Council of Europe
Cybercrime Programme Office (C-PROC)

# CYBERCRIME –challenges and transversal issues

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

Bucharest, 4 June 2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

# 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: CONTEXT

## Cybercrime and e-evidence: increasing and transversal challenges that affect human rights, democracy and the rule of law:

- **Scale and complexity versus criminal justice capacities and resources**
- **How to reconcile security and fundamental rights**
- **Preference to criminal justice approach but ….**

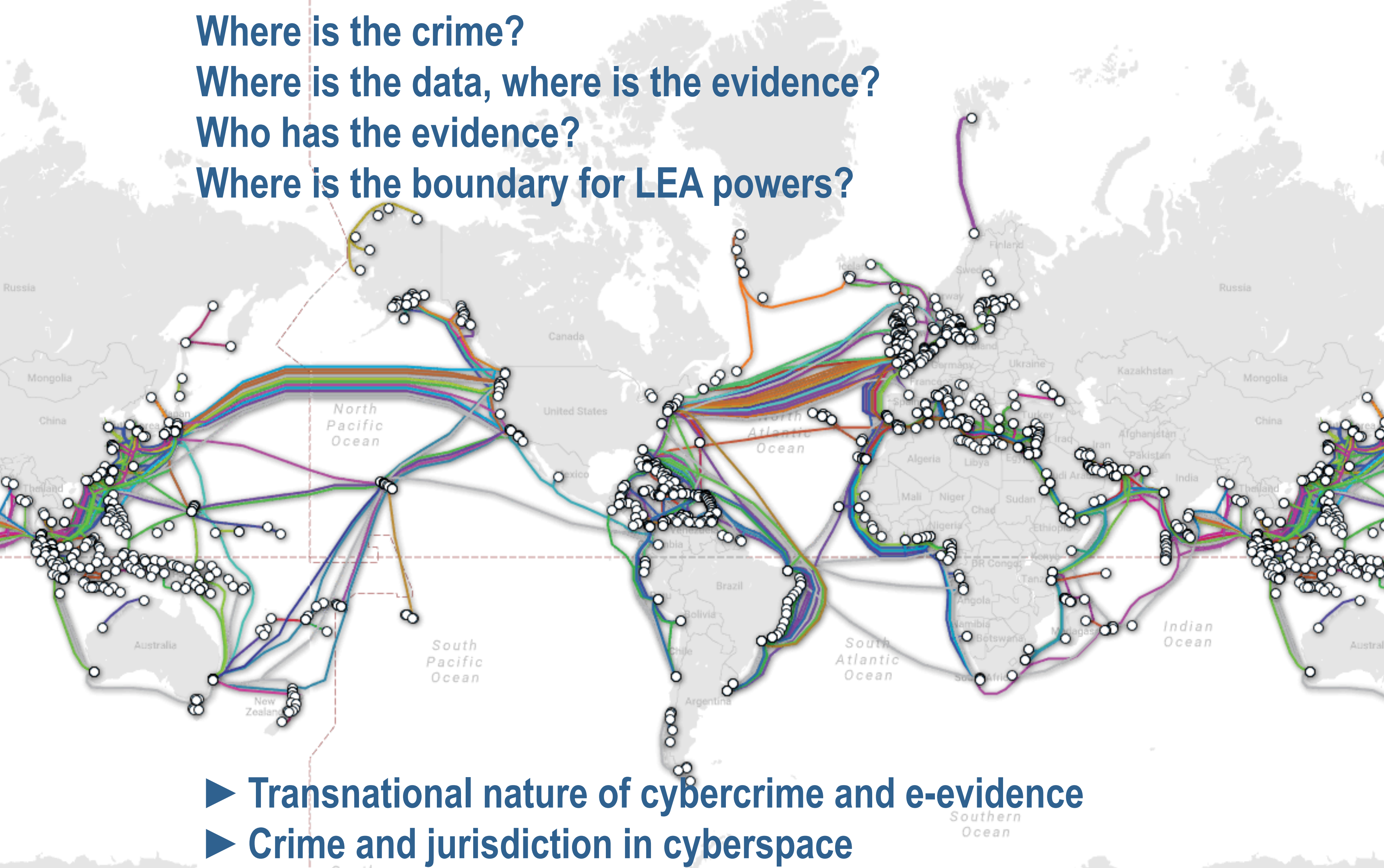
## Council of Europe response:

- **Budapest Convention and Protocol XR**
- **Capacity building (C-PROC)**
- **T-CY work on Protocol**

## Considerations:

- **Political fragmentation and diverging interests in cyberspace**
- **EU e-evidence proposals**
- **Developments at UN**

# Example: Crime and evidence in the cloud



Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?

- ► Transnational nature of cybercrime and e-evidence
- ► Crime and jurisdiction in cyberspace

# Cybercrime and electronic evidence: challenges

## Cybercrime and e-evidence are transversal challenges that affect human rights, democracy and the rule of law

- Ransomware (WannaCry, NotPetya)
- DDOS
- Critical information infrastructure attacks
- Election interference
- Data breaches
- Cyberviolence
- Child sexual abuse materials
- Fraud
- Cryptocurrencies (means and targets of crime)
- Darkmarkets
- Social engineering
- Etc.

**Issues:**

- Technology (Static vs dynamic IP addresses, encryption, VPN, NATs, IoT etc.)
- Criminals or Governments?
- Cybercrime or cyberwarfare?
- Criminal justice or national security / defence?
- Security or fundamental rights?
- Data protection or crime prevention and criminal justice?
- Territoriality of criminal justice versus crime and evidence in the cloud?

# 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)
- **Elections** (role of social media in the election campaigns, attacks on the electronic vote systems)
- **Hate speech** (criminalised or not)

Virgil.spiridon@coe.int

**www.coe.int/cybercrime**