African Forum on Cybercrime, Addis Ababa, 16 – 18 October 2018

Workshop 4: Current status of cybercrime legislation in Africa and international standards

Cybercrime legislation in Africa and the Budapest Convention: An overview

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

www.coe.int/cybercrime

Cybercrime legislation in Africa: Issues for discussion

Legislation on cybercrime AND electronic evidence: what is needed?

- Making attacks against and by means of computers a criminal offence ► What substantive criminal law?
- Empowering law enforcement authorities to secure electronic evidence in relation to any crime ► What procedural law powers? What safeguards?
- Enabling international cooperation ► What is needed in terms of harmonisation/ compatibility of domestic legislation with international standards?

Domestic legislation on cybercrime and e-evidence: What international benchmarks?

- Budapest Convention on Cybercrime ► what relevance, what benefits for Africa?

Legislation on cybercrime and e-evidence in Africa: what is the state of play?

- What is the current situation? Examples of good practice?
- How to move ahead with domestic reforms of legislation?

Cooperation on Cybercrime: The approach of the 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

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

Budapest Convention on Cybercrime as a guideline

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	?

Budapest Convention on Cybercrime as a guideline

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	?

Budapest Convention on Cybercrime: evolving

- Budapest Convention: technology neutral
- Guidance Notes
  - Notion of computer systems
  - Botnets
  - DDOS attacks
  - Critical information infrastructure attacks
  - Malware
  - Spam
  - Identity theft / phishing in relation to fraud
  - Terrorism
  - Transborder access to data (Article 32)
  - Production orders for subscriber information (Article 18)

Budapest Convention on Cybercrime: evolving

- Protocol on Xenophobia and Racism committed via Computer Systems

- In preparation: 2nd Additional Protocol on Enhanced International Cooperation and Access to evidence in the Cloud
  - A. Provisions for more efficient MLA
  - 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

How to accede to the Budapest Convention

Treaty open for accession by any State (article 37)

Phase 1:

- If a country has legislation in place or advanced draft: 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: Argentina, Australia, Cabo Verde, Chile, Costa Rica, Dominican Republic, Mauritius, Morocco, Panama, Philippines, Senegal, Tonga
- Invited: Colombia, Ghana, Mexico, Nigeria, Paraguay, Peru

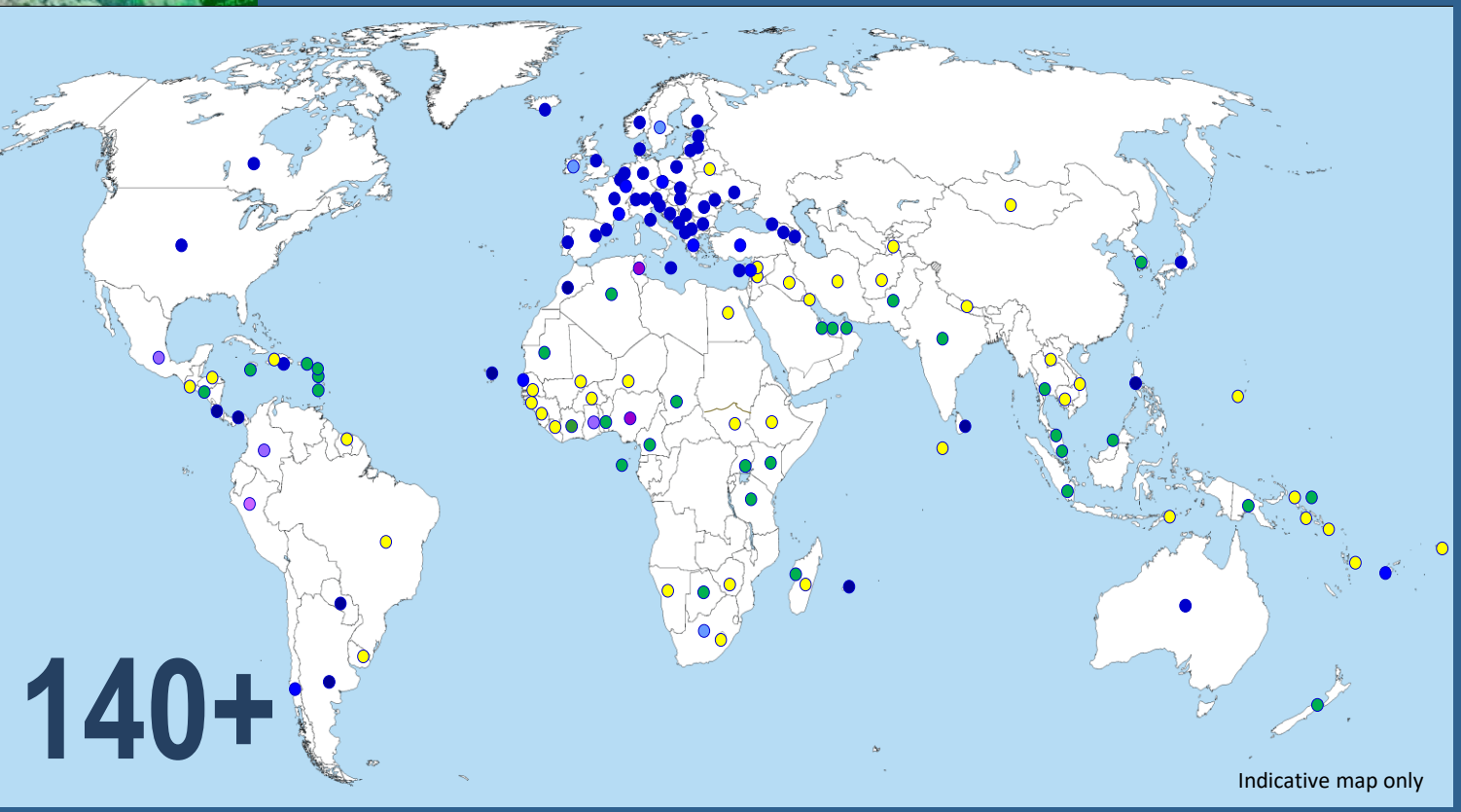
Benefits of joining Budapest Convention

- ✓ 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?

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+

Legislation on cybercrime AND electronic evidence: Progress 2013 – 2018 re substantive criminal law

By January 2013	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	6	11%	18	33%	30	56%
All Americas	35	10	29%	12	34%	13	37%
All Asia	42	13	31%	17	40%	12	29%
All Europe	48	38	79%	8	17%	2	4%
All Oceania	14	3	21%	6	43%	5	36%
All	**193**	**70**	**36%**	**61**	**32%**	**62**	**32%**

By January 2018	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	14	26%	21	39%	19	35%
All Americas	35	14	40%	15	43%	6	17%
All Asia	42	17	40%	18	43%	7	17%
All Europe	48	44	92%	4	8%	0	0%
All Oceania	14	5	36%	6	43%	3	21%
All	**193**	**94**	**49%**	**64**	**33%**	**35**	**18%**

Substantive criminal law on cybercrime: developments 2013 - 2018

- ► Good practices available in Africa
- ► Concern: Laws on cybercrime used to prosecute speech

- The protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is
  - prescribed by law
  - necessary in a democratic society
  - proportionate

- Broad, vaguely defined provisions do not meet these requirements
  - "use of computers with intent to compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger …"
  - "use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … "
  - "creation of sites with a view to disseminating ideas contrary to public order or morality"

- Problematic trend ► Discredits legitimate action on cybercrime ► violates fundamental rights

Legislation on cybercrime AND electronic evidence: Progress 2013 – 2018 re procedural powers

Specific procedural powers		In January 2013			In January 2018	
	States	Largely in place			Largely in place	
All Africa	54	5	*9%*		10	*19%*
All Americas	35	5	*14%*		9	*26%*
All Asia	42	8	*19%*		13	*31%*
All Europe	48	31	*65%*		39	*81%*
All Oceania	14	1	*7%*		3	*21%*
All	**193**	**50**	***26%***		**74**	***38%***

- **Some** good practices available in Africa
- Increasing data protection regulations in Africa
- Data Protection Convention 108 ► Cabo Verde, Mauritius, Morocco, Senegal + support to Kenya and Nigeria
- Often reliance on general powers
- Problem of safeguards

- Often reliance on general powers
- Problem of safeguards

Legislation on cybercrime AND electronic evidence: CONCLUSIONS

- Criminalising attacks against and by means of computers:
  - Good progress in Africa
  - Some concerns over vague, broadly defined provisions
- Procedural powers to secure electronic evidence:
  - Some progress in Africa
  - Specific, well-defined powers with conditions and safeguards needed
  - Progress in terms of data protection regulations
  - Data protection Convention 108/+ available for Africa
- Budapest Convention on Cybercrime is relevant for Africa:
  - Used as guideline in an increasing number of countries of Africa
  - Some countries have joined or are joining to benefit from membership
- Legislation must be backed up by capacity building


www.coe.int/cybercrime