UNODC
United Nations Office on Drugs and Crime

International legal frameworks for combating cybercrime: the UNODC perspective

Dimosthenis Chrysikos
Organized Crime and Illicit Trafficking Branch
Division for Treaty Affairs, UNODC

OAS REMJA Working Group on Cybercrime
Ninth meeting (Washington D.C., 12-13 December 2016)

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.

https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

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

  https://www.unodc.org/documents/organized-crime/cybercrime/Study_on_the_Effects.pdf

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 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
- 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)

- ✓ Handbook on identity-related crime (2011)

http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

- ✓ 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.

Procedural and enforcement provisions

- **Electronic evidence**
  - Traditional criminal procedural laws typically contain provisions on the gathering and admissibility of evidence.
  - Fragile nature: easily altered, damaged or destroyed by improper handling or improper examination. Special precautions to document, collect, preserve and examine this type of evidence.
  - Admissibility of electronic evidence in courts

- **Investigative powers and measures**
  - Obtaining evidence of cybercrime requires a combination of both traditional and new investigation techniques.
  - While legal approaches vary, key investigative powers include search and seizure, orders for computer data, real-time collection of data and data preservation.

- **Jurisdictional issues**
  - Need for flexibility and establishment of different jurisdictional bases (transnational nature of cybercrime)

International cooperation

- **Mutual legal assistance involving electronic evidence**:
  - Crimes involving electronic evidence pose unique challenges for international cooperation.
  - Owing to the **volatile nature of electronic evidence**, international cooperation to combat cybercrime requires a **timely response** and the ability to request specialized investigative actions, including the **preservation and production of data by private sector providers**.
  - Response times for mutual legal assistance requests involving the investigation of cybercrime may often fall outside service providers' data retention periods or may enable perpetrators to permanently destroy key digital evidence.
  - Effective international cooperation in cases involving electronic evidence therefore requires **mechanisms for the expedited preservation of data pending the consideration of further investigative measures**

International standards

- **Binding multilateral instruments**

  - Both ad hoc instruments on cybercrime of regional impact and instruments of international cooperation in criminal matters (also to combat cybercrime).
  - Council of Europe Convention on Cybercrime: benchmark of international standards.
  - The issue of the necessity of a global instrument still open.
  - Applicability of UNTOC, when necessary conditions are met. Broad scope of international cooperation provisions

Capacity-building

- **Technical assistance for different groups: policy-makers and legislators; criminal justice and law enforcement personnel; central authorities**

  - UNODC Global Programme on Cybercrime
  - Training courses for prosecutors, investigators and law enforcement authorities on electronic evidence and cybercrime investigations
  - UNODC Cybercrime Repository
  - MLA Request Writer Tool (with a separate module on electronic evidence)

Capacity-building

- **Centralized cybercrime structures or units**

  - Specialization of national law enforcement authorities in the investigation of cybercrime (or even “conventional” crime involving electronic evidence)
  - Concentration of resources in a single place to build capacity on specialized investigation techniques and to adequately gather and analyze electronic evidence
  - Further training provided by such structures or units to other local law enforcement agencies

Expediting the MLA process involving electronic evidence

- **Mutual Legal Assistance Request Writer Tool**:

  - Tool to provide guidance to practitioners through each step of the drafting process of a mutual legal assistance request.
  - The advantage offered by the tool is that the necessary information is saved in order to generate, at the final stage, the draft request in a format ready for signature and submission.
  - Usefulness of the tool as:
    - ✓ a practical guide for practitioners from developing countries which could accelerate the submission of MLA requests; and
    - ✓ as a way to generate a format of requests that could be accepted by counterparts in developed countries acting as requested States.

Expediting the MLA process

- **Revised version of the Mutual Legal Assistance Request Writer Tool**:

  - **Electronic evidence module**

    - ✓**Expedited preservation of stored computer data**

      Order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of the Requested State and in respect of which there is the intention to submit a formal request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

Expediting the MLA process

- **Revised version of the Mutual Legal Assistance Request Writer Tool**:

  - **Electronic evidence module**

    - ✓**Ensuring access to stored computer data**

      Search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the Requested State, including data that has been preserved

Expediting the MLA process

- **Revised version of the Mutual Legal Assistance Request Writer Tool**:

  - **Elextronic evidence module**

    - ✓ **Real-time collection of traffic data**

      Real-time collection of traffic data associated with specified communications in the territory of the Requested State transmitted by means of a computer system.

UNODC
United Nations Office on Drugs and Crime

Thank you for your attention

Contact Information:
Organized Crime and Illicit Trafficking Branch
Division for Treaty Affairs
UNODC, Vienna

dimosthenis.chrysikos@unodc.org
Tel.: +43-1-26060-5586