UNODC’s activities towards the strengthening of criminal investigation teams in Public Ministries.

ITU Regional Cybersecurity Forum for Americas
Santo Domingo, Dominican Republic

23-25 November 2009
Introduction

- Mission: Facilitate the security and justice for all through supporting the States and its citizens against the threats of drugs, crime and terrorism.

- UNODC seeks to achieve security and justice for all, helping people and States to be safe from the threats of drugs, crime and terrorism.
Topic Areas

- Terrorism
- Money Laundering
- Corruption
- Organized crime and illicit trafficking (persons, migrants, weapons)
- Crime prevention and criminal justice reform
- Drug Demand Reduction and HIV
- Research and analysis of threats
- Forensic and scientific services

Focusing on an integrated program and experience to achieve the greatest impact on its results.
Mandate

The UNODC’s work is guided by a wide range of international legal instruments and a set of rules and regulations of the United Nations in crime prevention and criminal justice.

• United Nations Convention against Corruption.

The Convention is complemented by the following three protocols:

• The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children.
• The Protocol against the Smuggling of Migrants by Land, Sea and Air.
• The Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition.
Mandate

• International legal framework against terrorism.
  – Security Council Resolutions against Terrorism.
  – Comprehensive and integrated strategy against terrorism, which recognizes the UNODC as the main office responsible for providing legal assistance in preventing terrorism. (General Assembly - 2006).

• Standards and rules of the United Nations concerning the prevention of crime and criminal justice.
Cybercrime in the scope of UNODC

- The transnational nature of cybercrime, the involvement of the organized crime groups and the weaknesses governance that give sustainability to these forms of crime, make them highly relevant to the mandate of UNODC.

- It refers to the activity where the computer or network is the source, tool, target or scene of a crime. These crimes can be divided into:
  1. Those who aim to network computers or devices on the same directly.
  2. Those that are facilitated by computer networks or devices whose primary objective is independent of network or device itself.
Why UNODC?

- Only global intergovernmental body working in crime prevention and criminal justice
- Mandate to implement the UNTOC (United Nations Convention against Transnational Organized Crime)
- Comparative advantages through specialised 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 multi-lateral platform and extensive network of field offices.
UNODC actions for the strengthening the justice system and law enforcement institutions in their fight against cybercrime

- Ensure the elimination of "safe havens" for the cybercriminals.
- Coordinate the cooperation in its investigation and prosecution.
- Exchanging information to fight it.
- Train and equip law enforcement personnel to confront it.
- Protecting data security and computer systems.
- Allow the preservation and quick access to electronic information belonging to a criminal investigation.
- Remember to citizenship requirements to prevent and combat it.

- Ensure mutual aid schemes for timely investigations and for the collection and exchange of evidence.
- Designing solutions that help prevent and detect this activity.
- Take into account both the protection of individual freedoms and privacy and the ability of governments to combat it.
- Identify and disseminate best practices and promote the association of public and private organizations to combat it.
Some relevant issues or vulnerabilities to address in the scope of institutional strengthening in the criminal investigation field require attention.

- Organized crime uses instruments for their activities along with technological advances.
- The way and capacity of reaction of the Public Ministry investigation teams is limited in resources and methods to combat effectively this scourge.
- Weak inter-institutional integration to face complex causes.
- Bureaucracy of legal procedures in prosecution. In general, the criminal prosecution institutions are awaiting for the compliant be made.
- Overload generated by less complex cases or without much significance.
- Limited use of alternative solutions and discrentional decisions in prosecution.
- Use of a bureaucratic management model and rigid working structures.
Improving and strengthening investigation teams would provide benefits for better addressing of cybercrime cases, identified as complex, some of which are:

- A much less bureaucratic working model, flexible and timely.
- Proactive analysis capacity of criminal activity.
- Dynamic team integration for the case to be investigated according to their characteristics and demands of specialization (technical and legal).
- Prosecutor leadership and coordination.
- Case analysis and possible scenario development for faster *modus operandi* identification, thru an extensive use of IT tools as well as brainstorming, mind mapping methodologies.
- Better coordination at local, national and international levels.
- Budget and resource requirements planning.
- Regular strategy monitoring (feedback)
- Use of the discreional faculties from criminal prosecution to be concentrate in the most relevant cases and participants with the greatest responsibility.
THANK YOU

Alberto Bolaña Wittenberger
Senior Consultant
UNODC - Panama Program Regional Office
alberto.bolana@unodc.org
For more information please contact:

Gillian Murray
Focal Point for Cybercrime, Division for Treaty Affairs.
UNODC - Viena, Austria
Gillian.murray@unodc.org