GLACY+
Global Action on Cybercrime Extended

WEBINAR

The establishment and functioning of specialised cybercrime units

29 April 2020, Bucharest

Speakers:

- **Virgil SPIRIDON**
Head of Operations
C-PROC, Council of Europe
- **Daniel CUCIURIANU**
Head of Bucharest Cybercrime Unit, Romanian National Police
- **Gustav Herbert YANKSON**
Head of the Cybercrime Unit, Ghana National Police
- **Dong Uk KIM**
Specialised Officer, GLACY+ project, Cybercrime Directorate, INTERPOL

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

OBJECTIVE and EXPECTED RESULTS

The process for the establishment and functioning of specialised cybercrime units at the Police Service

Participants will learn about:

- the role of a Cybercrime Unit, its competences, personnel selection, training and equipment requirements, cooperation strategies (public-private, international), investigation tools and procedures, reporting system
- the value of the support and role of specialised cybercrime units for the investigations of other crime areas
- share experience on current challenges and perspective solutions, also in the light of the outbreak of cyber threats related to the global COVID19 crisis

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

AGENDA

- Specialised cybercrime units part of cybercrime strategy
- Steps towards the creation
- Internal organization
- Responsibilities
- Models
- COE resources

Specialised cybercrime units part of cybercrime strategy

- Ensure an effective LE response to offences against and by means of computers and to any offences involving electronic evidence
- Engage in inter-agency cooperation
- Contribute to the development of the legislation, policies and strategies
- Conduct prevention and awareness campaigns
- Enhance international cooperation

Steps towards the creation

- Assessment of the current cybercrime situation
- Management decision
- Legal framework and responsibilities
- Competences
- Location

Internal organization

- Based on the organization culture
- Skills of the managers
- Independence of the unit
- Specialised sections
- Financial resources
- Staff and equipment
- Visibility of the Unit
- Action plan and evaluation mechanism

Responsibilities

- Establish the strategies/policies/evaluations
- Reporting mechanism/statistics
- Coordination and providing assistance to the field offices
- Develop the internal standard procedures
- Conduct investigations/forensic/undercover/intelligence
- Specialised support to other non cybercrime police units
- Establish the national training program
- Coordination of the inter-agency cooperation
- Coordination of the public-private partnership
- Coordination of the international cooperation

Models

- “Cybercrime units” - investigating all types of cybercrime committed and have computer forensic functions
- “High tech crime units” - investigating offences against computers and include computer forensic functions
- “Computer forensic units” - collecting and analysing electronic evidence
- “Central units” - coordination, strategic and intelligence functions
- Crime-specific units
- Cyber patrols/OSINT
- Specialised prosecution units

COE useful resources

- CyberCrime @ IPA/ Global Project on Cybercrime/ EU Cybercrime Task Force, Specialised cybercrime units - Good practice study, November 2011
- Council of Europe/Economic Crime Division, The functioning of 24/7 points of contact for cybercrime (discussion paper prepared by the Project on Cybercrime)
- GLACY Project, Reports on cybercrime reporting systems
- Council of Europe, Cybercrime strategies (Updated version)
- Council of Europe, Electronic Evidence Guide
- Council of Europe, Digital Forensic Lab Guide
- Standard Operating Procedures