COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

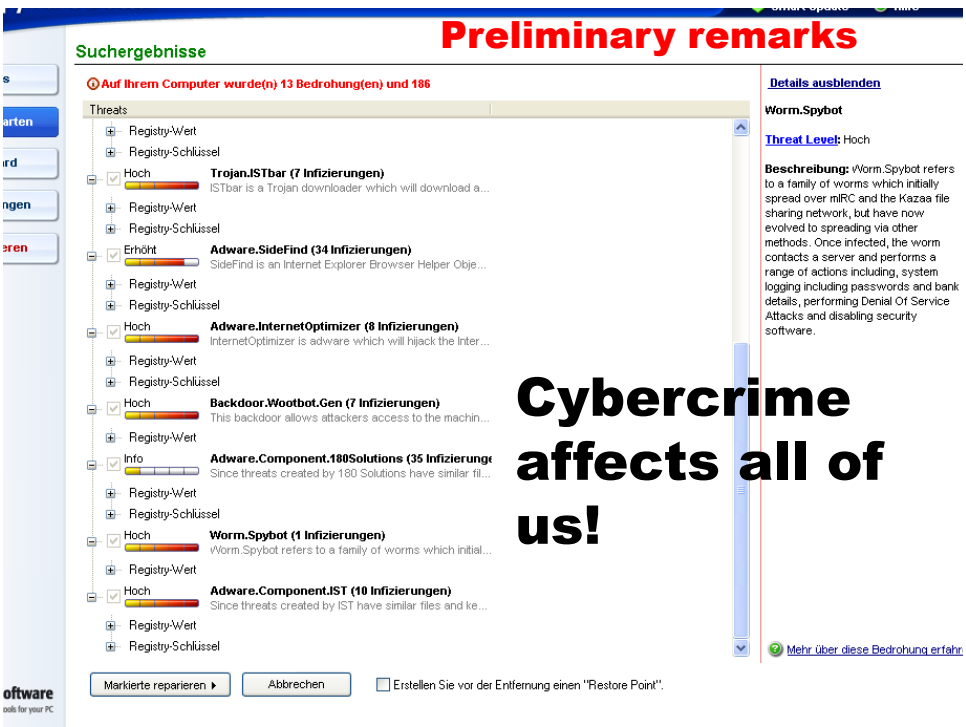
The Convention on Cybercrime:

A framework for legislation and international cooperation for countries of the Caribbean region

OAS/US DOJ Workshop on cybercrime legislation in the Caribbean region (Port of Spain, 13-15 May 2008)

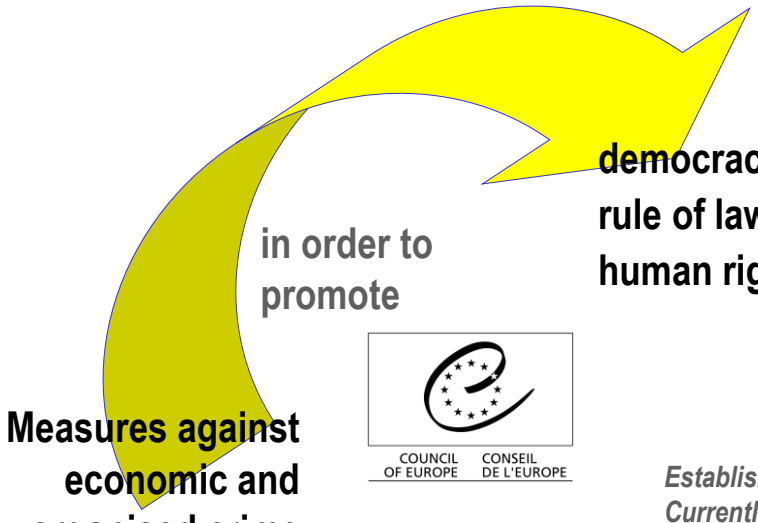
Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1



2

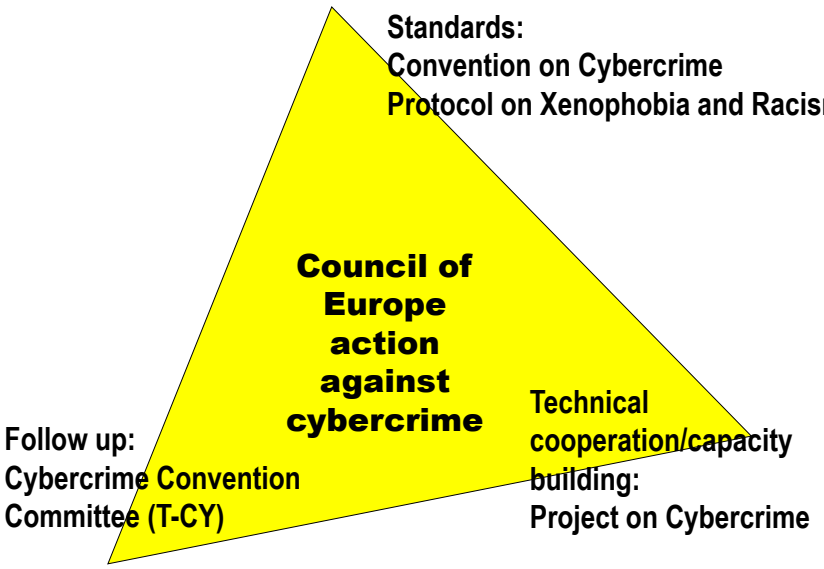
About the Council of Europe … www.coe.int



Established in 1949
Currently 47
member States

3

The approach against cybercrime



4

1 Cybercrime – current challenges

Dependency of societies on information and communication technologies. This dependency makes societies highly vulnerable to cybercrimes

- Shift in the threat landscape: from broad, mass, multi-purpose attacks to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes
- Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading
- Spam nuisance and carriers of malware
- Child pornography and sexual exploitation on the internet increasingly commercial
- Offenders increasingly organising for crime aimed at generating illicit profits
- Offences related to identity theft
- Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)
- Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)
- Growing risk of cyber-attacks against critical infrastructure

But: Vast majority of people use ICT for legitimate purposes
Need to balance security and civil rights concerns

5

5

2 The criminal law response

- Criminalise certain conduct ▶ substantive criminal law
- Give law enforcement/criminal justice the means to investigate, prosecute and adjudicate cybercrimes (immediate actions, electronic evidence) ▶ criminal procedure law
- Allow for efficient international cooperation ▶ harmonise legislation, make provisions and establish institutions for police and judicial cooperation, conclude or join agreements

6

6

Substantive criminal law

Legislation to deal with – as a minimum:

- **Illegal access to a computer system** ("hacking", circumventing password protection, key-logging, exploiting software loopholes etc)
- **Illegal interception** (violating privacy of data communication)
- **Data interference** (malicious codes, viruses, trojan horses etc)
- **System interference** (hindering the lawful use of computer systems)
- **Misuse of devices** (tools to commit cyber-offences)
- **Computer-related forgery** (similar to forgery of tangible documents)
- **Computer-related fraud** (similar to real life fraud)
- **Child pornography**
- **Infringement of copyright and related rights**

Criminalising specific techniques/technologies or conduct?

7

7

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

8

8

3 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

9

9

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

10

10

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)

11

11

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!

12

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

13

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

14

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

15

15

Implementation – current status

- The Convention entered into force in July 2004
- 22 ratifications + 22 signatures (as of 1 April 2008)
- Signed by Canada, Japan, South Africa, ratified by USA
- Costa Rica, Mexico, Philippines have been invited to accede
- Legislative amendments adopted or underway in many other countries (Argentina, Brazil, Colombia, Dominican Republic, Egypt, India, Indonesia, Nigeria, Philippines, Sri Lanka etc.) and accession to the Convention under consideration

= Major global trend towards better cybercrime legislation

= Convention provides a global standard

16

4 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

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	?

17

17

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.

Commonwealth Model Computer and Computer Related Crimes Bill

5. A person who intentionally, without lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

18

Model law function of the Convention - for example:

Article 2 of the Convention: illegal access

Dominican Republic (Law 53-07)

Article 6.- Illegal access. The fact of acceding to an electronic, computing, telematics or telecommunications system, or its component parts, whether or not by usurping an identity or exceeding authorisation, shall be punished with a prison sentence of between three months and one year and a fine of up to two hundred times the minimum wage.

Barbados (Computer Misuse)

PROHIBITED CONDUCT

4. (1) A person who knowingly or recklessly, and without lawful excuse or justification,
(a) gains access to the whole or any part of a computer system;
(b) causes a programme to be executed;
(c) uses the programme to gain access to any data;
(d) copies or moves the programme or data
(i) to any storage medium other than that in which that programme or data is held; or
(ii) to a different location in the storage medium in which that programme or data is held; or
(e) alters or erases the programme or data
is guilty of an offence and is liable on conviction on indictment to a fine of $25 000 or to imprisonment for a term of 2 years or to both.

+ Sections 9-12

19

Model law function of the Convention - for example:

Article 5 of the Convention: system interference

- **Establish as criminal offences under domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.**

20

Model law function of the Convention - for example:

Article 5 of the Convention: system interference

Commonwealth Model Computer and Computer Related Crimes Bill

7.(1) A person who intentionally or recklessly, without lawful excuse or justification:
(a) hinders or interferes with the functioning of a computer system; or
(b) hinders or interferes with a person who is lawfully using or operating a computer system;
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

In subsection (1) "hinder", in relation to a computer system, includes but is not limited to:
(a) cutting the electricity supply to a computer system; and
(b) causing electromagnetic interference to a computer system; and
(c) corrupting a computer system by any means; and
(d) inputting, deleting or altering computer data;

21

Model law function of the Convention - for example:

Article 5 of the Convention: system interference

Dominican Republic (Law 53-07)

Article 11.- Sabotage. The fact of altering, deforming, impeding, disabling, causing to malfunction, damaging or destroying an electronic, computing, telematics or telecommunications system or the programmes and logical operations run by such system shall be punished with a prison sentence of between three months and two years and a fine of between three and five hundred times the minimum wage.

22

Model law function of the Convention - for example:

Article 5 of the Convention: system interference

Barbados

6. A person who knowingly or recklessly, and without lawful excuse or justification,
(a) hinders the functioning of a computer system by
(i) preventing the supply of electricity, permanently or otherwise, to a computer system;
(ii) causing electromagnetic interference to a computer system;
(iii) corrupting the computer system by any means;
(iv) adding, deleting or altering computer data; or

(b) interferes with the functioning of a computer system or with a person who is lawfully using or operating a computer system
is guilty of an offence and is liable on conviction on indictment to a fine of $50 000 or to imprisonment for a term of 5 years or to both.

23

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.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

24

Model law function of the Convention - for example:

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

Commonwealth Model Computer and Computer Related Crimes Bill

17.(1)If a police officer is satisfied that:
(a) data stored in a computer system is reasonably required for the purposes of a criminal investigation; and
(b) there is a risk that the data may be destroyed or rendered inaccessible;
the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.
(2) The period may be extended beyond 7 days if, on an ex parte application, a [***judge] [magistrate] authorizes an extension for a further specified period of*** time.

25

Model law function of the Convention - for example:

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

Dominican Republic

Article 53.- Safeguarding the data. The competent authorities must take prompt action to safeguard the data contained in an information system or its component parts, or the system traffic data, especially where the latter are exposed to loss or modification.

[Regulation to implement this provision being developed]

26

Model law function of the Convention - for example:

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

Barbados

20. (1) Where a police officer satisfies a Judge on the basis of an *ex parte application that*
***(a) data stored in a computer system is reasonably required for the* purposes of a criminal investigation; and**
***(b) there is a risk that the data may be destroyed or rendered* inaccessible,**
the Judge may make an order requiring the person in control of the computer system to ensure that the data specified in the order be preserved for a period of up to 14 days.
(2) The period may be extended beyond 14 days where, on an *ex parte application, a Judge authorises an extension for a further* specified period of time.

27

5 The Convention as a framework for international cooperation

- The Convention (Chapter III) is increasingly used as a legal basis for international cooperation
- Contributes to the creation of additional 24/7 points of contact
- Examples of good practice available

Issues:

- Need to enhance the number of countries that are party to the Convention
- Need to make 24/7 points of contact more effective
- Preliminary measures (e.g. expedited preservation) need to be followed up by efficient MLA process

28

28

6 Accession to the Convention - benefits for countries of the Americas

- 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

29

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

30

Acceding to the Convention: Example Philippines

- April 2007: CoE participation in the APEC/ASEAN cybersecurity workshop in Manila with a formal request for support during the meeting
- May 2007: Written analysis of the draft law by CoE experts
- June 2007: Participation of representative from the Philippines in Octopus Interface Conference
- July/September 2007: Revised draft law prepared in Philippines
- September 2007: Request for accession from Philippines
- October 2007: Dep of Justice/Dep of ICT/CoE workshop in Manila to review new version of the draft law with recommendations for further improvements
- March 2008: Committee of Ministers and Parties agree to invite Philippines
- 2008: Draft law now in Parliament for hearings

31

31

7 Issues (1)

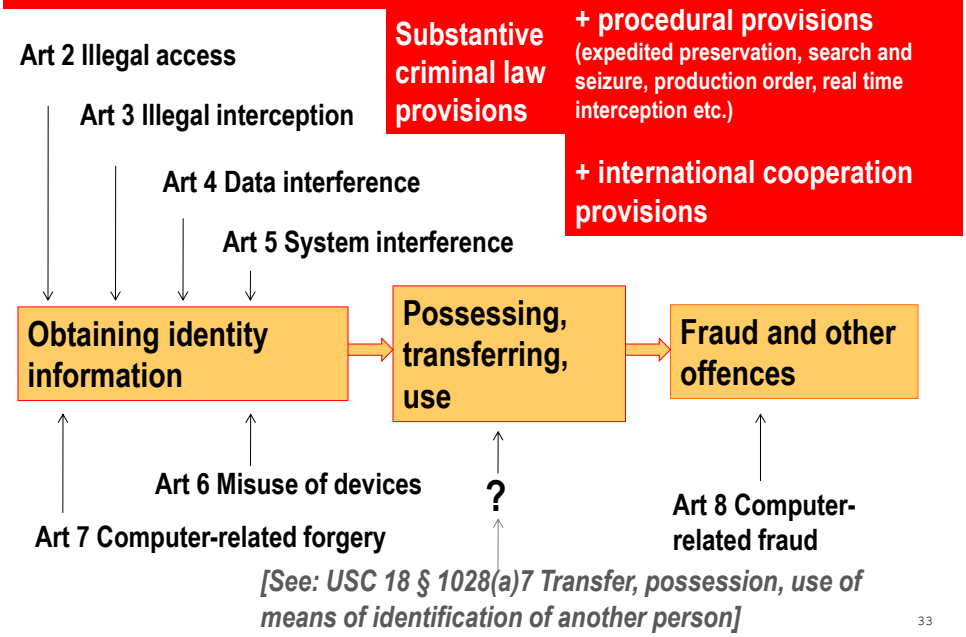
How does the Convention cover attacks against critical information infrastructure or "cyber-terrrorism"?

- Cyberattacks covered by Art 4 (data interference) and Art 5 (system interference) of the Convention on Cybercrime
- Investigative tools and international cooperation provisions of the Convention can also be applied against cyberterrorism

32

32

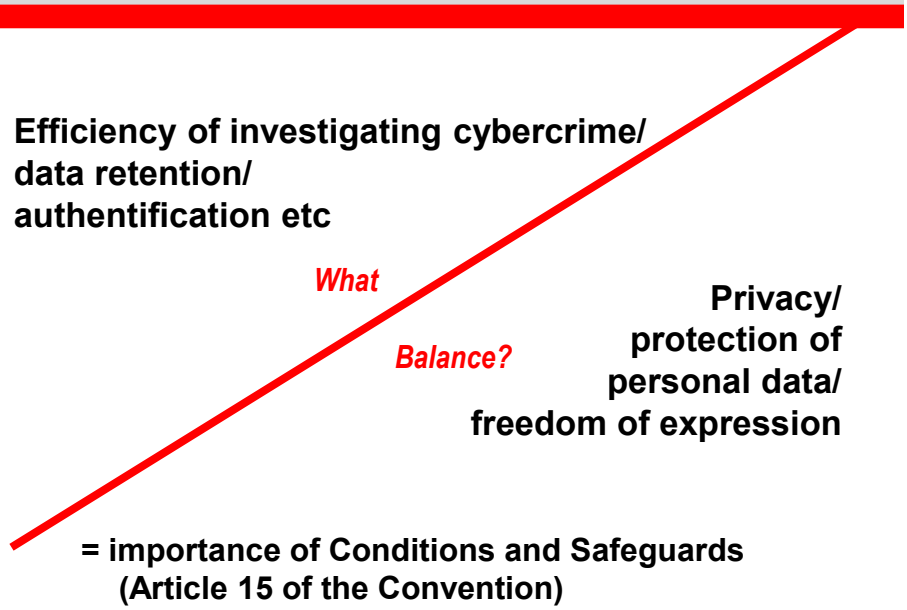
Issues (2): does the Convention cover phishing / identity theft?



33

33

Issues (3)

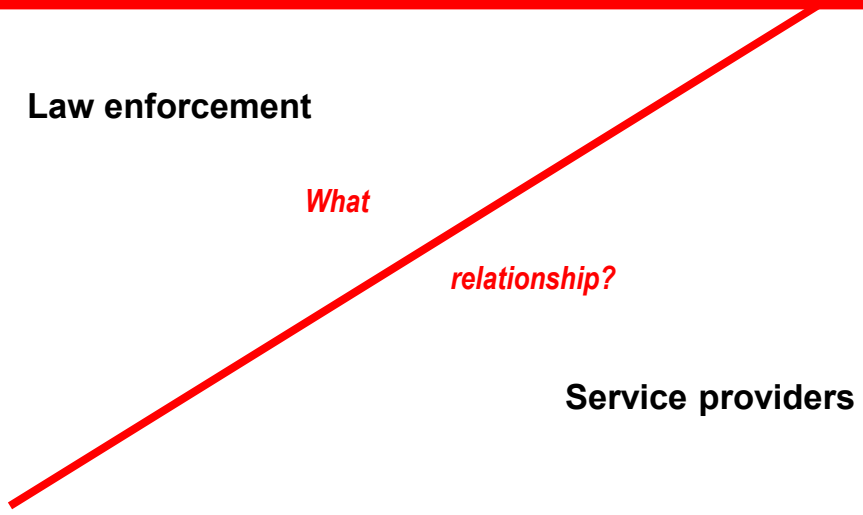


= importance of Conditions and Safeguards
(Article 15 of the Convention)

34

34

Issues (4)



35

35

Issues (4): Law enforcement – ISP cooperation

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008:

- **Common measures (including protection of rights and freedoms)**
- **Measures to be taken by law enforcement**
- **Measures to be taken by service providers**

36

36

8 The way ahead

- Review legislation against the provisions of the Convention
- If necessary take steps to strengthen legislation
- Consider accession to the Convention as a framework for international cooperation
- Council of Europe ready to provide support: legislative analysis, workshops on cybercrime legislation

37

37

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Thank you.

Alexander.seger@coe.int

38

38