



Cybercrime Training Strategies: Philippines

PHILIPPINE DELEGATION

International Workshop on Cybercrime Training
Strategies for Law Enforcement Agencies and
access to ECTEG materials
15-16 June 2017
Brussels, Belgium

OUTLINE

- 1. Legal Framework**
- 2. Department of Justice-Office of Cybercrime**
- 3. Trainings Conducted**

INTRODUCTION

- International Law
 - **Convention on Cybercrime (Budapest, November 23, 2001)**
“a common criminal policy aimed at the protection of society against cybercrime...” (Convention on Cybercrime, Preamble)
- Domestic Law
 - **Cybercrime Prevention Act of 2012 (RA 10175)**
“...the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.” (RA 10175, Sec. 2)

DEPARTMENT OF JUSTICE – OFFICE OF CYBERCRIME (DOJ-OOC)

- Designated as the central authority in all matters related to international mutual assistance and extradition. (RA 10175, Sec. 23)
- Acts as Competent Authority for all requests for assistance for investigation or proceedings concerning cybercrimes, including the provision of technical advice. (RA 10175 IRR, Sec. 28(a))
- Facilitates international cooperation with other law enforcement agencies on... capacity-building related to cybercrime prevention, suppression, and prosecution. (RA 10175 IRR, Sec. 28(g))

CYBERCRIME TRAININGS CONDUCTED

- **CYBERCRIME INVESTIGATION TRAININGS**

- This particular series of trainings conducted by the OOC is entitled **“Investigating and Prosecuting Cybercrimes: Focus on Electronic Evidence”**.
- The objective is to impart knowledge to the law enforcers on how to preserve, utilize, and appreciate ICTs in conducting their investigations that would involve computers, computer systems, and computer data, among others.
- The DOJ-OOC has trained a total of **520** investigators, prosecutors, and public attorneys as of **March 2017**.
- **13 out of 18 Regions** in the Philippines.

CYBERCRIME TRAININGS CONDUCTED

- **FIRST RESPONDERS FOR CYBERCRIME - TRAINING OF TRAINERS**
 - Initiated by the DOJ-OOC in partnership with the COE-EU GLACY Project
 - The objective of the course is to establish a cadre of trainers in cyber incident response who will be able to cascade and instruct their colleagues on the proper approach to a crime scene containing electronic evidence and to process such in ways that will preserve its integrity and value.
 - The DOJ-OOC has trained **120** law enforcers as of **April 2017**.

CYBERCRIME TRAININGS CONDUCTED

- **BASIC AND ADVANCED DIGITAL FORENSICS**

- Initiated by the DOJ-OOC

- This particular training underscored the need to have a basic level understanding of digital forensics, which should be an essential knowledge area for all law enforcement officers.

- **32** investigators, **10** prosecutors, **4** state counsels, and **10** public attorneys finished the Basic Course as of **June 2016**.

- **20** investigators accomplished the Advanced Course in **June 2016**.

CYBERCRIME TRAININGS CONDUCTED

- **BASIC ELECTRONIC EVIDENCE RECOVERY (BEER) TRAINING**
 - Initiated by the DOJ-OOC
 - Patterned after US Anti-Terrorism Assistance Program's (USATA) Introduction to Digital Forensics Investigation (IDFI).
 - Designed to orient the participants with the basics of digital forensics in line with domestic laws and international best practices.
 - A total of **45** investigators, prosecutors, and public attorneys attended this training in February 2017.

CYBERCRIME TRAININGS CONDUCTED

- **Open Source Intelligence Gathering Training (OSIGT)**
 - Initiated by the DOJ-OOC
 - The training underscores the importance of developing techniques in gathering intelligence online, as well as understanding various open source tools in aid of investigation.
 - **35** agents were trained in **May 2017**.

CYBERCRIME TRAININGS CONDUCTED

- **BASIC JUDICIAL TRAINING ON CYBERCRIME**
 - Joint project of DOJ-OOC, COE-EU GLACY, and Philippine Judicial Academy
 - This particular training's objective is to train judges on how to appreciate electronic evidence presented before their respective courts, as well as to give clarity to the tenor of the laws affecting ICTs, so that they can be enlightened in applying these laws when resolving cases.
 - The DOJ-OOC has trained **90** judges through this Basic Course as of **June 2016**.

CYBERCRIME TRAININGS CONDUCTED

- **ADVANCED JUDICIAL TRAINING ON CYBERCRIME**

- Joint project of DOJ-OOC, COE-EU GLACY, and Philippine Judicial Academy
- This training is intended to reinforce the knowledge previously gained and to provide a greater insight into the challenges and methodologies involved in developing air-tight cases involving cybercrime and/or electronic evidence.
- The DOJ-OOC has trained **20** judges through this Advanced Course as of **June 2016**.

The background is a dark blue-grey color. In the four corners, there are decorative white line-art patterns resembling circuit boards or neural networks. These patterns consist of thin lines that branch out and terminate in small circles, creating a sense of connectivity and technology.

THANK YOU!

PHILIPPINE DELEGATION

State Counsel ANGELA MARIE DE GRACIA