CNPDS/UN ISPAC Courmayeur Conference on Cybercrime 2-4 Dec 2011

Budapest Convention on Cybercrime 10 years on – Lessons learnt

www.coe.int/octopus
alexander.seger@coe.int

www.coe.int/cybercrime

1

About Budapest Convention:

- Criminalising conduct
- Efficient investigations through procedural law tools + conditions and safeguards
- International cooperation

Concept of cybercrime:

- Offences against and by means of computers
- Electronic evidence related to any crime

Criminal justice treaty:

- cyberCRIME
- rule of law + human rights principles

Note:

- Guideline + treaty
- Generic (conduct) + specific
- Negotiated + accepted
- Scalable
  - Membership
  - Contents (protools)
  - Link to other standards
- Mature and proven to work:
  - 10 y+ preparation
  - 10 y implementation
- Risk of lower standards and digital divide if new treaty were prepared

www.coe.int/cybercrime

2

Budapest Convention (23 Nov 2001 – 23 Nov 2011): key achievements

- Process of legislative reforms worldwide
- Global outreach, global impact: 55 countries ratified, signed, invited to accede. Cooperation with at least another 55 countries
- Catalyst for capacity building
- Increased criminal justice measures
- Increased cooperation between parties
- Trusted partnerships and multi-stakeholder cooperation around a common normative framework
- An essential element of norms of behaviour for cyberspace
- Contribution to human rights and the rule of law in cyberspace
- Protecting you and your rights

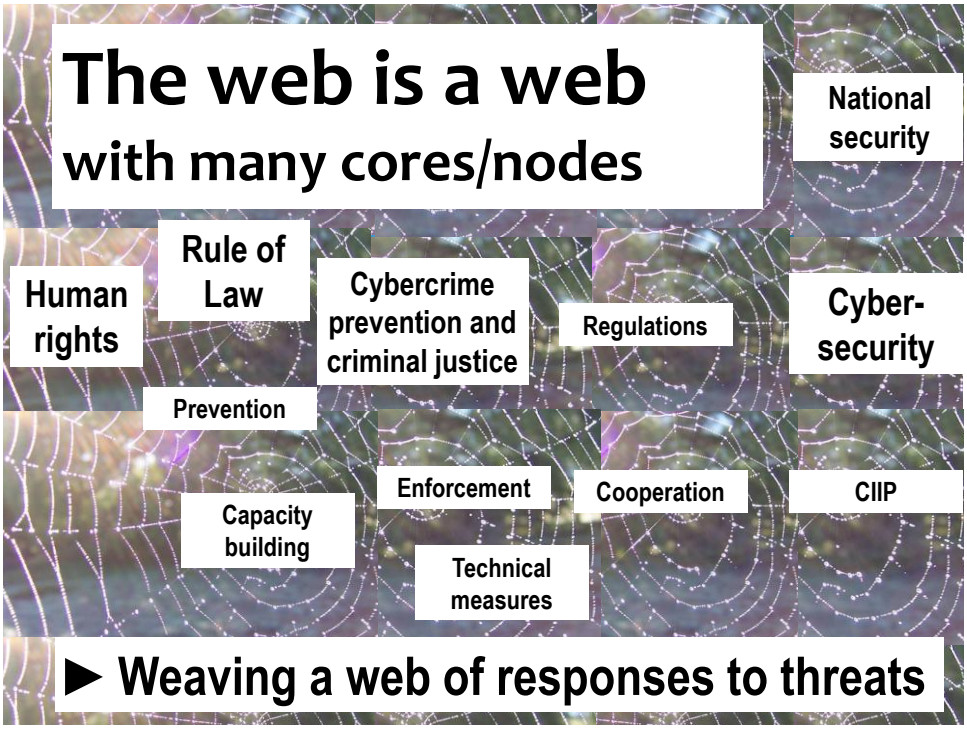
www.coe.int/cybercrime

3

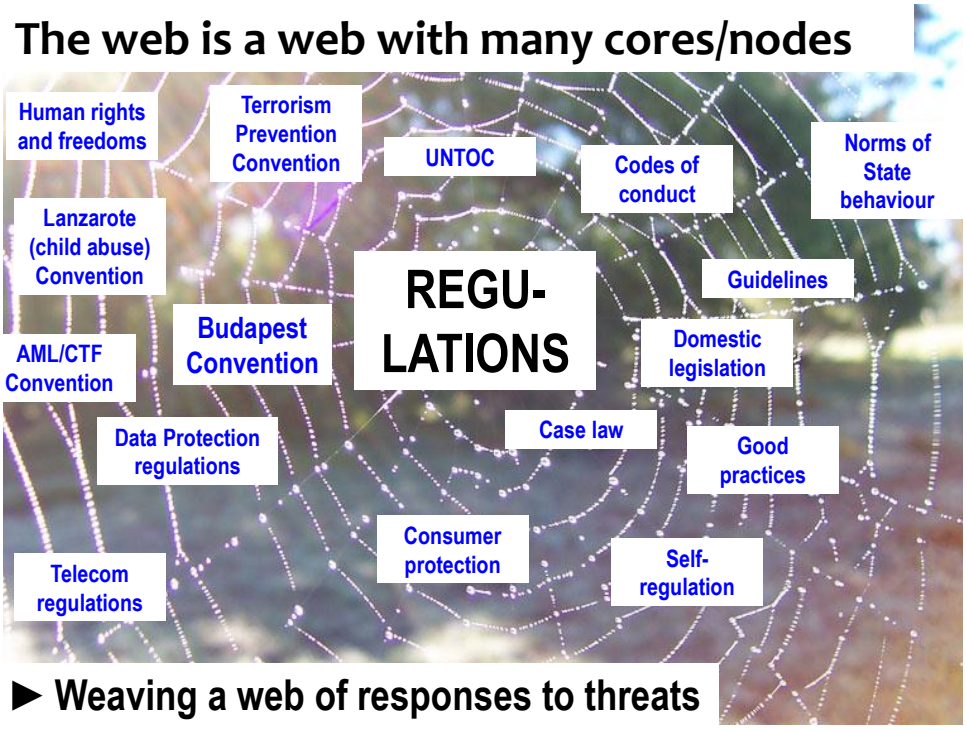
Lessons learnt:

1. Standards, norms, good practices on cyberCRIME available: Focus on capacity building to support implementation
2. Budapest Convention as a guideline for legislation
3. Increase accession to Convention as framework for trusted international cooperation against cybercrime
4. Ensure rule of law / human rights principles (Article 15 + Convention 108)
5. Solutions to transborder access by LEA
6. Enhance cooperation between international organisations to serve societies
7. Clarify concepts of cybercrime and cybersecurity – complementary but different solutions
8. Separate the issues (e.g. cybersecurity: norms on State behaviour in cyberspace?)
9. The web is a web: need to weave a web of responses

4


The web is a web
with many cores/nodes
National security
Human rights
Rule of Law
Cybercrime prevention and criminal justice
Regulations
Cyber-security
Prevention
Enforcement
Cooperation
CIIP
Capacity building
Technical measures
► Weaving a web of responses to threats

5


The web is a web with many cores/nodes
Human rights and freedoms
Terrorism Prevention Convention
UNTOC
Codes of conduct
Norms of State behaviour
Lanzarote (child abuse) Convention
REGU-LATIONS
Guidelines
Budapest Convention
Domestic legislation
AML/CTF Convention
Data Protection regulations
Case law
Good practices
Consumer protection
Telecom regulations
Self-regulation
► Weaving a web of responses to threats

6

The web is a web with many cores/nodes

► Weaving a web of responses to threats

The most efficient way ahead:

- ► **Build on and implement existing standards and practices**
- ► **Capacity building for cybercrime prevention and criminal justice**
- ► **Document and disseminate good practices**
- ► **Cooperate to expand and strengthen a web of responses**

7