NATIONAL CYBER SECURITY CENTRE
Securing Ghana's Digital Journey...

Ministry of Communications

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Workshop on Cybercrime and Electronic Evidence for Judges of the Supreme Court (Accra, Ghana, 23 October 2018)
Court of Appeals (24 October 2018)

Cybercrime and e-evidence: challenges and responses

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

Cybercrime and e-evidence: threats and challenges

Cybercrime and other offences involving evidence on computer systems (e-evidence):

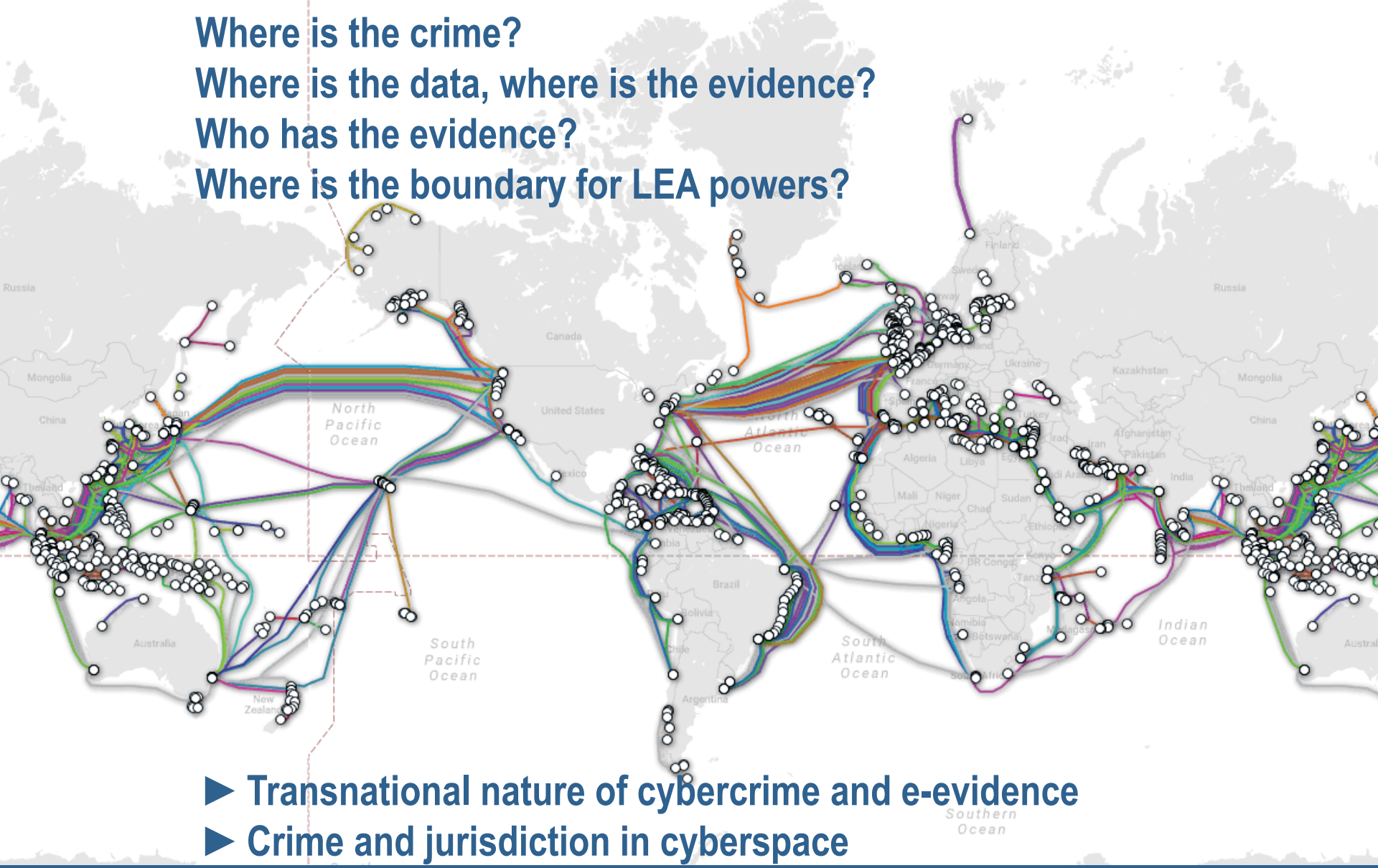
WHO DID IT?

No data, no evidence, no justice

- Billions of users and devices
- Trillions of attacks
- Millions of offences
- Is there any type of crime without e-evidence?
- Investigations % ?
- Convictions % ?

Cybercrime and e-evidence: threats and challenges

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 e-evidence: threats and challenges

Life in cyberspace, rights in cyberspace

Core political, economic and security interests in cyberspace

► How to reconcile security and fundamental rights?

Cybercrime and e-evidence: threats and challenges

Towards solutions

- Differentiate data needed
  - Subscriber information
  - Traffic data
  - Content data
- Legal framework
  - Substantive criminal law
  - Specific procedural powers to obtain data
  - Safeguards + data protection regime
- Cooperation at all levels
  - Training for ALL criminal justice officials
  - Interagency cooperation
  - Cooperation with service providers
  - International cooperation
  - Budapest Convention on Cybercrime
- Additional solutions on access to evidence in the cloud
  - Protocol to Budapest Convention

Questions?

What international benchmarks?

► Budapest Convention on Cybercrime

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 orders
- Interception of computer data

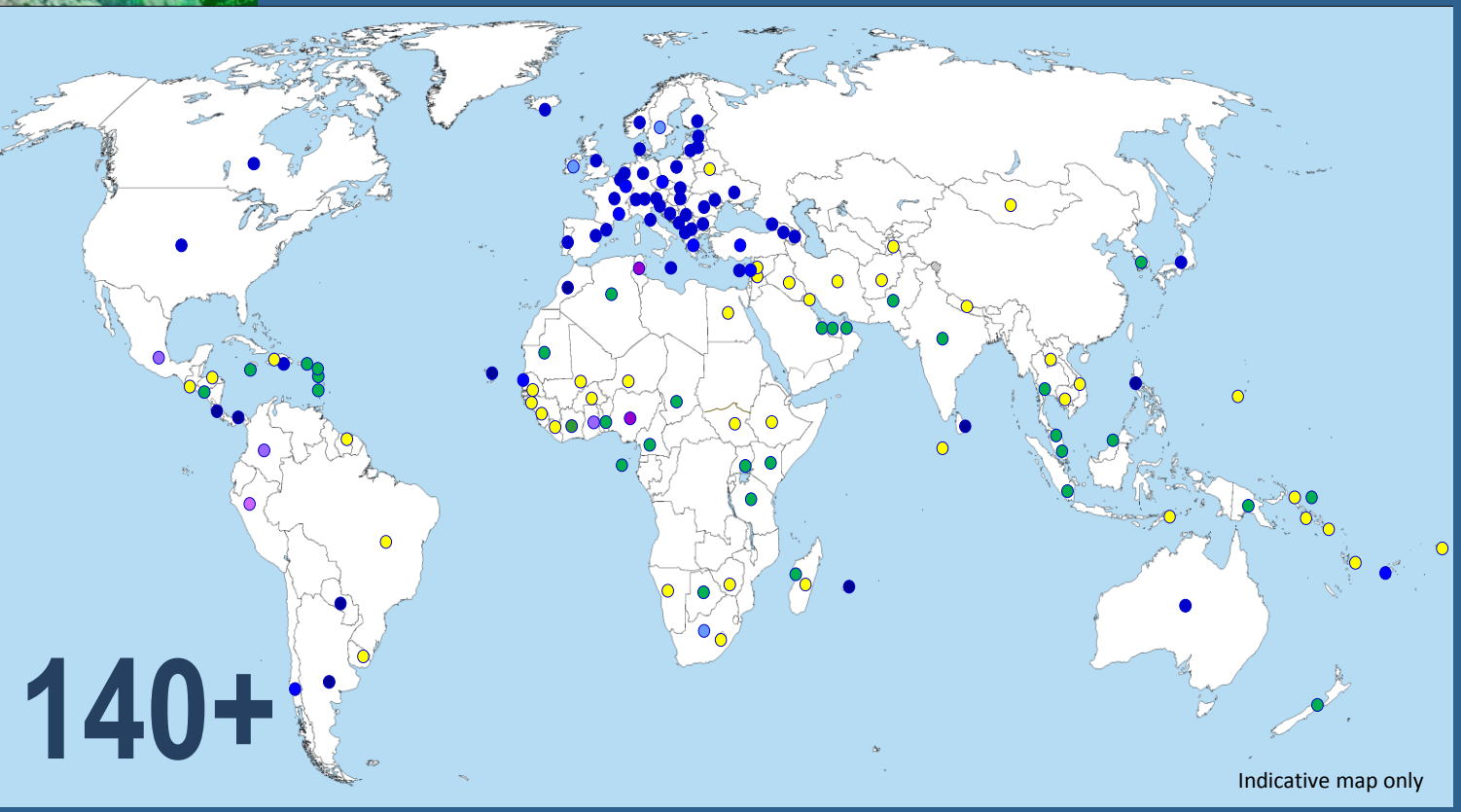
Limited by safeguards

+

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

Harmonisation

Reach of the Budapest Convention



Parties:

- ✓ Cabo Verde
- ✓ Mauritius
- ✓ Morocco
- ✓ Senegal

Signatory / invited to accede:

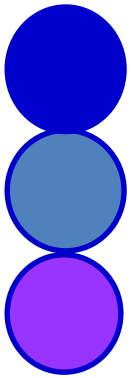
- ○ Ghana
- ○ Nigeria
- ○ South Africa
- ○ Tunisia

Ratified/acceded: 61

Signed: 4

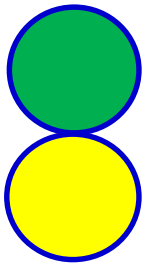
Invited to accede: 6

= 71



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

Further States drawing on Budapest Convention for legislation = 50+



Substantive criminal law

Article	Budapest Convention	Domestic provisions
Art. 1	Definitions	?
Art. 2	Illegal access	?
Art. 3	Illegal interception	?
Art. 4	Data interference	?
Art. 5	System interference	?
Art. 6	Misuse of devices	?
Art. 7	Computer-related forgery	?
Art. 8	Computer-related fraud	?
Art. 9	Child pornography	?
Art. 10	IPR offences	?
Art. 11	Attempt, aiding, abetting	?
Art. 12	Corporate liability	?

Cybercrime and e-evidence: legal framework

Budapest Convention

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Ghana
Electronic Transactions Act, 2008 (Act 772)

Access to protected computer

S.118. A person who secures unauthorised access or attempts to secure access to a protected system in contravention of a provision of this Act commits an offence and is liable on summary conviction to a fine of not more than five thousand penalty units or to a term of imprisonment of not more than ten years or to both.

Procedural powers

Article	Budapest Convention	Domestic provisions
Art. 15	Conditions and safeguards	?
Art. 16	Expedited preservation	?
Art. 17	Expedited preservation and partial disclosure of traffic data	?
Art 18	Production orders	?
Art. 19	Search and seizure	?
Art. 20	Real-time collection traffic data	?
Art. 21	Interception of content data	?

Cybercrime and e-evidence: legal framework

Article 18 – Production order

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. ….

Section 99 of ETA (Act 772) Law enforcement officer and third party assistance

Section 102 of ETA (Act 772) Disclosure of electronic information
102. (1) …
(2) A provider of an electronic communication service or remote computing service shall disclose a record or other information related to a subscriber or customer to a law enforcement agency:
(a) on receipt of a Court order for the disclosure, or
(b) on receipt of the written consent of the subscriber or customer to the disclosure.

Cybercrime and e-evidence: legal framework

Legal framework of Ghana ► largely meets minimum standards of Budapest Convention but fine-tuning recommended based on 10 years of ETA

- Broaden illegal access provision
- Differentiate powers for subscriber versus traffic versus content data
- Production orders in ETA and EOCOA
- Broaden "system interference"
- Introduce real-time collection of traffic data
- Etc.

Questions?

Cybercrime and e-evidence: institutional capacities

Multiple law enforcement agencies for cybercrime and e-evidence:

- Cybercrime Unit of the CID
- Bureau of National Investigations (BNI)
- Economic and Organised Crime Office (EOCO)
- National Security Council (coordination)
- Financial Intelligence Center (Financial Intelligence Unit)

- Division of competencies?
- Interagency cooperation?
- Uniform procedures for handling e-evidence?
- Make use of E-evidence Guide

Cybercrime and e-evidence: institutional capacities

If all types of offences may involve e-evidence, any police officer, prosecutor or judge may become involved ►

- **How to ensure that all have at least basic skills?**
- **How to ensure specialisation of some prosecutors and judges?**

LEA training strategy with baseline of skills required.

Specialisation of a team of prosecutors

Clarify responsibilities for prosecuting cybercrime

Training of judges and prosecutors ► Judicial Training Institute

Further specialise judges of the Financial and Economic Crime Court (FECC)

Questions?

WHO has the evidence?

► Cooperation with service providers in Ghana

Legal obligation to preserve, retain, produce, collect or intercept

+ culture of cooperation

What about multi-national service providers

► Offering a service in Ghana without being established in Ghana?

Budapest Convention

Article 18 – Production order

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a. ….; and

b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. ….

Direct cooperation with providers across jurisdictions

	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
Parties and Observers (70 States)	Received	Disclosure	%
Albania	27	14	53%
Belgium	2 521	2 301	91%
Cabo Verde	40	20	50%
France	29 400	18 466	63%
Ghana	0	0	0%
Germany	35 596	20 172	57%
Mauritius	2	0	0%
Morocco	30	18	59%
Nigeria	7	5	71%
Portugal	3 569	2 394	67%
Senegal	2	0	0%
Turkey	8 618	4 739	55%
United Kingdom	31 954	23 073	72%
Total (excluding USA)	170 680	109 093	64%

International cooperation under Budapest Convention ▶
Combination: regular MLA + expedited and provisional measures

Article	Budapest Convention
Art. 23	General princip. (subsidiarity)
Art. 24	Extradition
Art. 25	General rules
Art. 26	Spontaneous information
Art. 27	MLA in absence of treaty
Art. 28	Confidentiality

International cooperation under Budapest Convention ▶ Combination: regular MLA + expedited and provisional measures

Article	Budapest Convention
Art. 29	Expedited preservation
Art. 30	Partial disclosure traffic data
Art. 31	MLA accessing data
Art. 32	Transborder access
Art. 33	MLA collection traffic data
Art. 34	MLA interception content
Art. 35	24/7 point of contact

Cybercrime and e-evidence: Towards a Protocol to the Budapest Convention

A. Provisions for more efficient MLA

- Emergency MLA
- Joint investigations
- Video conferencing
- Language of requests
- Etc.

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of extending searches transborder

D. Safeguards/data protection

Terms of reference approved in June 2017.

Negotiations: Sep 2017 – Dec 2019.

Question:

Ghana about to become a Party to the Budapest Convention

► How to permit Ghana to engage in intensive international cooperation on cybercrime and electronic evidence with currently 71 other Parties?