harm;
  - Computer-content-related acts
- Boundaries between cybercrime and conventional crime increasingly blurred

UNODC Cybercrime Study (draft)

- GA resolution 65/230: in line with paragraph 42 of the Salvador Declaration (Twelfth UN Crime Congress), establishment of an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.
- The draft Study (2013) represented a “snapshot” in time of crime prevention and criminal justice efforts to prevent and combat cybercrime

Criminal justice responses to cybercrime

Divergent national approaches

- Historical legal differences but also different socio-cultural approaches and constitutional orders

Need for harmonization

- Also through international instruments
- Substantive provisions: criminalization
- Procedural and enforcement provisions: electronic evidence, investigative powers and measures, jurisdictional issues
- International cooperation

Substantive Provisions: Criminalization

Widespread criminalization of cybercrime acts

- With the primary exception of spam offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia and online solicitation or "grooming" of children.

Specific cybercrime offences v. general offences

- Core cybercrime acts against the confidentiality, integrity and accessibility of computer systems criminalized in many jurisdictions using cyber-specific offences.
- Computer-related acts such as those involving breach of privacy, fraud or forgery and identity offences mostly criminalized using general offences.

ICT-facilitated child sexual abuse and exploitation

UNODC study on the effects of new information technologies on the abuse and exploitation of children (ECOSOC resolution 2011/13)

- Global picture of the problem
- Definition of the typology of the crimes that need to be addressed
- Appropriate responses at national and international levels
- Concrete guiding tool for technical assistance

Identity-related crime (committed online)

United Nations study on fraud and the criminal misuse and falsification of identity (2007)

- Mandate: Economic and Social Council resolution 2004/26 of 21 July 2004 on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes"

- Initial concept: "criminal misuse and falsification of identity"

Identity-related crime (committed online)

- “Identity theft”: Taking identification or personal information in a manner analogous to theft, including theft of tangible documents and intangible information and deceptively persuading individuals to surrender documents or information voluntarily.
- “Identity fraud”: The subsequent use of identification or identity information to deceive others.
- “Identity-related crime”: more generic form to cover all forms of illicit conduct involving identity.

Identity-related crime (committed online)

Different crimes involving the criminal misuse and falsification of identity:

- Illicit taking of ID documents or information (theft, “phishing” or “pharming”, skimming of credit cards)
- Stolen documents or information used to commit other crimes (fraud) or to obtain further ID and build false identity for later use
- Illicitly taken ID documents or identity information traded or sold as a form of illicit commodity

Identity-related crime (committed online)

Different crimes involving the criminal misuse and falsification of identity:

- Alteration of legitimate ID documents (forgery)
- Fabrication of ID documents (forgery)
- Tampering with underlying identity documents
- General offences of corruption and bribery related to the use of false or misleading information

Identity-related crime (committed online)

- Identity-related crime represents a new criminal justice perspective on an old problem which emphasizes abuse of identity itself rather than other crimes supported by identity abuse.
- **New approach**: Criminalization of abuses of identity or identification information as such, as opposed to the traditional approach of criminalizing other activities committed using false identities.
- Protection of two groups of victims:
  - Those whose identities are misused; and
  - Those who may be the victims of other offences committed using false identities.

Identity-related crime (committed online)

Core group of experts on identity-related crime: six meetings (2007-2013)

- Consultative platform on identity-related crime with the aim to bring together senior public sector representatives, business leaders, international and regional organizations and other stakeholders to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime.

Review

- Cybercrime: Identifying the challenge
- UNODC Cybercrime Study (draft)
- Criminal justice responses to cybercrime
- Substantive provisions: criminalization
- Identity-related crime (committed online)

End of Lecture