GLACY+

Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Establishment and functioning of specialised cybercrime units

Date and hour	**29/04/2020** 12h00 (Eastern European Summer Time: GMT +3 hours)
Speakers	Virgil SPIRIDON, Head of Operations, Cybercrime Programme Office, Directorate General of Human Rights and Rule of Law, Council of Europe Daniel CUCIURIANU, Head of Cybercrime Unit, Bucharest Brigade for Countering Organised Criminality, Romanian National Police Gustav Herbert YANKSON, Head of the Cybercrime Unit, Ghana National Police Dong Uk KIM, Specialised Officer, GLACY+ project, Cybercrime Directorate, INTERPOL
Objectives	The webinar will focus on processes for the establishment and functioning of specialised cybercrime units at the Police Service, the required capacities and responsibilities, the procedures and best practices for conducting investigations, including the need for inter-agency cooperation and police-to-police international cooperation. The session will provide general recommendations regarding the development and consolidation of existing units, in line with the international standards provided by the Budapest Convention. The experience of the Romanian Police, the Ghana Police and INTERPOL will complement with practical example of the setup of specialised units on cybercrime and case studies to emphasise the support provided for the investigation of other crime areas. During the webinar, participants will be encouraged to share insights about current issues and experiences, also in the light of the outbreak of cyber threats related to the COVID19 global crisis.
Expected outcomes	• Acquire knowledge on 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.

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

	• Learn about the value of the support and role of specialised cybercrime units for the investigations of other crime areas. • Engage in discussions with peer-participants and share experience on current challenges and perspective solutions, also in the light of the outbreak of cyber threats related to the global COVID19 crisis.
Background	With societies relying more than ever on the use of information and communication technologies, and with the parallel increase of crimes committed through the use of them, the work of Police Services worldwide has shifted more and more consistently to the on-line world. The challenges posed by cybercrime are to be addressed through specialized units, equipped with adequate legal and technical tools. The current outbreak of the COVID 19 pandemic and the related increase of cyber threats related to it, offer an example of how cyber criminals are continuously trying to adapt their illegal activities and benefit even from a global crisis. Several examples in this regard have been reported, such as: • Phishing campaigns and malware distribution through seemingly genuine websites or documents providing information or advice on COVID-19 are used to infect computers and extract user credentials. • Ransomware shutting down medical, scientific or other health-related facilities where individuals are tested for COVID-19 or where vaccines are being developed in order to extort ransom. • Attacks against critical infrastructures or international organizations, such as World Health Organization. • Ransomware targeting mobile phones through apps claiming to provide genuine information on COVID-19 in order to extract payments. • Offenders obtaining access to the systems of companies or other organisations by targeting employees who are teleworking. • Fraud schemes where people are tricked into purchasing goods such as masks, hand sanitizers, but also fake medicines claiming to prevent or cure SARS-CoV-2. • Misinformation or fake news are spread by trolls and fake media accounts to create panic, social instability and distrust in governments or in measures taken by their health authorities In this context, specialized cybercrime units play a major role for investigating cyber threats, enforcing relevant laws and securing criminals to justice, thus maintaining public safety and order. It is therefore essential that efficient organizational models and consistent procedures are put in place, so as to also expedite cross-country cooperation with foreign criminal justice authorities and service providers.
Expected duration	1h30 (45’ presentations + 45’ discussion)

Participants	Up to 50 participants are expected. Participation in this seminar is restricted to Law Enforcement officers only. Each registered participant will receive a confirmation email one day prior to the webinar with instructions on how to connect and rules of engagement.
Relevant resources	Council of Europe, Specialised Cybercrime Units – Good Practice Study Council of Europe, The functioning of 24/7 points of contact for cybercrime Council of Europe, Report on Cybercrime Reporting Systems Council of Europe, Cybercrime Strategies Cybercrime strategies (Updated version)
C-PROC related activities	The webinar is carried out under Result 2.2 "Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries" and in particular under Activity 2.2.2 "Advice on the setting up and development of cybercrime and computer forensic units (structure, ISO standards, international good practice) with reference to the gap areas identified in assessments in priority countries". This activity is supported also by CyberSouth project, under the Result 2 "Specialised police services and interagency as well public/private cooperation strengthened through a sustainable approach", activity 2.3.

www.coe.int/cybercrime