COUNCIL OF EUROPE CONSEIL DE L'EUROPE

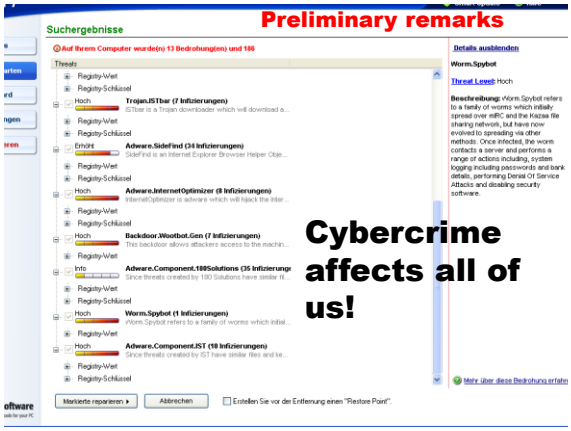
www.coe.int/cybercrime

The Convention on Cybercrime: An opportunity for Nigeria

Abuja, Nigeria (July 2009)

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

Preliminary remarks

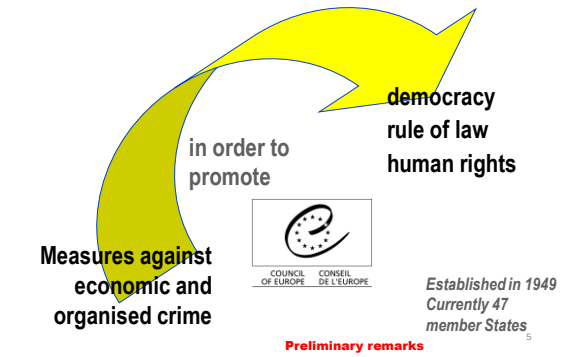


Cybercrime affects all of us!

Preliminary remarks

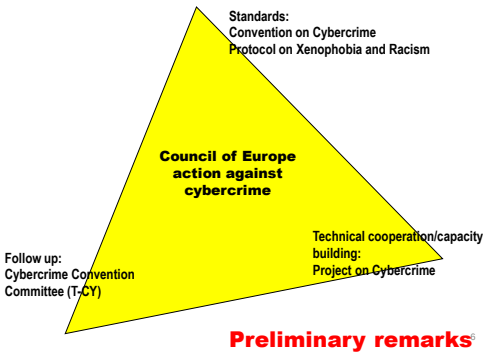
No cybercrime in Nigeria!?

About the Council of Europe ... www.coe.int



Preliminary remarks

The approach against cybercrime



Preliminary remarks

1 Why worry about cybercrime?

- Opportunities provided by information and communication technologies
- Information society: where is your private life taking place?
- Confidentiality, integrity, and availability of your computer data
- Reliance of public infrastructure on ICT
- Reliance of business on ICT
- Dependency of societies on ICT = vulnerability to cybercrime
- Need for secure and accessible ICT

But:

- Vast majority of people use ICT for legitimate purposes
- Safeguards and guarantees to ensure security and protect fundamental rights

7

2 What is cybercrime?

Offences against computers	Offences through computers
1. Offences against the confidentiality, integrity and availability of computer data and systems	2. Computer-related forgery and fraud
	3. Content-related offences (child pornography, xenophobia, racism)
	4. Offences related to intellectual property rights and similar rights
➢ Illegal access to a computer system ➢ Illegal interception ➢ Data interference ➢ System interference ➢ Misuse of devices	+ Electronic evidence!

8

The legislative response 1: Substantive Criminal Law

Legislation to deal with – as a minimum:

- Illegal access to a computer system
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery and fraud
- Child pornography, xenophobia, racism
- Infringement of copyright and related rights

Criminalising specific techniques/technologies or conduct?

9

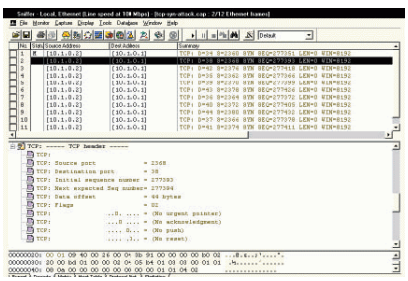
3 Investigating, prosecuting, adjudicating cybercrime: challenges

Evidence

10

Challenges

Electronic evidence



Challenges

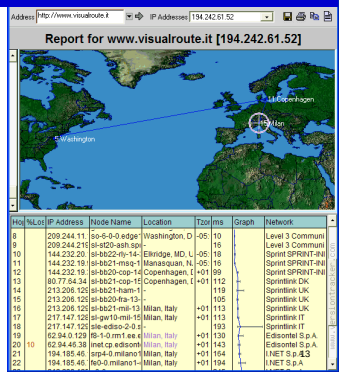
Many different kind of devices

12

Challenges

Electronic evidence is volatile evidence

➢ need for efficient, urgent measures



The legislative response 2: Procedural Law

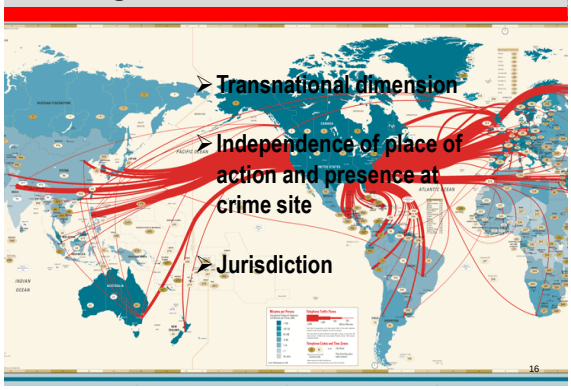
Legislation to provide for – as a minimum:

- ➢ Expedited preservation of stored computer data
- ➢ Expedited preservation and partial disclosure of traffic data
- ➢ Production order
- ➢ Search and seizure of stored computer data
- ➢ Real-time collection of traffic data
- ➢ Interception of content data
- ➢ Procedural safeguards

14

4 More challenges: cybercrime as transnational crime

Challenges



- ➢ Transnational dimension
- ➢ Independence of place of action and presence at crime site
- ➢ Jurisdiction

16

The legislative response 3: International cooperation

- ➢ Harmonise legislation with other countries
- ➢ Join international agreements
- ➢ Provide for mutual legal assistance and other provisions for international cooperation
- ➢ Introduce specific provisions for:
  - Expedited preservation of stored computer data
  - Expedited disclosure of preserved computer data
  - Mutual assistance regarding accessing stored computer data
  - Trans-border access to stored computer data (public/with consent)
  - Mutual assistance in real-time collection of traffic data
  - Mutual assistance regarding interception of content data
  - 24/7 network

5 = The Convention on Cybercrime

The Budapest Convention on Cybercrime as a response:

➢ A guideline for consistent substantive and procedural legislation

➢ A framework for efficient international cooperation

18

The Convention on Cybercrime

- Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
- Opened for signature in Budapest in November 2001
- In force since July 2004

The Protocol on Xenophobia and Racism Committed through Computer Systems

- Opened for signature in January 2003
- In force since March 2006

19

Structure and content of the Convention

Chapter I: Definitions

Chapter II: Measures at national level
- Section 1 - Substantive criminal law (offences to be criminalised)
- Section 2 - Procedural law
- Section 3 - Jurisdiction

Chapter III: International cooperation
- Section 1 - General principles
- Section 2 - Specific provisions

Chapter IV: Final provisions

20

Chapter II – Measures at national level

Section 1 – Substantive criminal law

- Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
- Title 2 – Computer-related offences (forgery, fraud)
- Title 3 – Content-related offences (child pornography)
- Title 4 – Infringements of copyright and related rights
- Title 5 – Ancillary liability and sanctions (attempt, aiding, abetting, corporate liability, sanctions and measures)

21

Section 2 – Procedural law

- Title 1 – Common provisions (scope of procedural provisions, conditions and safeguards)
- Title 2 – Expedited preservation of stored computer data (and traffic data and partial disclosure)
- Title 3 – Production order
- Title 4 – Search and seizure of stored computer data
- Title 5 – Real-time collection of computer data (traffic data, interception of content data)

These apply to all criminal offences involving a computer system!

Chapter III - International cooperation
Section 1 – General principles

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

Chapter III - International cooperation...

Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data (public/with consent)
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance re interception of content data
- Art 35 - 24/7 network

Chapter IV – Final provisions

- Art 36 Signature and entry into force (open to member States and non-members which have participated in its elaboration)
- Art 37 Accession (any State may accede following majority vote in Committee of Ministers and unanimous vote by the parties entitled to sit on the Committee of Ministers)
- Art 40 – 43 Declarations, reservations
- Art 46 – Consultations of the parties

25

Implementation – current status

- The Convention entered into force in July 2004
- 26 ratifications + 20 signatures (as of July 2009)
- Signed by Canada, Japan, South Africa, ratified by USA
- Chile, Costa Rica, Dominican Republic, Mexico, Philippines have been invited to accede
- Legislative amendments underway or completed in many other countries (Argentina, Brazil, Colombia, Egypt, India, Sri Lanka etc.) and accession to the Convention under consideration

= Convention provides a global standard

6 Model law function of the Convention

- Use as a checklist
- Compare provisions
- Use wording

Country profiles on cybercrime legislation as a tool for analysis and sharing of good practices

www.coe.int/cybercrime

Provision of Convention	Provision in national law
Art 4 System interference	?
Art 6 Misuse of devices	?
Art 9 Child pornography	?
Art 16 Expedited preservation	?
Art 18 Production order	?

27

Model law function of the Convention - for example:

Article 2 of the Convention: illegal access

- Establish as criminal offences under 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.

Nigeria Cybersecurity Bill 2008

7. (1) Any person who without authority or in excess of his authority accesses any computer for the purpose of:
(a) securing access to any program; or
(b) data held in that computer; or
(c) committing any act which constitute an offence under any law for time being in force in Nigeria, commits an offence and shall be liable on conviction:
...

= ok if this includes access to a part of a system

28

Model law function of the Convention - for example:

Article 4 of the Convention: data interference

- Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
- A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Cybersecurity bill 2008

System Interference
11. (1) Any person who without authority or in excess of authority interferes with any computer network in such a manner as to cause any data or program or software held in any computer within the network to be modified, damaged, suppressed, destroyed, deteriorated or otherwise rendered ineffective, commits an offence and shall be liable on conviction to a fine of not less than N1,000,000 or imprisonment for a term of not less than 5 years or to both such fine and imprisonment.

= Data interference not covered...

29

Model law function of the Convention - for example:

Article 16 of the Convention: Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification

Cybersecurity bill 2008

15. (1) Every service provider shall keep all traffic, subscriber information or any specific content on its computer or network for such period of time as the Agency may require.
(2) Every service provider shall, at the request of any law enforcement agency:
(a) provide the law enforcement agency with any traffic of subscriber information required to be kept under subsection (1) of this section; or
(b) preserve, hold or retain any related content.

Why limit to ISPs?

30

Note: Data preservation versus data retention

Convention on Cybercrime: data preservation

Law enforcement to order or the preservation of **specified** computer data

(data to be kept by ISP or person until ordered to hand over to law enforcement under another warrant)

European Union: Data Retention

ISPs to retain **all** subscriber and traffic data for six to 24 months (and to be deleted afterwards) but only hand specific data over to law enforcement upon a warrant

Article 15 of the Bill should be clarified.

31

7 Accession to the Convention - benefits for Nigeria

- Coherent national approach to legislation on cybercrime
- Facilitates the gathering of electronic evidence
- Facilitates the investigation of cyberlaundering, cyberterrorism and other serious crime
- Harmonisation and compatibility of criminal law provisions on cybercrime with those of other countries
- Legal and institutional basis for international law enforcement and judicial cooperation with other parties to the Convention
- Participation in the Consultations of the Parties
- The treaty as a platform facilitating public-private cooperation

Acceding to the Convention

Article 37: Convention is open for accession by third countries

Accession process:

1. Once legislation has been adopted or is in advanced stage, government to send a letter to Secretary General of CoE with a request to initiate consultation with parties to the Convention
2. Secretariat of CoE will carry out consultations and put question before Committee of Ministers
3. If vote is positive, the country will be invited to accede
4. The country is then free to decide when to accede, that is, deposit the instrument of accession

8 The way ahead

- Nigeria to analyse and improve national legislation in view of provisions of Convention on Cybercrime
- Consider accession to the Convention as a framework for international cooperation
- Council of Europe ready to provide support: legislative analysis, workshops on cybercrime legislation

34

Thank you

Alexander.seger@coe.int

35