



The framework of the Convention on Cybercrime: Update

Alexander Seger
Head of Cybercrime Division
Council of Europe

Context

- War, conflict, insecurity
- International law violations
- Human rights violations
- Injustice
- Inequality
- Economic crises
- Autocracies, democratic back-sliding
- Climate change
- Crises of truth

Crises

- Cyberattacks
- Cybercrime
- Dis-/misinformation
- Hate crime, hate speech online
- Impunity for crime online
- “Non-cooperative countries and territories”

Need

- ▶ More cooperation
- ▶ Common solutions
- ▶ More justice
- ▶ More accountability
- ▶ Strengthen human rights and rule of law
- ▶ Effective criminal justice response



Framework of the Convention on Cybercrime

- ▶ more cooperation, accountability, security, human rights and justice in cyberspace

COUNCIL OF EUROPE

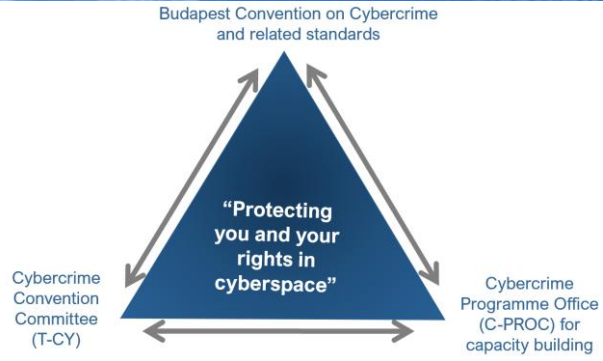


CONSEIL DE L'EUROPE



Status and formula for success

- Convention on Cybercrime
- First Protocol on XR
- Second Protocol on e-evidence



Convention on Cybercrime (2001):

1. Offences against and by means of computer systems (articles 2-12)
 - CIA offences (illegal access, data/system interference etc.), forgery and fraud, “child pornography”, IPR
2. Procedural powers to investigate cybercrime and collect e-evidence in relation to **any** offence (articles 14-21)
 - Expedited preservation, production orders, search and seizure, interception, safeguards
3. International cooperation on cybercrime **and** e-evidence
 - General provisions, expedited preservation, MLA, 24/7 network

About

First Protocol on xenophobia and racism (2003):

- Racist and xenophobic materials
- Dissemination of XR materials
- Racist and xenophobic motivated threat
- Racist and xenophobic motivated insult
- Denial, gross minimization, approval or justification of genocide or crimes against humanity

Second Protocol on enhanced cooperation and disclosure of e-evidence (2022):

- Scope: criminal investigations and proceedings related to computer systems and data and collection of e-evidence re **any** criminal offence
- Direct cooperation with service providers and registrars in other Parties
- Giving effect to production orders from other Parties
- Expedited cooperation in emergencies
- Video conferencing
- Joint investigation teams and joint investigations
- Data protection and other safeguards

T-CY Guidance Notes

- Computer system # 1
- Botnets # 2
- Transborder access (Article 32) # 3
- Identity Theft # 4
- DDOS attacks # 5
- Critical infrastructure attacks # 6
- Malware # 7
- Spam # 8
- Election interference # 9
- Production orders for subscriber information # 10
- Terrorism # 11
- Ransomware #12
- Scope of powers #13

Convention on Cybercrime: reach/membership

Convention on Cybercrime: Status 10 December 2023		
Parties	68	
Signatories	2	Ireland (signed 2002), South Africa (signed 2001)
Invited to accede	21	Most recent: Cameroon, Kazakhstan, Kiribati, Republic of Korea, Rwanda, São Tomé and Príncipe, Sierra Leone, Uruguay Note: Consider 5-year validity of invitation (Tunisia February 2024, Benin June 2024)
Total	91	

Convention on Cybercrime: reach/membership



Global state of cybercrime legislation – cursory survey (edition December 2023)

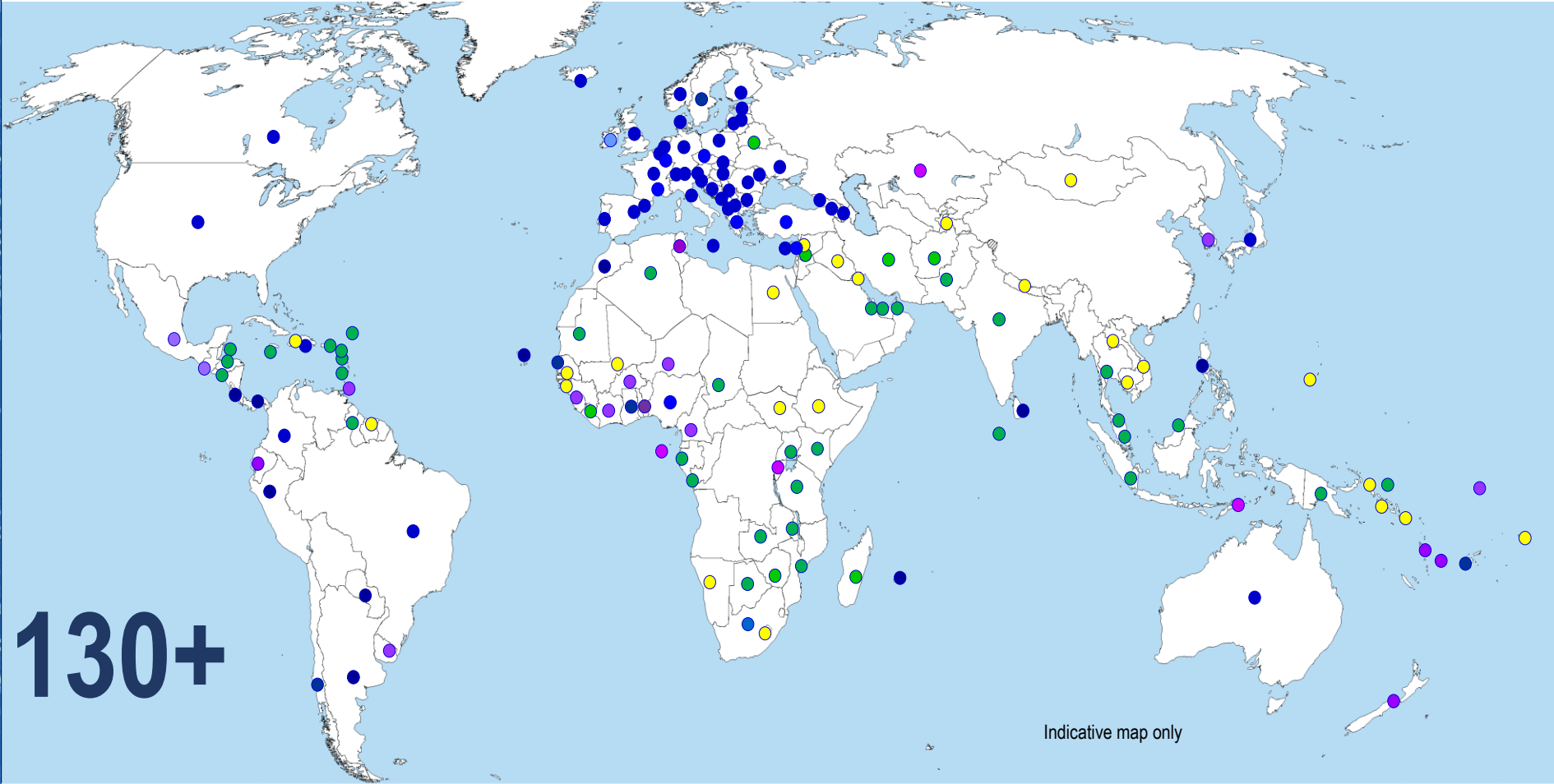
Substantive criminal law broadly aligned with
Convention on Cybercrime:

- 2013: 70 States (36%)
- 2018: 93 States (49%)
- 2023: 131 States (68%)

Parties, signatories or invited to accede:

- 2013: 57 States (30%)
- 2018: 71 States (37%)
- 2023: 91 States (47%)

Convention on Cybercrime: reach/membership



Parties:	68	■		
Signed:	2	■	Other States with substantive laws broadly in line with Budapest Convention:	40 ■
Invited to accede:	21	■	Further States drawing on Budapest Convention for legislation:	30+ ■
	= 91			= 70+

Note: Concern

Cybercrime laws increasingly used to address speech in broad and vague terms

- ▶ Prescribed by law? Clear, precise, foreseeable?
Necessary? Proportionate?

Convention on Cybercrime: reach/membership

First Protocol on Xenophobia and Racism: Status 10 December 2023

Parties	35	Most recent: Iceland (January 2023), Slovakia (June 2023)
Signatories	10	
Invited to accede	(38)	Note: all States invited to accede to the Convention may also accede to the First Protocol

Octopus Project



Implementing the First Protocol
to the
Convention on Cybercrime
on Xenophobia and Racism:
Good practice study

Strasbourg, 1 December 2023 (provisional)

Convention on Cybercrime: reach/membership

Second Protocol on electronic evidence: Status 10 December 2023

Parties	2	Serbia (February 2023), Japan (May 2023)
Signatories	41	Most recent: Armenia (November 2023), Cabo Verde, Ghana, Hungary, Malta (all in June 2023), Mauritius (May 2023)

5 ratifications needed for entry into force: ► 2024?

Why has this framework been functioning and obtained broad acceptance over 22+ years?

- Consensus principle: initiated, negotiated, managed by consensus
- Mature texts prepared and negotiated over several years
- Scope: specific criminal justice treaty
- Terms, concepts, definitions: clear, technology-neutral, timeless, specific & flexible, limited number, work in different legal systems
- Safeguards: system of human rights and rule of law conditions and safeguards
- Offences: limited number of offences, technology-neutral
- Procedural powers: broad approach (e-evidence of any offence) but specific provisions and subject to conditions and safeguards
- International cooperation: broad (e-evidence of any offence) but specific provisions and conditions, grounds for refusal, no interference with other treaties and agreements
- Keeps evolving

Lessons for UN treaty process (AHC*)

- Terms, concepts, specific provisions: ensure consistency with Budapest Convention
 - ▶ increased likelihood of agreement on UN treaty
 - ▶ consistency with 130+ States
- Narrow criminal justice treaty with limited number of offences and specific procedural powers more likely to reach agreement
- The stronger the safeguards, the broader the scope of cooperation
- Added value: an additional treaty based on UNTOC, UNCAC and Budapest Convention would permit more States to cooperate more & permit synergies with BC and other treaties

*UN Ad Hoc Committee to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes

Budapest Convention the formula for success

