

HEMISPHERIC FORUM ON INTERNATIONAL COOPERATION AGAINST CYBERCRIME
Santo Domingo, 5-7 December 2017

Strategies on cybercrime: considerations

Alexander Seger
Council of Europe
alexander.seger@coe.int

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

Prevention and control of cybercrime: why?



Cybercrime

- ▶ Security/trust/resilience/reliability of ICT
- ▶ Security of society and rights of individuals
- ▶ Human rights
- ▶ Democracy
- ▶ Rule of law

Prevention and control of cybercrime: what?

Cybercrime

- ▶ Offences against computer systems and data
- ▶ Offences by means of computer systems and data

+

Electronic evidence

- ▶ Any crime may involve evidence in electronic form on a computer system
- ▶ Needed in criminal proceedings
- ▶ No data, no evidence, no justice

= Capacity building for all criminal justice officials needed!



Cybercrime and e-evidence: why a strategy?

- ▶ **Political commitment**
- ▶ **Define objectives and targets and monitor progress**
- ▶ **Coherence**
- ▶ **Multi-stakeholder cooperation**
- ▶ **Budgets**
- ▶ **Facilitate capacity building**

Cybercrime or cybersecurity strategy?

- **Interrelated and complementary**
- **Cybercrime and e-evidence often (partially) included in cybersecurity strategies**
- **Further elaboration required**



Example Chile: National Cybersecurity Policy 2017 – 2022

Objectives by 2022:

- A. The country will have in place a robust and resilient information infrastructure, prepared to face and recover from cybersecurity incidents, under a risk management approach

- B. The State will protect people's rights in cyberspace**
 - 1. Crime prevention and trust building in cyberspace**
 - 2. Priority setting in the implementation of punishing measures (including adoption of legislation in line with Budapest Convention)**
 - 3. Multi-sectoral prevention (including capacity building)**
 - 4. Respect for and promotion of fundamental rights**

- C. Chile will develop a cybersecurity culture based on education, good practices and accountability in the management of digital technologies

- D. The country will carry out cooperation actions with other stakeholders in the field of cybersecurity and will actively participate in international forums and discussions (including Budapest Convention on Cybercrime)**

- E. The country will promote the development of a cybersecurity industry serving its strategic objectives

Cybercrime and e-evidence: Elements of a strategy

Objective

Protecting society / individuals and their rights in cyberspace



Protection against:

- **Intentional attacks against and by means of computers**
- **Any crime involving electronic evidence on a computer system**



- **Cybercrime reporting**
- **Prevention**
- **Legislation**
 - **Criminalising conduct**
 - **Law enforcement powers (with safeguards)**
- **Specialised units**
- **Interagency cooperation**
- **Law enforcement training**
- **Judicial training**
- **Public/private cooperation**
- **Effective international cooperation**
- **Financial investigations and fraud/ML/TF prevention**
- **Protection of children**

1 Budapest Convention on Cybercrime

- Criminalising conduct
- Powers for law enforcement to secure electronic evidence
- International cooperation

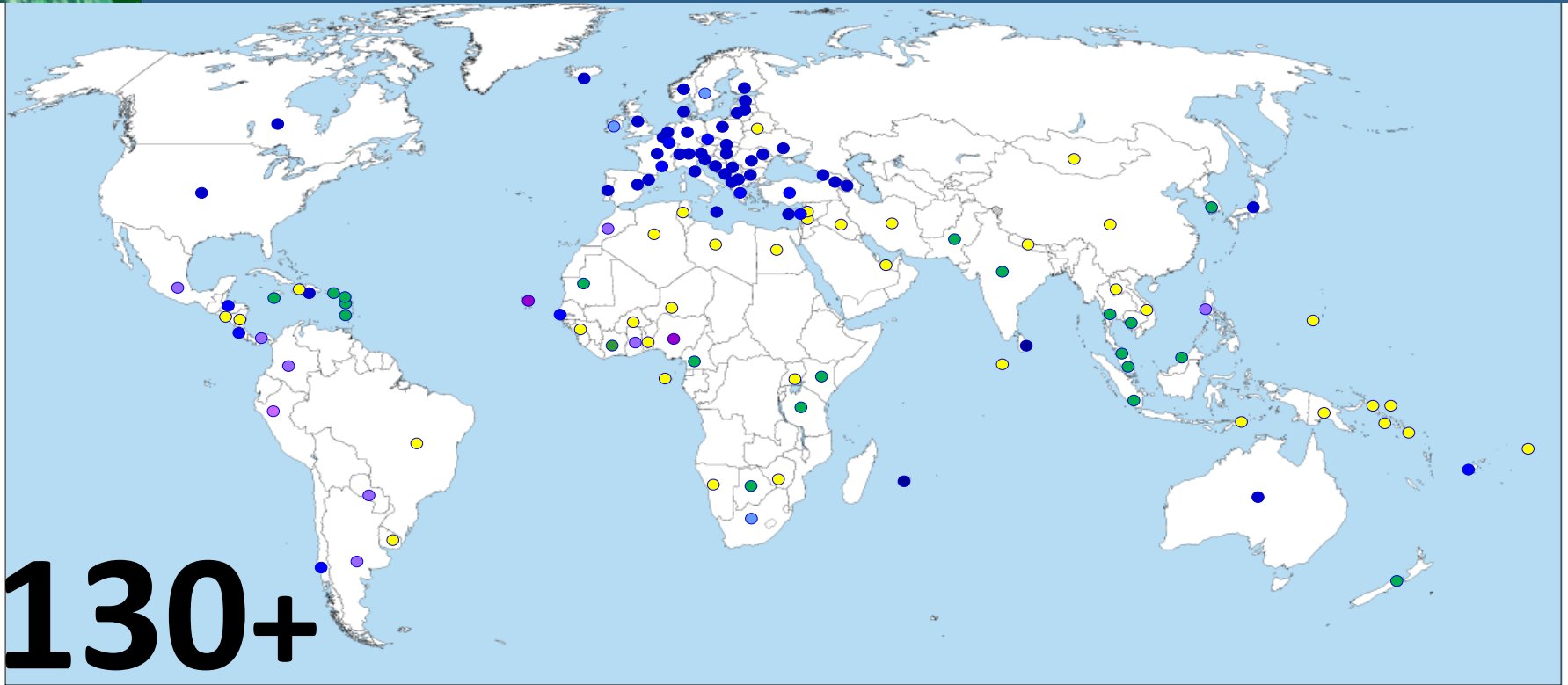
2 Cybercrime Convention Committee

- Assessing and guiding implementation
- Preparing additional solutions: access to evidence in the cloud



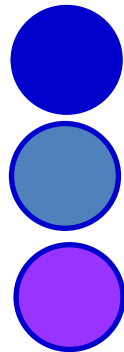
3 Capacity building ►
C-PROC

Reach of the Budapest Convention

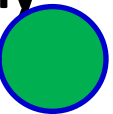


Indicative map only

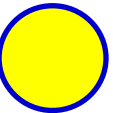
Budapest Convention
Ratified/acceded: 56
Signed: 4
Invited to accede: 10
= 70



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



**Further States drawing on Budapest
Convention for legislation = 45+**





Crime and jurisdiction in cyberspace ► solutions being negotiated by the Cybercrime Convention Committee

Specific issues being 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

Solutions:

1. More efficient MLA [agreed by T-CY]
2. Guidance Note on Article 18 [approved by T-CY in February 2017]
3. Domestic rules on production orders (Article 18) [agreed by T-CY]
4. Cooperation with providers: practical measures [agreed by T-CY]
5. Protocol to Budapest Convention [negotiations started in Sep 2017]

Capacity building on cybercrime electronic evidence

GLACY+ and other programmes:

- **Legislation**
 - **Specialised law enforcement units**
 - **Training of prosecutors and judges**
 - **Public/private cooperation**
 - **Targeting proceeds from crime online**
 - **International cooperation**
- ▶ **Dedicated Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania**
 - ▶ **Cooperation with OAS and other organisations**

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

Conclusion

Consider Budapest Convention for:

- ▶ **Protection of individuals and their rights**
- ▶ **Consistent legislation**
- ▶ **International cooperation**
- ▶ **Negotiation of new international solutions**
- ▶ **Capacity building**
- ▶ **Support to cybercrime strategies**