Internet Governance Forum 2010 (Vilnius, Lithuania)

Cybercrime: common standards and joint action

Workshop 23

Wednesday 15 September, 14.15–16.15 (Room 4)

Instruments and tools to cope with cybercrime are already available. The core problem is that these are not necessarily implemented in all countries and regions of the world. The workshop is to discuss the following possible solutions:

- **Reinforcing global capacity building (technical assistance) efforts to support countries in the implementation of existing tools and instruments in a pragmatic manner**
- **Setting up of a mechanism (a type of "Cybercrime Action Task Force") to determine needs and review progress made by countries in the implementation of the Budapest Convention and other instruments and tools.**

Panellists:

- Markko Künnapu, Estonia
- Rusudan Mikhelidze, Georgia
- Zahid Jamil, Pakistan
- Jayantha Fernando, Sri Lanka
- Laurent Masson, Microsoft
- Cristina Schulman, Council of Europe

Moderator:

- Alexander Seger, Council of Europe

Markko Künnapu, Ministry of Justice of Estonia and chair of the Cybercrime Convention Committee (T-CY)

Value of the Budapest Convention as a common standard for joint action globally

- **The Convention is the single legally binding international instrument and therefore we encourage States to become a Party.**
- **States should establish at least minimum standards concerning legislation and operational capacity.**
- **States should take advantage of the benefits provided by the Cybercrime Convention Committee (T-CY) and the Project on Cybercrime.**
- **In order to fight cyberattacks and cybercrimes effectively at the global level we urge States to cooperate with each other using the Convention as a legal basis.**

WS 23 - Cybercrime: common standards and joint action

Rusudan Mikhelidze, Ministry of Justice of Georgia

EU/COE joint project on Cybercrime in Georgia (2009/2010) as an example for capacity building to address specific needs

The role of ITCs has increased dramatically in recent years. Communities face negative consequences of cybercrime as a modern form of offence. It is vital that the governments are duly equipped with necessary capacity to cope with existing threats and adequately respond to the incidents of cybercrime.

How do such projects benefit governments?

1. They help deliberation on a policy level, support fostering political will to tackle cybercrime by planning and implementing concrete actions;
2. They provide required technical expertise in addressing existing legislative gaps;
3. They assist development of necessary human capacity;
4. They pave the way towards public-private dialogue resulting in a solid partnership.

The project launched an important reform, which was picked up by policy-makers. That reform is now self-sustainable beyond the lifetime of the project.

WS 23 - Cybercrime: common standards and joint action

Zahid Jamil, Pakistan

View from Pakistan

Friends (incl. Signatories) of the Convention & Donor Agencies to do following:

<u>Make it a bilateral priority (just like IPR and Arbitration)</u>

- Link convention/model adoption to development funding to
- Link convention/model adoption to trade policy with other countries to this
- Sovereignty is based upon recognition in the global community of *de facto* and *de jure* system of law and order and with it come responsibilities
- Not a one way street - or a one way bridge
- Bridging of a Digital Divide requires developing country recipients to respect the bridge that is to be built and prioritise security both ways for such a bridge

<u>Resourced / coordinated awareness and myth-busting process</u>

- In general and in particular in organisations where there seem to be misconceptions
- Work with developing country multi-stakeholders (biz, civil society, legal/judicial community)

WS 23 - Cybercrime: common standards and joint action

Jayantha Fernando, Director/Legal Advisor, ICT Agency of Sri Lanka

Sri Lankan Experience

- Significant ICT Sector growth in recent times (literacy rates – from 5 % in 2004 to over 25%- 2009) and BPO sector growth
- Growing challenges - Cyber Crime
- Legislative and other measures to combat Cyber Crime
  - Payment Devices Frauds Act No. 30 of 2006
  - Computer Crimes Act No. 24 of 2007
  - Obscene Publication Ordinance (Amd) Bill 2010 – Punish Child Pornography
  - Establishment of Sri Lanka CERT (Full member of APCERT and FIRST)
    - Built on a Private sector driven model with State Support
- Value of Budapest Convention
  - Balancing various rights (Users, Victims and Service Providers)
  - Ensure consistency and compatibility of legislation (for mutual assistance and extradition)
  - Training & capacity building
- Technical Assistance
  - COE (Enforcement and Judicial Training), Microsoft (Security Co-operation Program)
  - Need for Donor Assistance – Law reform & Cyber Crime should be included in ICT development assistance programs

WS 23 - Cybercrime: common standards and joint action

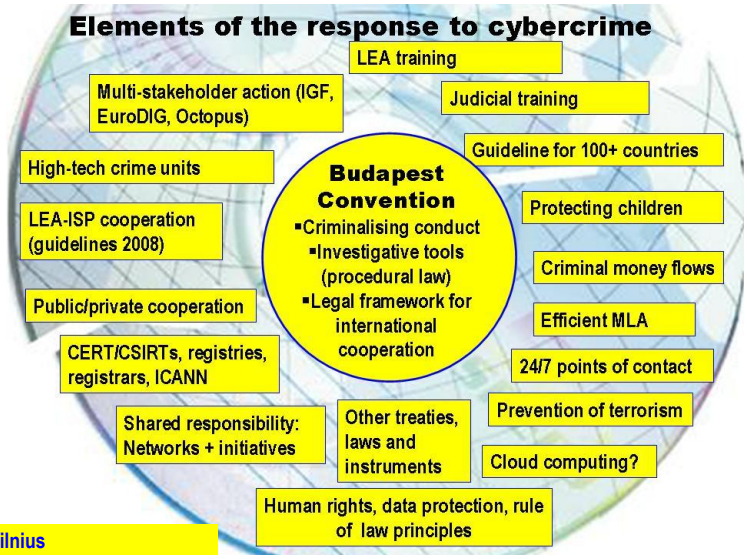
Laurent Masson, Director for Anti-Piracy and Digital Crimes for Microsoft in Europe, Middle East and Africa (EMEA)

Public-Private: Joint actions

- Establish the framework
  - **Legislation** : Argentina, Mexico, Indonesia, Philippines, Georgia, UAE…
  - **Best Practices** : France, Germany, Ukraine…
  - **National agenda** : Nigeria
- Build the infrastructure
  - **Train & Educate**
    - Upon request: Egypt, Mexico, Pakistan, Albania, Serbia…
    - Long term program with academia : 2CENTRE
  - **Collect and share data** (Signal Spam - France)
  - **Enable contact**
    - Public/Private CICILE
    - Company initiative : Microsoft Law Enforcement Portal

Cristina Schulman, Council of Europe

The Budapest Convention serves a basis for joint action against cybercrime: legislation, protection of children, public-private cooperation, data protection, international cooperation, technical assistance, training, institution building



For discussion

- Common standards, tools and good practices? Available
- Examples of joint action for capacity building/technical assistance? Available
- Common standards, tools and good practices applied everywhere? No

If full implementation of existing standards, tools and good practices is the most pragmatic way ahead to help societies meet the challenge of cybercrime, how can this be supported?

- Global capacity building effort?
- Reviewing needs?
- Resources?
- Political commitment?
- Monitoring progress?
- *"Cybercrime Action Task Force"?*