ROUND TABLE-Cybercrime threats

Virgil SPIRIDON
Head of Operations
C-PROC, Council of Europe

Bucharest, 2 October 2019

www.coe.int/cybercrime

Aim of the round table

- To discuss challenges of cybercrime and online child exploitations
- To identify new synergies with public and private partners
- To introduce the work of the Council of Europe – Cybercrime Programme Office

Partners

- General Inspectorate of Romanian Police (Cybercrime Unit)
- The Romanian National Computer Security Incident Response Team (CERT-RO)
- Bitdefender
- UNICEF Romania
- Save the Children Romania

Introduction

- **Cybercrime Programme Office (C-PROC)**
- **Cybercrime capacity building projects**
- **Cybercrime challenges**
- **Cybercrime and e-evidence as transversal challenges**

Cybercrime Programme Office (C-PROC)

- Committee of Ministers decision October 2013
- Operational as from April 2014
- Currently 30 staff
- Location: Bucharest, Romania
- Volume of projects: ca. 30 million EUR

- **Task: Support countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence**

Cybercrime Programme Office (C-PROC)

- Specialised Office of the Council of Europe to respond to the growing need for capacity-building on cybercrime worldwide in a visible and credible manner.
- Capacity-building activities b… …he intergovernmental activities of the Cybercrime … …CY), which is managed from Strasbourg.
- The Office is funded by extra…
- Identify needs for capacity-b… …crime.
- Advice, support and co-ordi… …tion and timely implementation of targeted … on cybercrime, including joint programmes with the European Union and other donors.
- Ensure the cooperation with the authorities of Romania in matters regarding cybercrime.

737 activities involving more than 150 countries since 2014

117 activities supported in first Semester 2019

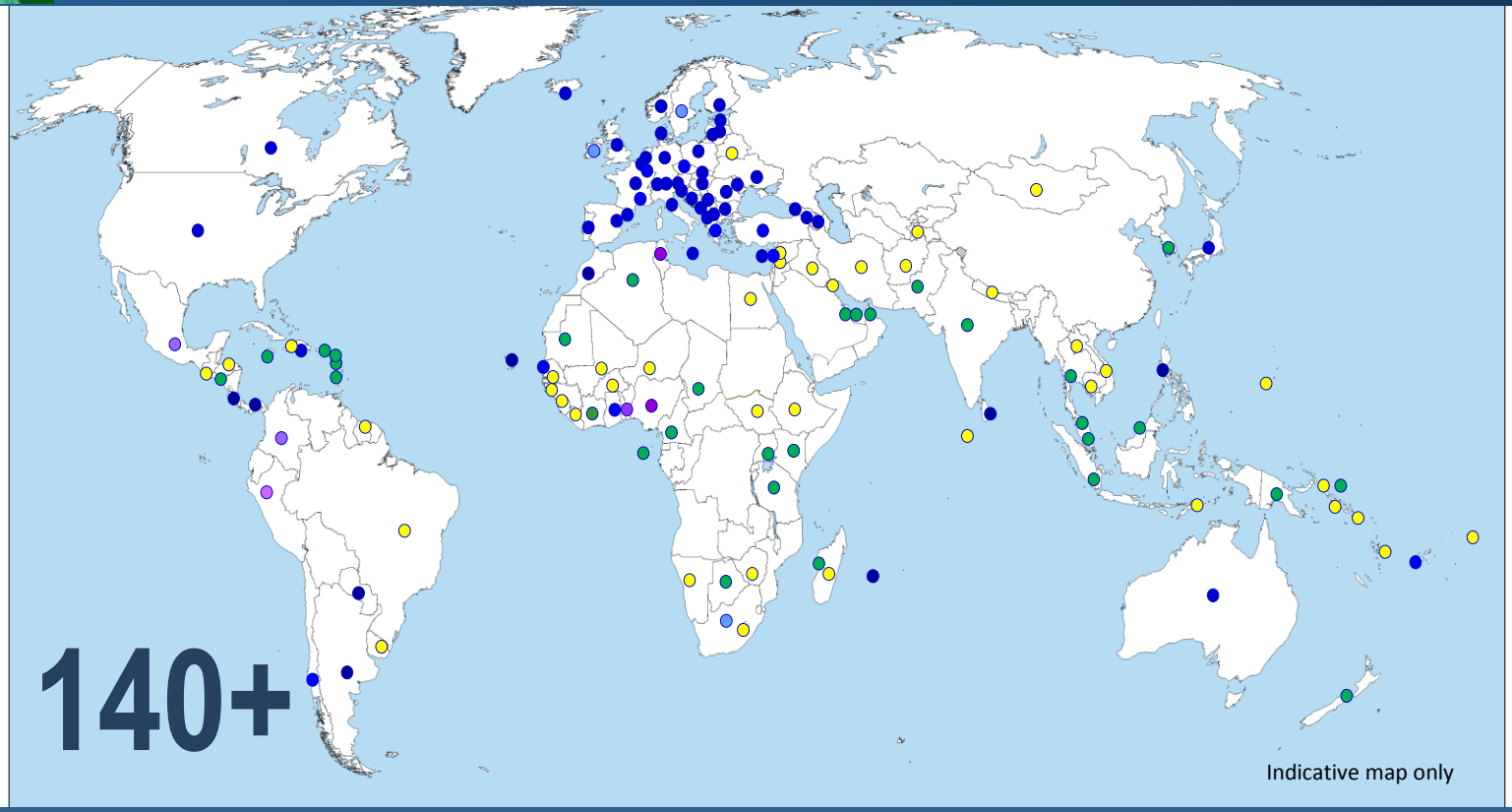
Cooperation on Cybercrime: The approach of the Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

REACH of the Budapest Convention



Ratified/acceded: 64

Signed: 3

Invited to accede: 6

= 73

Other States with laws/draft laws largely in line with Budapest Convention = 20+

Further States drawing on Budapest Convention for legislation = 50+

Keeping the Budapest Convention up to date

- Protocol on Xenophobia and Racisms via Computer Systems (31 Parties + 13 Signatories)

- Guidance Notes on
  - Notion of computer systems
  - Botnets
  - Malware
  - Spam
  - Terrorism
  - Transborder access to data (Article 32)
  - Production Orders for Subscriber Information (Article 18)
  - Election interference

- Protocol on enhanced international cooperation under negotiation

= Budapest Convention remains up-to-date and relevant

Current cybercrime capacity building projects

Cybercrime@Octopus (voluntary contribution funded)

CyberEast EU/COE Eastern Partnership region

iPROCEEDS EU/COE IPA region

GLACY+ EU/COE Joint Project on Global Action on Cybercrime

CyberSouth EU/COE MENA region

EndOCSEA IPA and EAP regions

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

Current cybercrime capacity building projects

Multiple objectives:

- Legislation and policies
- Specialised units (LE and prosecution)
- Training of LE representatives and magistrates
- Inter-agency cooperation
- Public/private cooperation
- Targeting proceeds from crime online
- International cooperation

- Priority to countries committed to implement Budapest Convention
- Support to any country regarding legislation

Towards a Protocol: Issues to be addressed

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Main challenges on cybercrime and e-evidence

- **New technological developments (**Encryption, TOR, Crypto-currency, VoIP, etc)
- **Limited resources for LE authorities**
- **Volatility of data**
- **Increasingly need of e-evidence from abroad and the cloud**
- **Jurisdiction** (territoriality of investigative powers versus data and services in the cloud)
- **Instruments and channels for international cooperation (**public authorities and private sector)

Cybercrime and electronic evidence: Transversal challenges

- **Definition of cybercrime** (crimes against computer systems and data and by means of computer systems)
- **Online child exploitation** (recruitment, images, abuses, financial and technical instruments)
- **Terrorism** (communication, propaganda, attacks, critical infrastructure, finance activities)
- **Drug trafficking** (communication, online selling, payment instrument)
- **Human beings trafficking** (recruitment, communication, payment instruments)

Cybercrime and electronic evidence: Transversal challenges

- **Electronic evidence in relation to ANY type of crime** (categories of data, exchange, international cooperation)
- **On-line financial investigations** (nature of cybercrime, payment instruments, money flow on the Internet)
- **Data protection** (conditions and safeguards)
- **Cybersecurity** (strategy, critical infrastructure, security measures, offences, cooperation LE and CERT)

Mapping study on cyberviolence -9 July 2018

- focuses on children and women
- computers used to create or facilitate violence
- agreed on the concept of cyber violence
- mapping acts that constitute cyberviolence and drawing conclusions as to typologies and concepts
- providing examples of national experiences and responses to such acts (including policies, strategies, legislation, cases and case law);
- discussing international responses under the Budapest Convention and other treaties (in particular the Istanbul and Lanzarote Conventions of the Council of Europe)
- developing recommendations as to the further course of action

Virgil.spiridon@coe.int

www.coe.int/cybercrime