www.coe.int/cybercrime

The Budapest Convention on Cybercrime and the question of "terrorist use of the Internet"

Internet Governance Forum, Baku, Azerbaijan, CoE Open Forum, 8 November 2012

alexander.seger@coe.int

1

Terrorist use of the Internet

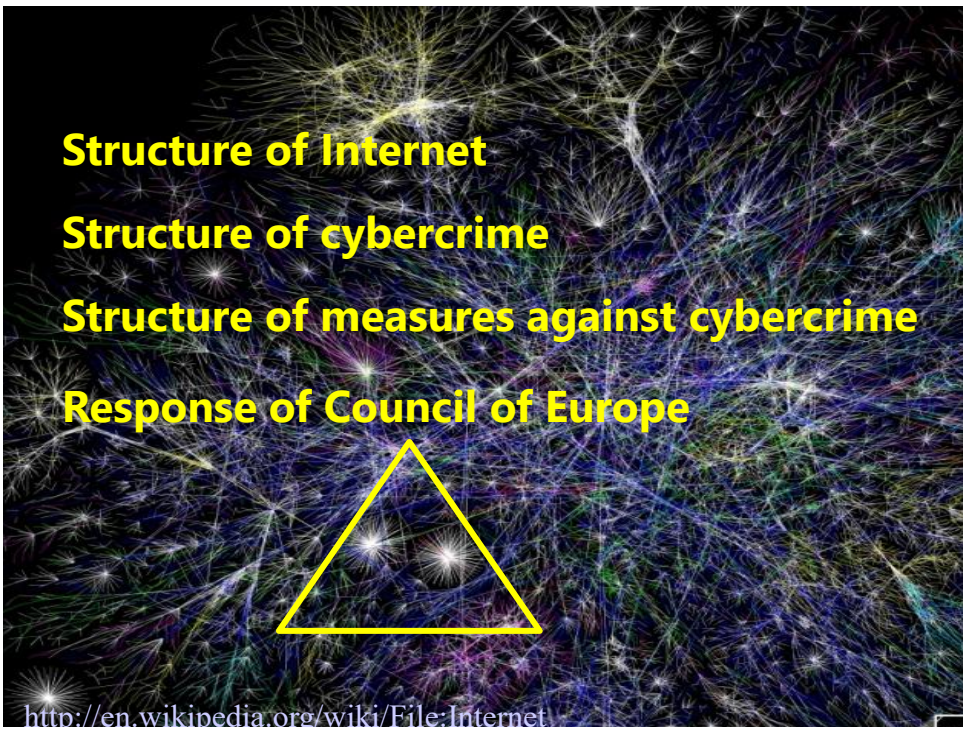
- Possible attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interests, including loss of life
- Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training
- Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

2

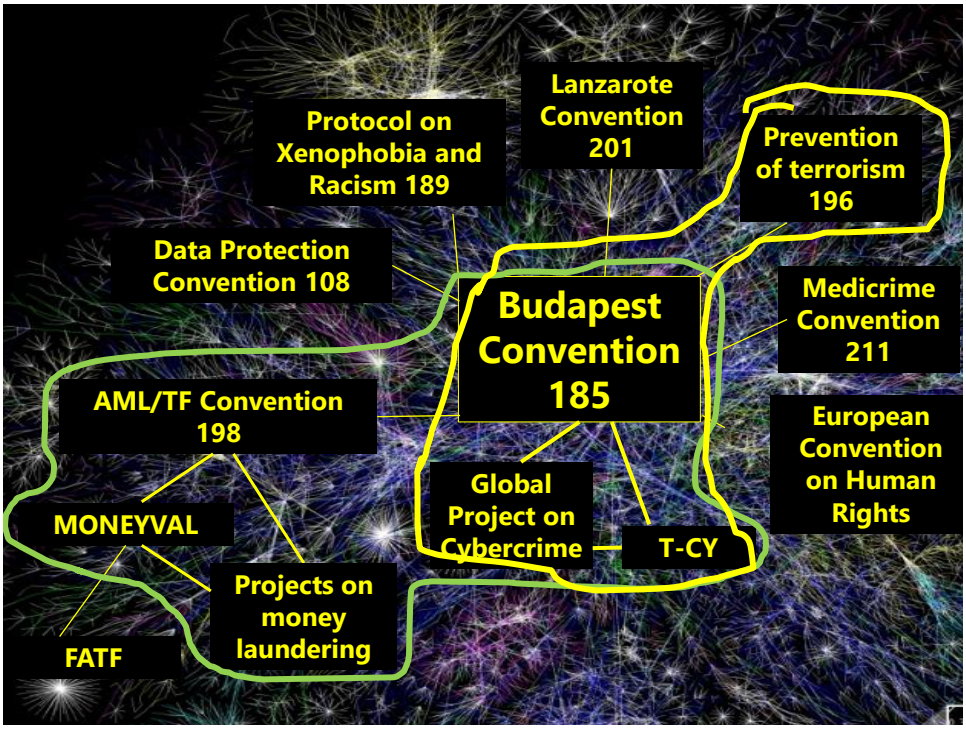
Cybercrime: Council of Europe approach

www.coe.int/cybercrime 3

3



4



5

About Budapest Convention on Cybercrime

Opened for signature November 2001 in Budapest

Followed by Cybercrime Convention Committee (T-CY) = Committee of the Parties

As at October 2012:

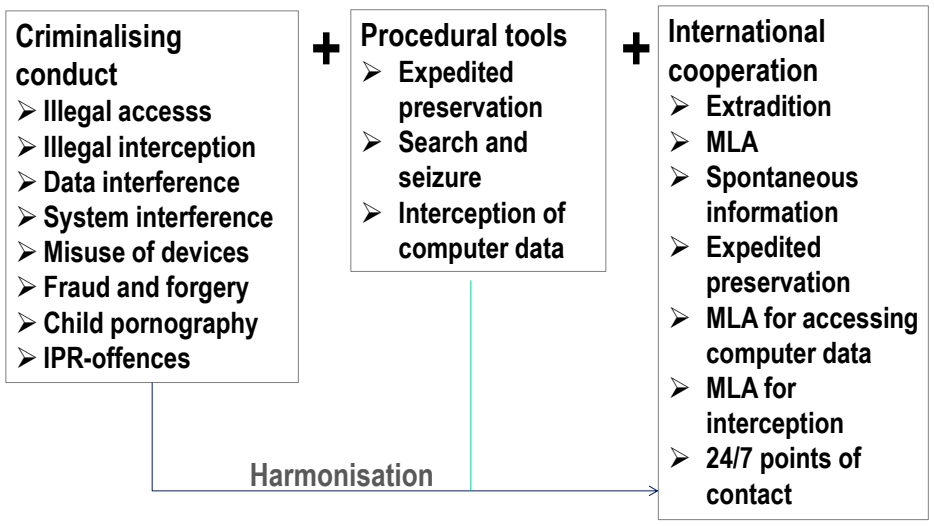
- 37 parties (35 European, Japan and USA)
- 10 signatories (9 European, Canada,, South Africa)
- 8 states invited to accede (Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines, Senegal)

= 55 states are parties/are committed to become parties

- Many more have used Budapest Convention as a guideline for domestic legislation

6

Scope of the Budapest Convention on Cybercrime



7

7

Data and system interference

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.

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.

8

The Convention on Cybercrime and terrorist use of ICT

- Convention aimed at comprehensive protection of integrity and availability of computer data and systems
- Data and system interference (including attacks against critical infrastructure through ICT) covered under Articles 4 and 5
- But review level of penalties: fines or 6 months imprisonment in some, up to 12 years imprisonment in other countries
- Procedural provisions apply
- International cooperation provisions apply
- Minimum of harmonisation of substantive and procedural law
- Convention on Cybercrime open for accession to third countries
- Main problem: More countries need to become Parties to the Convention

Convention on the Prevention of Terrorism (Council of Europe)

- Opened for signature in Warsaw 2005
- Entered into force in June 2007
- 29 ratifications + 15 signatures by Oct 2012
- Open for accession by third countries

Convention on the Prevention of Terrorism: contents

- Article 3 – National prevention policies + Article 4 – international cooperation on prevention of terrorism
- **Article 5 – Public provocation to commit a terrorist offence**
- **Article 6 – Recruitment for terrorism**
- **Article 7 – Training for terrorism**
- Article 8 – Irrelevance of the commission of a terrorist offence
- Article 13 – Protection, compensation and support for victims of terrorism
- Article 15 – Duty to investigate
- Article 17 – International co-operation in criminal matters
- Article 18 – Extradite or prosecute
- Article 20 – Exclusion of the political exception clause
- Article 21 – Discrimination clause
- Article 24 – Accession to the Convention

11

Convention on the Prevention of Terrorism: offences

Article 5 – Public provocation to commit a terrorist offence

1 For the purposes of this Convention, "public provocation to commit a terrorist offence" means the distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed

2 Each Party shall adopt such measures as may be necessary to establish public provocation to commit a terrorist offence, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

12

Convention on the Prevention of Terrorism: offences

Article 6 – Recruitment for terrorism

1 For the purposes of this Convention, "recruitment for terrorism" means to solicit another person to commit or participate in the commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group.

2 Each Party shall adopt such measures as may be necessary to establish recruitment for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Convention on the Prevention of Terrorism: offences

Article 7 – Training for terrorism

1 For the purposes of this Convention, “training for terrorism” means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence, knowing that the skills provided are intended to be used for this purpose.

2 Each Party shall adopt such measures as may be necessary to establish training for terrorism, as defined in paragraph 1, when committed unlawfully and intentionally, as a criminal offence under its domestic law.

Conclusion (I)

Attacks via internet/ICT on critical information infrastructure and other critical infrastructure, systems and legal interestets, including loss of life

Dissemination of illegal contents, including threats of terrorist attacks, incitement to or promotion of terrorism, recruitment or training

Use of ICT by terrorists for logistical purposes such as internal communication, gathering intelligence, target analyses

Covered by the

- Convention on Cybercrime

in combination with the

- Convention on the Prevention of Terrorism

15

CoE Human Rights Guidelines on Terrorism 2002

Guidelines on human rights and the fight against terrorism
adopted by the Committee of Ministers on 11 July 2002

I. States' obligation to protect everyone against terrorism

States are under the obligation to take the measures needed to protect the fundamental rights of everyone within their jurisdiction against terrorist acts, especially the right to life. This positive obligation fully justifies States' fight against terrorism in accordance with the present guidelines.

16

CoE Human Rights Guidelines on Terrorism 2002

II. Prohibition of arbitrariness

All measures taken by States to fight terrorism must respect human rights and the principle of the rule of law, while excluding any form of arbitrariness, as well as any discriminatory or racist treatment, and must be subject to appropriate supervision.

III. Lawfulness of anti-terrorist measures

1. All measures taken by States to combat terrorism must be lawful.
2. When a measure restricts human rights, restrictions must be defined as precisely as possible and be necessary and proportionate to the aim pursued.

CoE Human Rights Guidelines on Terrorism 2002

V. Collection and processing of personal data by any competent authority in the field of State security

Within the context of the fight against terrorism, the collection and the processing of personal data by any competent authority in the field of State security may interfere with the respect for private life only if such collection and processing, in particular:

(i) are governed by appropriate provisions of domestic law;
(ii) are proportionate to the aim for which the collection and the processing were foreseen;
(iii) may be subject to supervision by an external independent authority.

CoE Human Rights Guidelines on Terrorism 2002

VI. Measures which interfere with privacy

1. Measures used in the fight against terrorism that interfere with privacy (in particular body searches, house searches, bugging, telephone tapping, surveillance of correspondence and use of undercover agents) must be provided for by law. It must be possible to challenge the lawfulness of these measures before a court.

CoE Human Rights Guidelines on Terrorism 2002

XV. Possible derogations

1. When the fight against terrorism takes place in a situation of war or public emergency which threatens the life of the nation, a State may adopt measures temporarily derogating from certain obligations ensuing from the international instruments of protection of human rights, to the extent strictly required by the exigencies of the situation, as well as within the limits and under the conditions fixed by international law. The State must notify the competent authorities of the adoption of such measures in accordance with the relevant international instruments.
2. States may never, however, and whatever the acts of the person suspected of terrorist activities, or convicted of such activities, derogate from the right to life as guaranteed by these international instruments, from the prohibition against torture or inhuman or degrading treatment or punishment, from the principle of legality of sentences and of measures, nor from the ban on the retrospective effect of criminal law.

Conclusions

The way ahead:

- Roll out the Budapest Convention on Cybercrime
- Technical assistance for capacity building
- Implementation of the Convention on the Prevention of Terrorism
- Reconcile security and human rights concerns and establish safeguards
- Disruption of attacks (take down/blocking/filtering of websites, servers, IP addresses, domains): what procedures, conditions, regulations?

21

www.coe.int/cybercrime

Thank you.

Alexander.seger@coe.int

22