COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

EU – US Expert Meeting on Cross-border Cooperation against Cybercrime

General Policy Context - A Council of Europe perspective

Brussels 5-6 November 2009

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

1

Context: Cybersecurity and fundamental rights

- Reliance of societies on ICT -> vulnerable to cybercrime and threats
- Global network/information society vs constitutional nation state
- Internet governance
- WSIS (Geneva 2003/Tunis 2005): ICT to contribute to development, human rights, democracy, rule of law
- Multitude of stakeholders
- Fora and networks (Internet Governance Forum, EuroDiG, ISF)
- Technological developments (cloud computing, IPv6 etc) -> what impact on security and fundamental rights?

Key question: how to ensure security while maintaining due process, freedom of expression and privacy in a global environment?

2

1 Convention on Cybercrime

- Global normative framework – but requires enhanced implementation
- Supported by EU (draft Stockholm Programme) and USA (US Cyberspace Review)
- Status of signatures and ratifications
  - 26 ratified + 20 signed
  - USA ratified in 2006
  - Signed by Canada, Japan, South Africa
  - Invited to accede: Chile, Costa Rica, DomRep, Mexico, Philippines
- EU M/S
  - Ratified: 15
  - Signed but not yet ratified: 12 (Austria, Belgium Czech Republic, Greece, Ireland, Luxembourg, Malta, Poland, Portugal, Spain, Sweden, UK)
- Protocol on Xenophobia and Racism committed through Computer Systems (CETS 189)
  - 15 ratified + 19 signed

www.coe.int/cybercrime

3

2 Cybercrime legislation

- Global trend towards stronger cybercrime legislation in all regions using CCC as a guideline
- CoE/EU + ASEAN, CoE/US + OAS + APEC cooperation
- Examples:
  - Europe: Review in countries that are parties (Albania, Georgia, Ukraine, BiH, Montenegro, "the former Yugoslav Republic of Macedonia")
  - Africa: Morocco (Advances Status of Association), Nigeria, Senegal
  - Asia: India, Indonesia, Korea, Philippines, Vietnam, ASEAN
  - Caribbean: DomRep, Barbados etc
  - Latin America: Argentina, Brazil, Chile, Colombia
- Need to provide continued support

www.coe.int/cybercrime

4

3 Cybercrime training

- Law enforcement training (Europol, 2Centre, Interpol)
- Judicial training (implement concept)
- Capacity building (HTCUs)
- Example: Egypt training on cybercrime (focus on child exploitation) for judges (5-9 Dec 09)
  - at National Centre for Judicial Studies
  - in cooperation with ICMEC, InHOPE, Microsoft
  - round table on institutionalising judicial training
- Need to reinforce capacity building

4 LEA – ISP cooperation

- Need cooperative approach against cybercrime
- 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
- Taken up by the European Union
- Used in several countries
- Support cooperative approaches also in other countries and regions

5 International cooperation

- Provisions of Convention on Cybercrime
- Other treaties and agreements
- Urgent measures + MLA
- 24/7 points of contact: Convention + G8 HTCSG + Interpol NCRP
- Expedited MLA?
- How to associate industry?
- How to create more open but trusted mechanisms/platform for cooperation?

6 Online sexual exploitation and abuse of children

- Convention on Cybercrime (CETS 185) Article 9 + procedural law measures + international cooperation
- Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)
- CoE/Project on Cybercrime: Global study on substantive criminal law
- Expedite cooperation by linking up ISPs, hotlines and law enforcement (contact list, cooperative platform)

7 Criminal money flows

- Follow the money
- Building bridges between AML and anti-cybercrime worlds
- Typology exercise Nov 09 – Dec 10 led by Russian Federation
- MONEYVAL + Project on Cybercrime + MOLI-RU project (EU/CoE)
- Contributions by different stakeholders

8 Data protection/privacy

- Council of Europe 1981: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 108)
- Protocol on supervisory authorities (CETS 181 of 2001)
- Council of Europe 1987: Recommendation R (87) 15 regulating the use personal data in the police sector

- a fundamental right
- condition for law enforcement cooperation
- condition for off-shoring
- Helps protect confidentiality, integrity and availability of data and systems

- CETS 108 open for non-member States
- CETS 108 to be updated
- Recommendation on profiling in preparation
- Reforms of CoE + EU + OECD instruments -> need for cooperation

Interoperability of devices + need for authentication + cloud computing + IPv6 -> need for global trusted data protection/privacy policies

9 Cloud computing

- Information security
- Law enforcement access
- Data protection/privacy

10 Capacity building

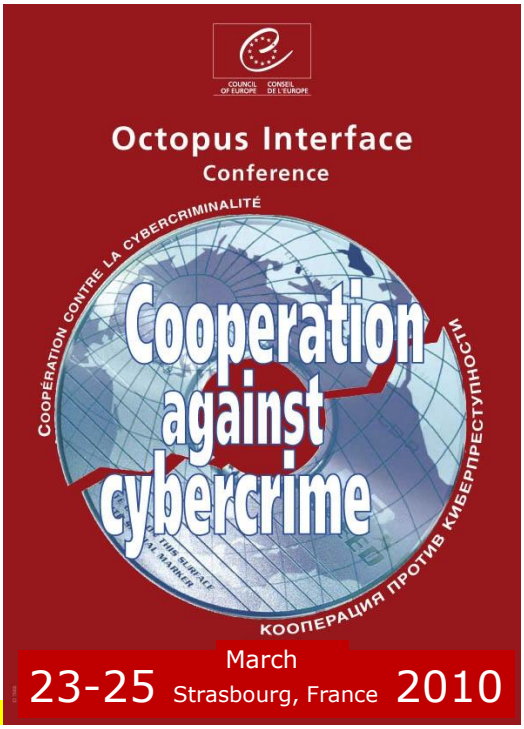
- Common agenda available
- Support implementation worldwide
- Make resources available
- PPP

Conclusions

- Convention on Cybercrime as common normative framework
- EU/COE cooperation
- CoE/US cooperation
- Multi-stakeholder cooperation
- Security and fundamental rights

Alexander.seger@coe.int

www.coe.int/cybercrime



13