UNODC tackling cybercrime in support of a safe and resilient AP-IS

Himal Ojha
Cybercrime/Digital Forensics Consultant
Global Programme on Cybercrime

Asia-Pacific Information Superhighway Steering Committee and WSIS Regional Review, Third Session

27 August 2019
UNITED NATIONS OFFICE ON DRUGS AND CRIME

GOAL:

To better equip governments to handle drugs, crime, terrorism, and corruption-related issues, by maximizing knowledge on these issues among governmental institutions and agencies, and also to maximizing awareness of said matters in public opinion, globally, nationally and at community level.

General Assembly resolution 65/230 and Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8

3 Pillars

- Field-based technical cooperation
- Research and analytical work
- Normative work to assist States in the ratification and implementation of the relevant international treaties and the development of domestic legislation

Global Programme on Cybercrime

- Cybercrime
- Online Child Protection
- Digital Forensics
Supporter Abu Mustafa is able to raise five bitcoins (approx. $1000) before his account was shut down by the FBI.

Mujahideen receives around 0.929 bitcoins (approx. $540) after adding the option of Bitcoin donation.

January 2015

June 2015
Ali Shukri Amin used social media to instruct donors on the use of Bitcoin to provide untraceable financial support to ISIS.

June 2016

Hamas shifts tactics in bitcoin fundraising.

January 2017

Indonesia’s financial transactions agency announces that Bitcoin was used by IS to fund terrorist activities in Indonesia.

April 2019
Hamas shifts tactics in bitcoin fundraising.
The objective: Project countries more effectively prevent and counter terrorism financing and money laundering through a better understanding of cryptocurrencies regulatory frameworks and enhanced capacities to identify and investigate crimes involving cryptocurrencies.

Beneficiary agencies: Central Banks, FIUs, Prosecution, Law Enforcement agencies of beneficiary countries.

Geographical scope:
Primary Scope: Cambodia, Myanmar, Lao PDR
Secondary Scope: Rest of ASEAN countries

Project Outputs:
- Strengthening domestic legal and regulatory frameworks on cryptocurrencies use for AML/CFT
- Awareness raised for law and policy makers on evolving cryptocurrencies threats
- Capacity building on effective AML/CFT investigation and prosecution

Project Activities:
1. **Train the Trainer Course** on Cryptocurrencies and Darknet Investigations - one regional event
2. **National Roundtables** on Cybercrime and Cryptocurrencies: Facilitate discussion and raise awareness on risks for AML CFT Money Laundering - one per project country
3. **National Capacity Building Training Courses** on Cryptocurrency and Darknet Investigations - one per project country
4. **Southeast Asian Working Group Meeting** on Cryptocurrencies - one regional conference

Timeline: March 2019 – March 2020
OUTCOME

Working Groups

- Southeast Asia Working Group on Cryptocurrencies
- UNODC Cryptocurrencies Experts Workshop

Mentoring

- Darknet and Cryptocurrencies Investigations Training

Executive Branches of Government and Specialized Officers

- Judges/Prosecutors
- Cybercrime Investigators
- Counter-Terrorism Investigators
- Intelligence Officers
- Central Bank/AMLO/FIU

700+ Personnel's Trained

OSINT, Online undercover operations
- Dedicated training infrastructure (VMs, mailing servers, avatars, Darknet)
Tackling wildlife cybercrime through the use of online platforms and other ICT mediums for illegal selling and trading

The Objective: To establish a functional digital forensics laboratory with appropriate hardware and software in Laos for investigation of wildlife cybercrime and other general cybercrime.

Beneficiary agencies: Lao Police Force

Project Outputs:
- Establishing a functional digital forensics lab
- Provide capacity building trainings to law enforcement agencies, investigators and prosecutors in different phases;
- Discuss the current state of cybersecurity, cybercrime and digital forensics in the country, the challenges and issues

Project Activities
- National Cybercrime Roundtable Discussion
- Establishment of functional Digital Forensics Laboratory
- National Training courses on Digital Forensics for cybercrime and wildlife investigations

Funded by the Government of Norway
Selection of Criteria of Selection

- Pre and Post Questionnaires
- Technical Skills & Enthusiasm

Modules:

- Introduction to Computer Data
- Imaging and Hashing
- Data Carving and Metadata
- Browser Artefacts
- Registry Artefacts
- Computer Forensic Strategies
- Image Acquisition
- Memory Forensics
- Mobile Forensics
- Solid State Drives and More

Beneficiaries:

- Department of Economic Police
- Police Academic
- Forensics Police Department
- Ministry of Agriculture and Forestry
- International Relations Department
- Department of Anti-Human Trafficking
- The Office of Supreme People’s Prosecutors
- Department of Immigration

Phase 1
3 days training

37 Participants

Phase 2
5 days training

23 Participants

Phase 3
5 days training

In the established Digital Forensics Laboratory

6 Participants

43 Participants

Practical case scenarios in every module
UNODC opens the first specialized Forensics Laboratory in Laos for analysing digital evidence

Vientiane (Lao PDR) 23 August 2019 - The United Nations Office on Drugs and Crime Global Programme on Cybercrime and the Lao People’s Democratic Republic Police Force have jointly opened Laos’ first Digital Forensics Laboratory. The lab will specialize in the analysis of digital evidence seized, or resulting from, criminal investigations in Laos including transnational organized crime, cybercrime and wildlife crime.
Standard Operating Procedures for Digital Evidence
OUTCOME

• Industry standard equipment's
• Increased efficiency of securing the evidence in relation to wildlife crime and general cybercrime
• Justifiable in the court of the law by preserving the integrity and existence of the evidence
• Prove the perpetrators in the court of law of his actions and be able to put him behind the bars.

The police force will be able to analyse at least 6 evidence per day

\[ 6 \times 30 = \text{around 180 evidence per month} \]

More than 2000 evidence per year
Cyber CT
Enhancing capacities to respond to cybercrime and to counter terrorist use of Information and Communications Technology throughout selected ASEAN member states

The objective: Project countries more effectively respond to cybercrime and are able to counter terrorist use of Information and Communications Technology by having increased capacities to detect, investigate and disrupt illicit cybercrime and terrorist activities.

Beneficiary agencies: Prosecution and Law Enforcement agencies of beneficiary countries

Geographical scope: Cambodia, Lao PDR, Myanmar, Vietnam

Project Outputs:
- Enhancing Regional Cybercrime Cooperation focused on Countering Terrorist use of Information and Communications Technologies (ICT)
- Enhancing Cyber Terrorism Investigation and cyber intelligence operational capability through Capability Maturity Assessment and Program Enhancement:

Project Activities:
1. Train the Trainer Course on Cyber Threat Intelligence in Counter-Terrorism Operations - one regional event
2. National capacity building training on Cyber Threat Intelligence in Counter-Terrorism Operations - one per project country
3. Regional training workshops on Cybercrime and Counter Terrorism Policy & Strategy Development - two events
4. Regional conference on Cyber Threat Intelligence in Counter-Terrorism Operations - one conference

Timeline: March 2019 – March 2020

Funded by The Government of Japan
Clearweb and Darknet Threat Assessment

Beneficiary agencies: Law Enforcement Agencies of Beneficiary Countries

Objective: ASEAN Member States to effectively be aware and address current cyber (dependent and enabled) threat landscape through the enhancement of Darknet Investigative and Reactive capabilities to counter cybercrime and transnational organized crime.

Geographical Scope: ASEAN Countries

Project Outputs:

• Specialized Clearweb and Darkweb Threat Assessment.
• Strengthening the capacity of Law Enforcement on Cryptocurrencies and Darknet Investigations.
• Awareness to government counterparts on cybercrime threat landscape and the use of technology for terrorist use.

Disclaimer:
Information discussed at NRTD is confidential.
Information shared in report dependent on Member States’ approval.

Funded by The Government of Japan
Thank You

UNODC Global Programme On Cybercrime

Himal Ojha

Mobile: +66 091 865 1023
WhatsApp: same as mobile
Email: himal.ojha@un.org
https://linkedin.com/in/himal.ojha