The international legal framework on Cybercrime and Electronic Evidence
The Budapest Convention
And
Capacity building programmes

Manuel DE ALMEIDA PEREIRA

Project Manager at the Cybercrime Programme Office
of the Council of Europe (C-PROC) in Bucharest, Romania
manuel.pereira@coe.int

Santo Domingo, Dominican Republic, 12-14 June 2019

OUTLINE

1. Origins
2. Definitions; narrow and broad sense
3. Challenges
4. The Budapest Convention; scope and accession process; benefits of the Budapest Convention
5. Approach of the CoE and the T-CY
6. The C-PROC and capacity building projects: The GLACY+ Project
7. Budapest Convention in the Asia-Pacific region

The origins of the "cyber" space

- **Cybernetics** – Pioneered in the late 1940s by a group of specialists in fields ranging from biology to engineering to social sciences, cybernetics was concerned with the **study of communication and control systems in living beings and machines**. The term cybernetic comes from the Greek word kubernētēs (κυβερνᾶν), 'steersman', from kubernan 'to steer'.
- **Cyberspace** – The term cyberspace only appeared in 1982, apparently coined by William Gibson in his science fiction novella 'Burning Chrome', and later in a novel called "Neuromancer". In the latter it was defined as "*A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.*"
- According to Oxford English Dictionary, **cyberspace is 'the space of virtual reality; the notional environment within which electronic communication (esp. via the Internet) occurs'**.
- Almost three decades later, is was not yet defined, in legal texts or legal studies the **real concept of cybercrime**

Famous sentences

"There will never be a market for more than 5 computers in the world".

Thomas Watson - Chairman of IBM - 1943

"There will never be a reason anyone would want a computer in their home".

Ken Olson, Founder of DEC - 1977

"A PC will never need more than 640K of memory".

Bill Gates - Founder of Microsoft - 1981

Cybercrime: Narrow and Broader Sense

- Normally used to describe a criminal activity in which a computer or a network are an essential part of a crime
- However cybercrime is also used to include other traditional crimes in which those same computers or networks are used to make the illicit activity possible

THE COMPUTER IS A TOOL OF THE CRIMINAL ACTIVITY e.g. Spamming, criminal copyright crimes through peer-to-peer networks, etc.
THE COMPUTER OR THE NETWORK IS A TARGET OF CRIME e.g. Unauthorized access, Malicious code, Mobile malware, ATM/POS malware, etc.
THE COMPUTER OR THE NETWORK MAKE COMMISSION OF CRIMES EASIER e.g. Nigerian fraud, Hacking, Phishing, Child Pornography, Drug smuggling
THE COMPUTER OR THE NETWORK IS THE PLACE OF THE CRIMINAL ACTIVITY e.g. Telecommunications' fraud

What is cybercrime

- Traditional crimes committed in the digital environment
  - specifically, the criminal act can just be committed within the digital environment
  - the crime cannot exist outside the virtual world and is generated inside it
    - computer fraud
    - computer forgery

What is cybercrime

- Crimes committed by the means of a computer system
  - cannot be distinguished from the same type of crime committed by other ways
  - no specificity
    - defamation committed by an electronic newspaper
    - threat committed by email
    - money laundering in a virtual bank, in the Internet

What is cybercrime

- Crimes against the computer environment
  - data interference
  - system interference
  - illegal access.

Cybercrime as a criminal justice matter – Main Challenges

- **Lack of common understanding** on cybercrime amongst the criminal justice authorities

- Cybercrime legislation in place only in a few countries, **heterogeneous legislative framework**
  - Definition of cybercrimes
  - **Dual criminality**

- Coping with **new technological paradigms**
  - Cloud Computing
  - Darknet and virtual currencies
  - Internet of Things

- **Reliable statistics** not fully available
  - Reported, Investigated, Prosecuted, Adjudicated Cases
  - Number and types of electronic evidences extracted, Devices analyzed

Cybercrime as a criminal justice matter – Main Challenges

- Cybercrime investigation units are usually understaffed and not **adequately trained/ skilled**
  - Use of VPN/ Tunneling and Proxy/ Use of darknets and virtual currencies
  - Understanding of the Modus Operandi/ Evidence to collect
  - Investigation into possible forms of Organized Crime vs. Single criminal

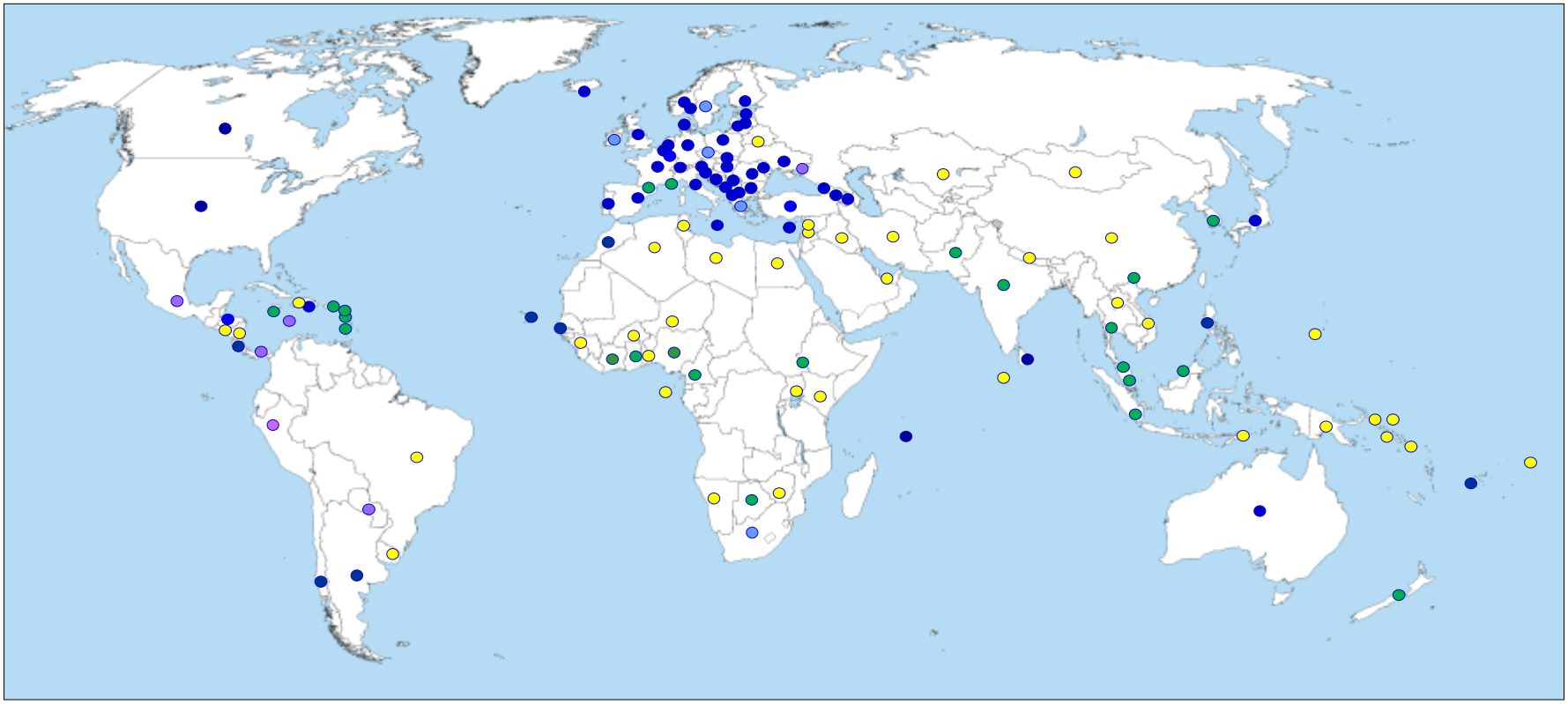
- **Limited technical capabilities** to support a successful investigation
  - Data/ mobile forensics laboratories outdated
  - Malware forensics and reverse engineering capacities
  - Collaboration with local telecommunication service providers

- **International cooperation**
  - Police to Police
  - International Judicial Cooperation
  - Interactions with international large service providers (Social Networks, etc.)

Council of Europe's Convention on Cybercrime – The Budapest Convention

- Opened for signature November 2001 in Budapest
- Followed by Cybercrime Convention Committee (T-CY)
- Open for accession by any State
- As of today, the only **binding international Treaty on cybercrime and electronic evidence**
- It gives high-level, technology-neutral definitions of cybercrime offences
- It sets standard procedures for investigation and prosecution on the national level, and puts relevant obligations on involved parties
- It defines procedural provisions for international cooperation, police-to-police and judicial
- Guidance notes are published by T-CY to interpret BC provisions in the light of new threats and new technological paradigms

Reach of the Budapest Convention



Budapest Convention
Ratified/acceded: 63

Signed: 3

Invited to accede: 4
= 70

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

Further States drawing on Budapest Convention for legislation = 45+

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Production order
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Production order
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Production order
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Acceding to the Budapest Convention

Treaty open for accession by any State (article 37)

Phase 1:

- If a country has legislation in place: Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit the instrument of accession at the Council of Europe

- Acceded: Australia, Chile, Dominican Republic, Mauritius, Panama, Senegal, Tonga, Costa Rica, Israel, Morocco and Philippines
- Invited: Argentina, Colombia and Mexico

Acceding to the Budapest Convention

- As a minimum the instrument for accession must include the **competent authorities for extradition** (Article 24), **MLA** (Article 27) and **24/7 POC** (Article 35).

- **Reservations and declarations** can be made according to the domestic legislation.

- For a reference on what other Parties did:

http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=Du8xp12S

- Once the internal procedures have been completed and all the signatures and approvals have been obtained, the accession instrument could be mailed to the Council of Europe or an authorized person (someone coming from the applying Country or the Ambassador in Paris) could go to Strasbourg and hand it over to the Secretary General.

Acceding to the Budapest Convention

Letter requesting accession should be sent to:

Mr. Alexander SEGER
Executive Secretary to the Budapest Convention
Head of Cybercrime Division
Strasbourg - France
alexander.seger@coe.int

Copy to:

Manuel ALMEIDA PEREIRA
Project Manager of GLACY+
Cybercrime Programme Office (C-PROC)
Bucharest - Romania
manuel.Pereira@coe.int

The accession process

1. **Expression of interest**
2. **Analysis of the legislation and of the context**
3. **Advisory mission on cybercrime legislation**
4. **Legislation in line with the provisions of the Budapest Convention**
5. **Request to join the BC, formalized by the Government and sent to the Council of Europe**
6. **Analysis of the request from the Treaty Office and decision from the Cybercrime Convention Committee**
7. **Invitation for the Country to join the BC**
8. **Ratification and instruments of accession deposited in Strasbourg**

Benefits of joining Budapest

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

"Cost": Commitment to cooperate

Disadvantages?

The approach of 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

The Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership:

- **63 Members** (State Parties)
- **10 Observer States**
- **12 organisations** (**African Union Commission**, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- **Assessments of the implementation of the Convention by the Parties**
- **Guidance Notes**
- **Draft legal instruments**

Two plenaries/year as well as Bureau and working group meetings

- **An effective follow up mechanism**
- **The T-CY appears to be the main inter-governmental body on cybercrime matters internationally**

Capacity building: Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania

- **Committee of Ministers decision October 2013**
- **Operational as from April 2014**
- **Currently 30 staff**
- **Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence**