GLACY+

Global action on Cybercrime Extended

Action Globale sur la Cybercriminalité Elargie

Version 10 March 2017

Act 2.2.2/ 2.2.3/ 2.2.4

Development of cybercrime investigations, digital forensics capabilities

combined with

National workshop and advice on interagency cooperation and public private collaboration to fight cybercrime

14-17 March 2017, Colombo, SRI LANKA

Provided under GLACY+ project

Outline

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Background and justification

As the use of and reliance on information technology becomes more and more pervasive in society, the targeting and exploitation of computer systems has also become increasingly common. Offences involving computers have grown rapidly both in number and in sophistication, and criminal justice authorities are called to face an ever increasing number of challenges in order to ensure efficient investigation and successful prosecution of related crimes. Many countries have undertaken efforts in recent years to establish specialized cybercrime units at the level of police authorities, as well as units responsible for digital forensics.

However, the initial assessments conducted under the GLACY+ Project have demonstrated that the organisational set up and functions of such units keep evolving and are not always based on international good practice. Further, interagency cooperation between specialised cybercrime units and other services, as well as collaboration between criminal justice authorities and private sector entities, such as Internet service providers and/or financial services, remain a challenge.

Building on the recommendations given in the Initial Assessment Report, this GLACY+ initiative will address these issues through offering advice and consultation about management and development of cybercrime investigation unit as well as digital forensic capabilities and through facilitating a workshop on interagency cooperation and public-private cooperation.

In the case of Sri Lanka, it was assessed that cybercrime related to the use of social media takes a large part of Sri Lankan Police workload, so training on open source investigation using search engine and social media will be provided. In addition, approach to a comprehensive digital forensic training was deemed essential for frontline investigators and will be also included in this activity.

Expected outcome

The mission will be carried out by INTERPOL, in its capacity of GLACY+ implementing partner, under Objective 2, Result 2 of the GLACY+ project, *Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries*.

It consists of two activities: a three-day advisory mission on development of cybercrime investigations and digital forensics capabilities, and a one-day workshop on interagency cooperation and public-private collaboration.

Building on preliminary results obtained during the initial assessment of Sri Lanka, the activities are expected to inform the cybercrime units' sustainable and constant development, by:

- Providing advice and guidelines on collection, analysis and handling of cybercrime statistics, on the implementation of standard operating procedure and on the development strategy.
- Training on open source investigation using search engine and social media, in consideration that social media related cybercrime takes big part of workload.
- Training first responders and frontline investigator to respond to increasing number of digital evidence to be collected and preserved
- Discussing collaboration issues, by bringing together cybercrime related governmental agency and private sector entities, on the occasion of the Workshop.

Participants

Participation is envisaged of up to 30 representatives of Law Enforcement agencies and other public agencies relevant to the topics described, involved on the basis of competencies and responsibilities required in the agenda below.

Recommended participants will therefore include:

- Representatives from cybercrime units from Sri Lanka Police.
- Frontline investigators working in cybercrime investigation division.
- Criminal investigators who seize or deal with digital evidence at field.
- Digital forensic examiner.
- Manager level officers who are in charge of policy and strategy making
- Responsible for law enforcement training.
- Staff who manage cooperation with private sectors.
- National CERT/ CSIRT

Administrative arrangements and location

The workshop will take place at the Sri Lanka Police in Colombo, Sri Lanka.

Two representatives from INTERPOL and one senior staff of C-PROC will constitute the visiting delegation.

Programme

Tuesday, 14 March 2017

9h00	**Opening event** – Sri Lankan Authorities – Sri Lanka Police – EU Delegation to Sri Lanka and the Maldives (TBC) – INTERPOL – Council of Europe
9h30	**Assessment of Cybercrime Investigation Units – Current procedures and potential issues** – Remarks from the Initial Assessment Report o Human Resources, Policies and strategies, Facility, other aspects – Interview with decision makers
11h00	Coffee break
11h15	**Assessment of Cybercrime Investigation Units – Current procedures and potential issues** - Interview with frontline investigators
13h00	Lunch break
14h00	**Advice and consultation**
15h30	Coffee break
15h45	**Advice and consultation** **Wrap-up and conclusions on Cybercrime Investigation Units**
17h00	End of day 1

Wednesday, 15 March 2017

9h00	**Assessment of Digital Forensics Capabilities** – Remarks from the Initial Assessment Report – Visit to the Digital Forensics Lab(s)
11h00	Coffee break
11h15	**Assessment of Digital Forensics Capabilities** – Visit to the Digital Forensics Lab(s) – Current capabilities, Tools used, Training received, Staff
13h00	Lunch break
14h00	**Advice and consultation**
15h30	Coffee break
15h45	**Advice and consultation** **Wrap-up and conclusions on Digital Forensics Capabilities**
17h00	End of day 2

Thursday, 16 March 2017

9h00	**Open Source Investigation** – Online tools, search engines, social media
11h30	Coffee break
11h45	**First Responder and Frontline investigator Training in Digital Forensic** – Introduction, First Responders – Handling electronic evidence in the lab
13h00	Lunch break
14h00	**First Responder and Frontline investigator Training in Digital Forensic** - Imaging - Mobile forensic extraction
15h30	Coffee break
15h45	**First Responder and Frontline investigator Training in Digital Forensic** - Understanding mobile apps
17h00	End of day 2

Friday, 17 March 2017

9h00	**Workshop on Interagency cooperation and Public-Private Cooperation on cybercrime** – Report from the assessments of Cybercrime Investigation Units and Digital Forensic Capabilities on aspects related to interagency cooperation and collaboration with private entities
11h00	Coffee break
11h15	- **The role of the national CERT** - **The role of the private sector – Telcos and Financial sector**
13h00	Lunch break
14h00	**Wrap-up and Recommendations**
15h00	End of day 2

Contacts

At the Council of Europe:

Matteo LUCCHETTI
Project Manager
Cybercrime Programme Office of the Council of Europe (C-PROC)
Bucharest, Romania
Tel: +40 21 201 78 30
matteo.lucchetti@coe.int

At INTERPOL:

Sungjin HONG
Digital Crime Officer
Cybercrime Directorate
INTERPOL Global Complex for Innovation
Singapore
Tel +65 6550 3513
s.hong@interpol.int

In Sri Lanka:

ASP Dharshika RANASINGHE
Police Department CID
Colombo, Sri Lanka
dharshikaranasinghe@hotmail.com