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

Cybercrime legislation and policies in Africa: Issues for discussion

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

www.coe.int/cybercrime

1

Cybercrime legislation and policies 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?

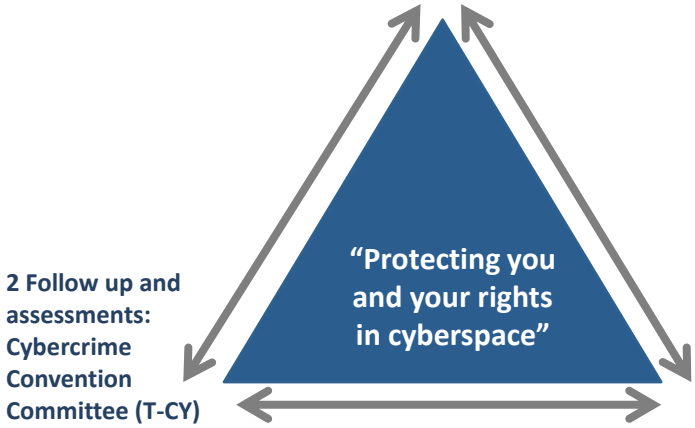
What legislation on cybercrime and e-evidence in Africa:

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

2

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

3

Legislation on cybercrime AND electronic evidence

What is needed?

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

4

Legislation on cybercrime AND electronic evidence

What international benchmarks?

► Scope of the 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

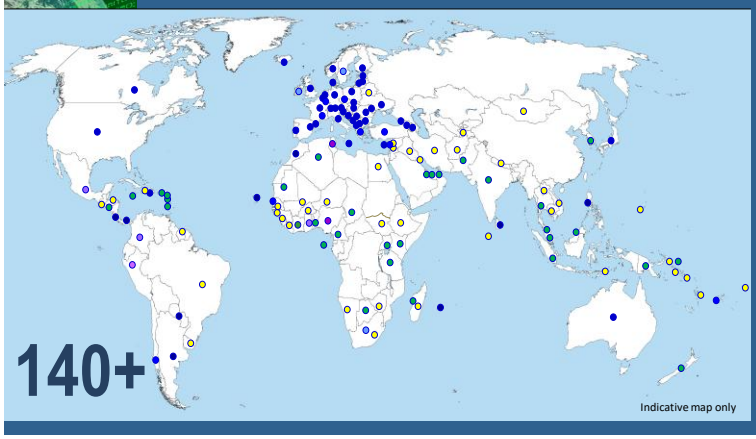
+

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

Harmonisation

5

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+

6

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%**

7

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%***

8

Cybercrime legislation and policies in Africa: Issues for discussion in Workshop 4

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?
- How to move ahead with domestic reforms of legislation?

9

10