The Budapest Convention

HELP Course
on Cybercrime and Electronic Evidence

THE 2021 HELP NETWORK E- CONFERENCE
"HUMAN RIGHTS RESPONSES TO GLOBAL CHALLENGES"

Virgil Spiridon

1 July 2021

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 Budapest Convention on Cybercrime

- **Negotiated by Council of Europe** (47 members)**, Canada, Japan, South Africa and USA**
- **Opened for signature on 23 November 2001 in Budapest**
- **Protocol on Xenophobia and Racism via computer systems (2003)**
- **Followed by Cybercrime Convention Committee (T-CY)** – Guidance Notes, Interpretation, Follow-up
- **Open for accession by any State – 66 Accessions/ Ratifications**
- **2nd Additional Protocol on enhanced cooperation an disclosure of electronic evidence**
- **As of today, the only international Treaty on cybercrime and electronic evidence**

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

- **Conditions, safeguards**

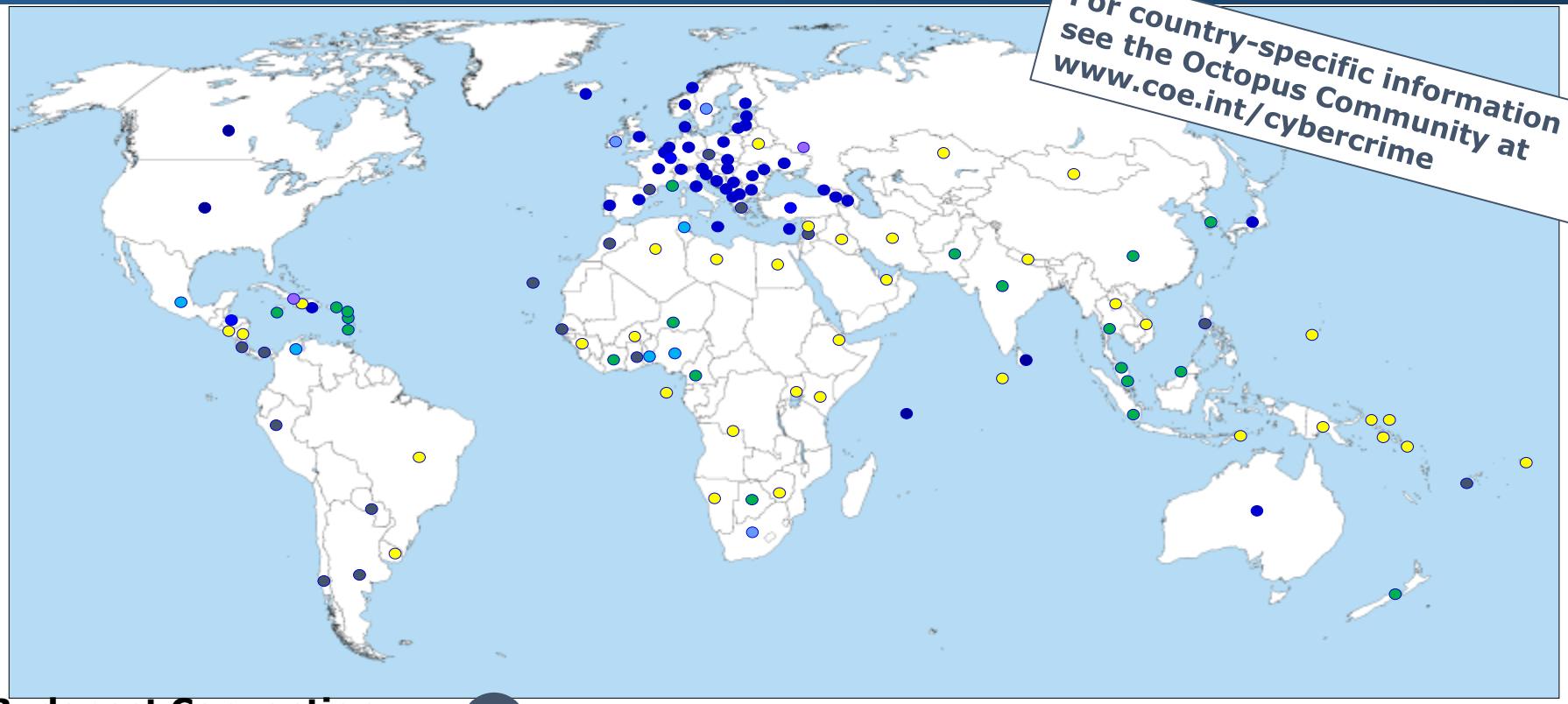
+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- Trans-border Access to Data
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Procedural powers and international cooperation for ANY CRIMINAL OFFENCE involving evidence on a computer system!

Reach of the Budapest Convention



Budapest Convention

Ratified/acceded: 66

Signed: 2

Invited to accede: 9

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

Further States drawing on Budapest Convention for legislation = 45+

HELP Course on Cybercrime

Rationale

YOU OBSERVE THAT ...

..it is a **real challenge** for the judiciary and law enforcement to strike a **fair balance** between all rights and freedoms of individuals, irrespective of whether victims or perpetrators.

"how deep a surgeon has to cut in order to heal?" - the question that has no definitive answer.

not many courses attempt to answer this question and even less address the topic of **cybercrime** and **electronic evidence and how to strike the balance with human rights**. it is time to take up the challenge and that is why you are here.

HERE WE GO !

Objectives

This course will...

...introduce you to the basic concepts related to **cybercrime** and **electronic evidence**.

In doing so, the course makes an overview of the **challenges** in **investigating** cybercrime, as well as the difficulties in **collecting and handling** of electronic evidence.

The **Budapest Convention** remains the key source throughout the whole course as the it provides tools to deal with the above challenges for the **protection of human rights** and **enforcement of legal order**.

The course is addressed to ...

legal professionals primarily, i.e. judges, prosecutors, lawyers and court staff. It could be easily followed by criminal investigators and police officers, as well as other law enforcement bodies specialized on prevention and investigation of cybercrime and related offences.

Target audience

criminal justice authorities worldwide, legal practitioners, defense attorneys, professionals for child protection, and **anyone willing to improve their knowledge on cybercrime and electronic evidence**.

Structure of the course

Module 1:	Introduction to computers, networks and cybercrime
Module 2:	Introduction to the Budapest Convention on Cybercrime
Module 3:	Substantive provisions
Module 4:	Electronic evidence and the BC procedural provisions
Module 5:	International cooperation provisions
Module 6:	Cybercrime in practice and Human Rights
Module 7:	The Second Additional Protocol to the Budapest Convention

THANK YOU!