SC World Congress – Panel: International response to cyber threats – New York, 10 Dec 2008

www.coe.int/cybercrime

cyberCRIME as a criminal justice issue

1. Offences against computer data and systems (malware, botnets etc)
2. Computer-related forgery and fraud (phishing/ID theft etc)
3. Content-related offences (child pornography, xenophobia, racism)
4. IPR related offences

Reliance on ICT - vulnerability

Terrorist use of the internet/ICT

- Possible attacks via internet/ICT on critical infrastructure
- Illegal contents, threats of attacks, incitement/promotion of terrorism, recruitment or training
- Use of ICT by terrorists for logistical purposes

Electronic evidence – volatile evidence

Multi-stakeholder environment – internet governance – need for common solutions

Transnational dimension – global crime scene – jurisdiction

Public-private cooperation – role of industry

Security – rights (privacy, freedom of expression, etc) – openess – access

Alexander Seger – Council of Europe – Strasbourg, France – alexander.seger@coe.int

1

A response: the Budapest Convention on Cybercrime of the Council of Europe

Criminalising conduct
- Illegal accesss
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools
- Expedited preservation
- Search and seizure
- Interception of computer data

+

International cooperation
- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

2

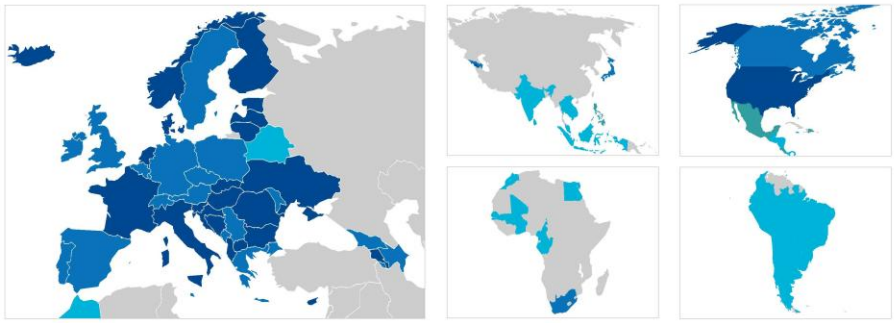
An additional response: the
Convention for the Prevention of Terrorism
of the Council of Europe (Warsaw 2005)

- Article 5 – Public provocation to commit a terrorist offence
- Article 6 – Recruitment for terrorism
- Article 7 – Training for 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 24 – Accession to the Convention

3

The Convention on Cybercrime: A global guideline for legislation and a framework for international cooperation

Source : Council of Europe, 18 November 2008



Countries that ratified the Convention

Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Cyprus, Croatia, Denmark, Estonia, Finland, France, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Slovak Republic, Slovenia, «The former Yugoslav Republic of Macedonia », Ukraine, United States

Countries that signed the Convention but did not yet ratify it

Austria, Azerbaijan, Belgium, Canada, Czech Republic, Georgia, Germany, Greece, Ireland, Japan, Liechtenstein, Luxembourg, Malta, Moldova, Montenegro, Poland, Portugal, Serbia, South Africa, Spain, Sweden, Switzerland, United Kingdom

Countries invited to accede

Costa Rica, Dominican Republic, Mexico, The Philippines

Council of Europe technical cooperation on cybercrime legislation with :

Africa: Benin, Burkina faso, Cameroun, Congo, Egypt, Gabon, Ghana, Mali, Marocco, Niger, Nigeria, Senegal, Togo

Asia: Brunei, Cambodgia, India, Indonesia, Laos, Malaysia, Singapore, Sri Lanka, Thailand, Vietnam

Europe: Belarus

Central and South America: Antigua and Barbuda, Argentina, Bahamas, Barbados, Belize, Bolivia, Brazil, Chile, Colombia, Dominica, Ecuador, El Salvador, Grenada, Guatemala, Honduras, Jamaica, Nicaragua, Panama, Paraguay, Peru, St Kitts and Nevis, St Vincent and Grenadines, Surinam, Trinidad and Tobago, Uruguay

www.coe.int/cybercrime

4

Project on Cybercrime

Supporting countries worldwide in the implementation of the Convention on Cybercrime

- Legislation
- 24/7 points of contact and international cooperation
- Law enforcement – ISP cooperation
- Training judges
- Child protection
- Data protection and privacy
- Multi-stakeholder cooperation

Phase 1 (Sep 2006 – Feb 2009)
Funded by Council of Europe, Microsoft, Estonia

Phase 2 (Mar 2009 – Jun 2011)
Budget: Euro 1.4 m
Funded by ?

Global Octopus Conference
Strasbourg
10-11 March 2009

5

Issues:

- Positive global trend since 2006 towards strengthening of cybercrime legislation in line with the Budapest Convention: needs to be sustained
- CyberCRIME: law, criminal justice, due process, rights, conditions, safeguards
- CyberSECURITY: technology/infrastructure protection/preventing, disrupting, handling attacks
- Public private partnerships. LEA - ISP cooperation. ISP responsibility.
- Jurisdiction and transborder /cloud investigations
- Follow the money
- Security AND fundamental rights

Thank you

Alexander.seger@coe.int

6