COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

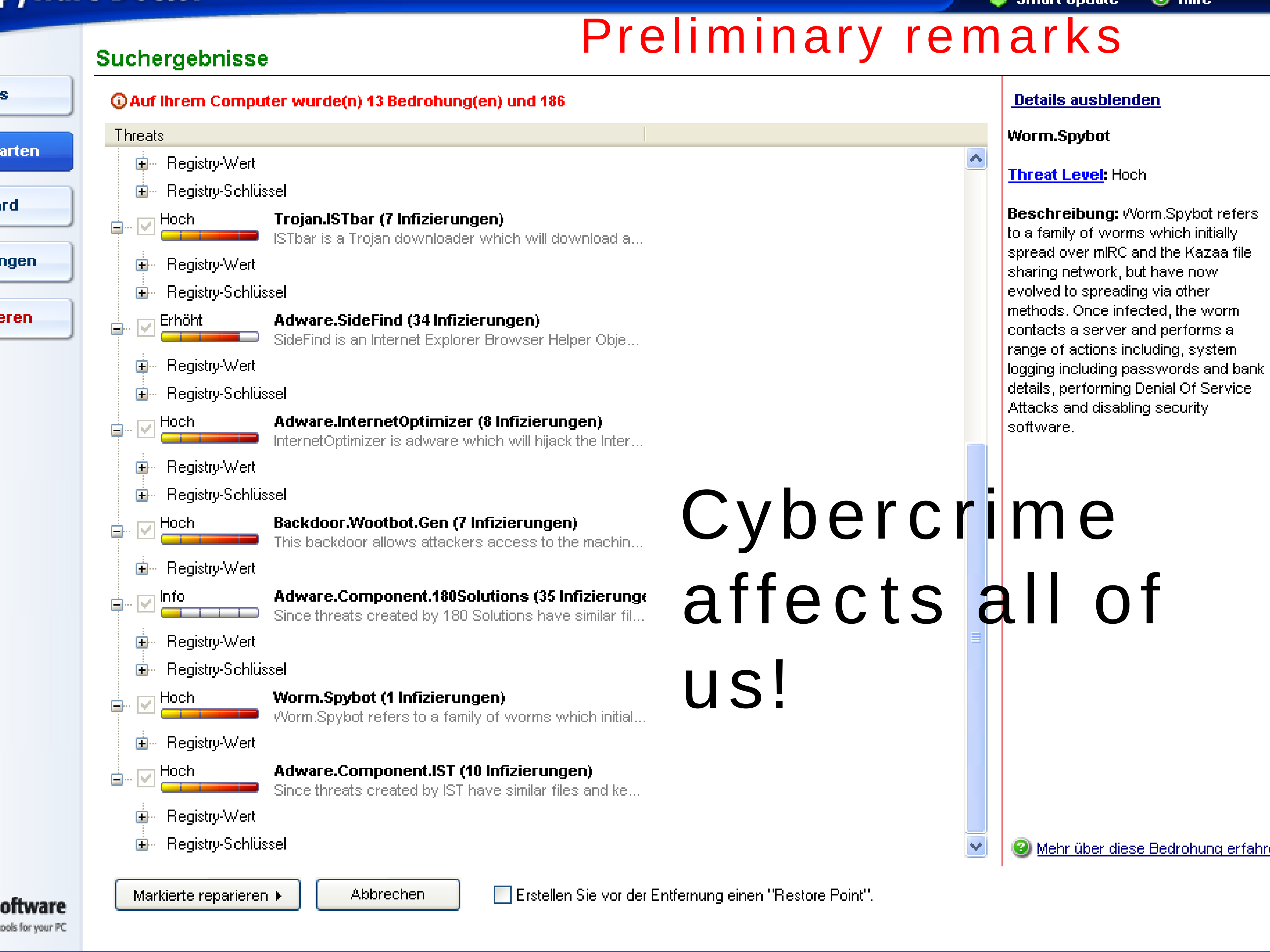
The Convention on Cybercrime:

A framework for legislation and international cooperation for countries of the Americas

Workshop on cybercrime legislation (Bogota, 3-5 Sep 2008)

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

Preliminary remarks



Suchergebnisse

Auf Ihrem Computer wurde(n) 13 Bedrohung(en) und 186

Threats

⊞ Registry-Wert

⊞ Registry-Schlüssel

⊟ ☑ Hoch — **Trojan.ISTbar (7 Infizierungen)**
ISTbar is a Trojan downloader which will download a...

⊞ Registry-Wert

⊞ Registry-Schlüssel

⊟ ☑ Erhöht — **Adware.SideFind (34 Infizierungen)**
SideFind is an Internet Explorer Browser Helper Obje...

⊞ Registry-Wert

⊞ Registry-Schlüssel

⊟ ☑ Hoch — **Adware.InternetOptimizer (8 Infizierungen)**
InternetOptimizer is adware which will hijack the Inter...

⊞ Registry-Wert

⊞ Registry-Schlüssel

⊟ ☑ Hoch — **Backdoor.Wootbot.Gen (7 Infizierungen)**
This backdoor allows attackers access to the machin...

⊞ Registry-Wert

⊟ ☑ Info — **Adware.Component.180Solutions (35 Infizierunge**
Since threats created by 180 Solutions have similar fil...

⊞ Registry-Wert

⊞ Registry-Schlüssel

⊟ ☑ Hoch — **Worm.Spybot (1 Infizierungen)**
Worm.Spybot refers to a family of worms which initial...

⊞ Registry-Wert

⊟ ☑ Hoch — **Adware.Component.IST (10 Infizierungen)**
Since threats created by IST have similar files and ke...

⊞ Registry-Wert

⊞ Registry-Schlüssel

Details ausblenden

Worm.Spybot

Threat Level: Hoch

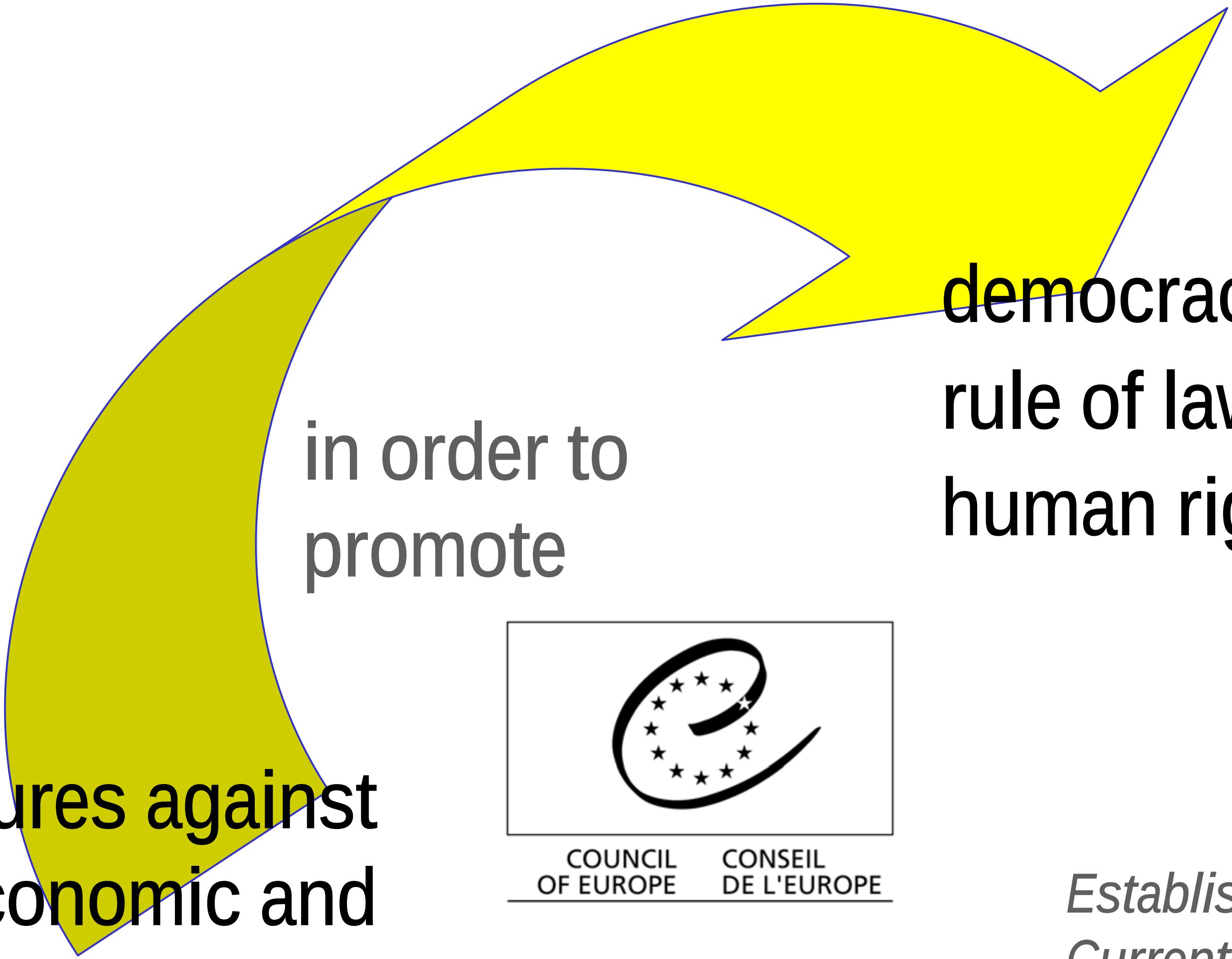
Beschreibung: Worm.Spybot refers to a family of worms which initially spread over mIRC and the Kazaa file sharing network, but have now evolved to spreading via other methods. Once infected, the worm contacts a server and performs a range of actions including, system logging including passwords and bank details, performing Denial Of Service Attacks and disabling security software.

Mehr über diese Bedrohung erfahr

Markierte reparieren ▸ | Abbrechen | □ Erstellen Sie vor der Entfernung einen "Restore Point".

Cybercrime affects all of us!

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



Measures against economic and organised crime

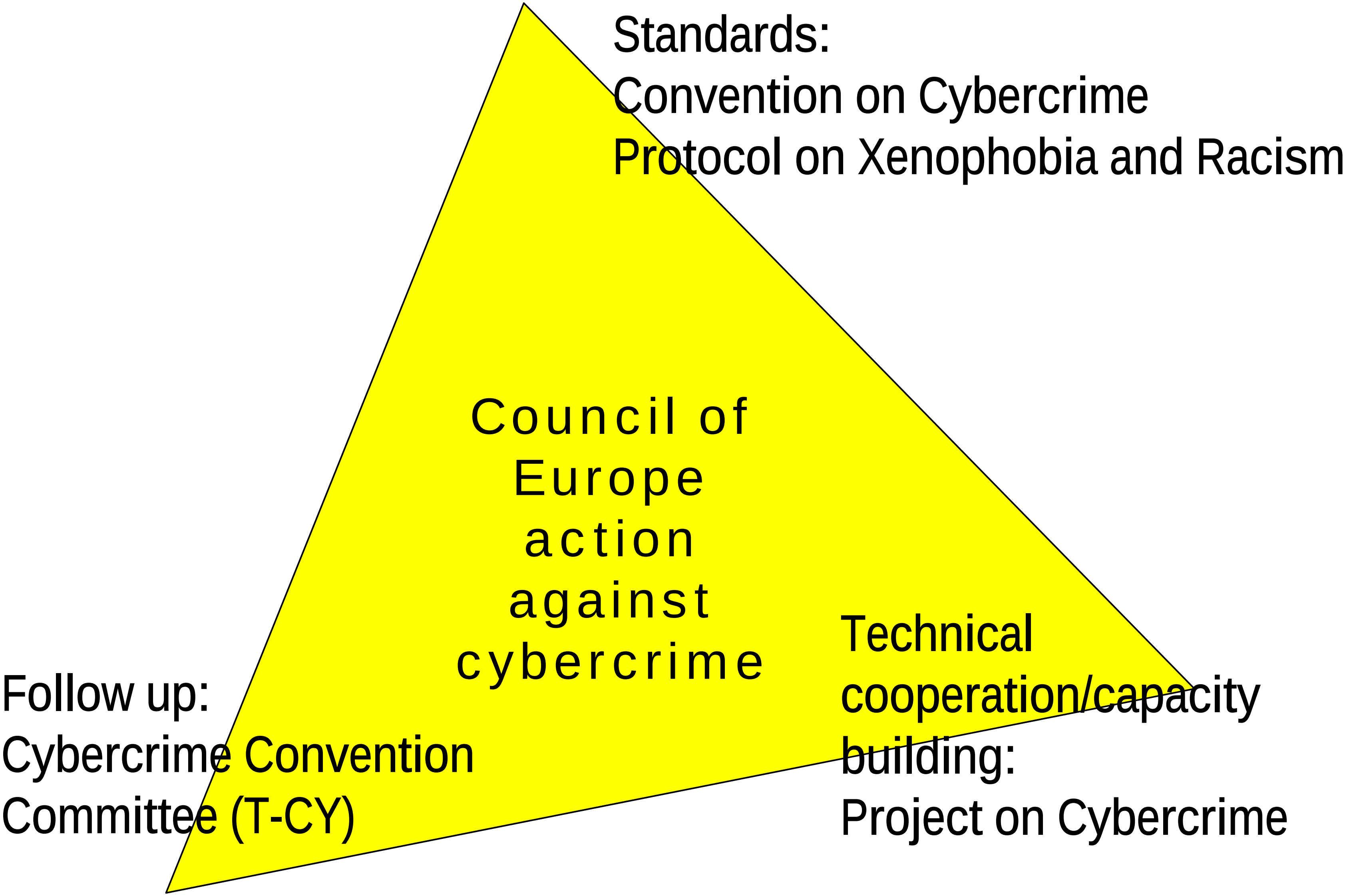
in order to promote

democracy
rule of law
human rights

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Established in 1949
Currently 47 member States

The approach against cybercrime



Standards:
Convention on Cybercrime
Protocol on Xenophobia and Racism

Council of Europe action against cybercrime

Follow up:
Cybercrime Convention Committee (T-CY)

Technical cooperation/capacity building:
Project on Cybercrime

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

Offenders increasingly organising for crime aimed at generating illicit profits

Botnets one of the central tools of criminal enterprises (DDOS, extortion, placing of adware and spyware)

Malware – that is, malicious codes and programmes including viruses, worms, trojan horses, spyware, bots and botnets – is evolving and rapidly spreading

Offences related to identity theft

Growing risk of cyber-attacks against critical infrastructure

Spam nuisance and carriers of malware

Child pornography and sexual exploitation on the internet increasingly commercial

Use of internet for terrorist purposes (attacks against infrastructure, logistics, recruitment, finances, propaganda)

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

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

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?

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

International cooperation

Legal basis/agreements for:

- Mutual legal assistance, extradition etc in cybercrime cases
- 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

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

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

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)

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

Implementation – current status

- The Convention entered into force in July 2004
- 23 ratifications + 22 signatures (as of July 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 and accession to the Convention under consideration

= Major global trend towards better cybercrime legislation

= Convention provides a global standard

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

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	?

Model law function of the Convention

Definition of terms

Key terms:

- “Computer system”
- “Computer data”
- “Service provider”
- “Traffic data”

How are these defined in your legislation?

Model law function of the Convention - for example:

Article 1 of the Convention on Cybercrime: Definitions

➢“computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data

➢“computer data” means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function

➢“service provider” means:
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service

➢”traffic data” means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service

Model law function of the Convention - for example:

Article 1 of the Convention on Cybercrime: Definitions

ART.35 (1) of Romania Law no 161/2003

- “computer system" means any device or assembly of interconnected devices or that are in an operational relation, out of which one or more provide the automatic data processing by means of a computer program

- “computer data” any representations of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can cause a computer system to perform a function

- “service provider” means:

i. any natural or legal person offering the users the possibility to communicate by means of a computer system;

ii. any other natural or legal person processing or storing computer data for the persons mentioned at item 1 and for the users of the services offered by these

- ”traffic data” are any computer data related to a communication achieved through a computer system and its products, representing a part of the communication chain, indicating the communication origin, destination, route, time, date, size, volume and duration, as well as the type of service used for communication

Model law function of the Convention - for example:

Article 1 of the Convention on Cybercrime: Definitions

Dominican Republic

Article 4. Definitions

Computer system: Any electronic device, regardless of its form, size, capacity or technology used, capable of processing data and/or signals and performing logical, arithmetical and memory functions by manipulating electronic, optical, magnetic, electro-chemical or any other type of impulses, including all input, output, processing, storage, programme, communication or other facilities connected or linked to or integrated with the system.

Computer data: Any information transmitted, saved, recorded, processed, copied or stored in any type of information system or in any of its component parts, such as those geared to the transmission, emission, storage, processing and reception of electro-magnetic signals, signs, signals, writing, still or moving images, videos, voice, sounds, data transmitted by optical, cellular or radio-electrical means, electro-magnetic systems or through any other channel suited to the purpose.

Model law function of the Convention

Substantive criminal law

How does your legislation deal with:

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

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.

Model law function of the Convention - for example:

Article 2 of the Convention: illegal access

ART.42 of Romania Law no 161/2003

1.The access, without right, to a computer system.

A person acts without right in the following situations:

a) is not authorised, in terms of the law or a contract;

b) exceeds the limits of the authorisation;

c) has no permission from the qualified person to give it, according to the law, to use, administer or control a computer system or to carry out scientific research in a computer system.

2. The act is committed with the intent of obtaining computer data.

3. The act is committed by infringing security measures.

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

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.

Model law function of the Convention - for example:

Article 5 of the Convention: system interference

ART.45 of Romania Law no 161/2003

Art. 45 – The act of causing serious hindering, without right, of the functioning of a computer system, by inputting, transmitting, altering, deleting or deteriorating computer data or by restricting the access to such data is a criminal offence and is punished with imprisonment from 3 to 15 years.

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.

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.

Procedural Law

How does your procedural legislation provide for:

- 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?

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.

3Each 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.

Model law function of the Convention - for example:

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

ART.54 of Romania Law no 161/2003

➢In urgent and duly justified cases, if there are data or substantiated indications regarding the preparation or the committing of a criminal offence by means of computer systems, in order to gather evidence or identify the perpetrators, it can be ordered the expeditious preservation of the computer data or traffic data, which are subject to the danger of destruction or alteration.

➢The preservation is ordered by the prosecutor through a motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.

➢The measure is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.

➢The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data, the respective person being obliged to expeditiously preserve them under confidentiality conditions.

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]

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.

Model law function of the Convention

International cooperation

What is your legal basis for:

- Mutual legal assistance, extradition etc in cybercrime cases
- 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 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

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

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

7 The way ahead

- Review legislation against the provisions of the Convention -> country profiles
- 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

Thank you.

Alexander.seger@coe.int