www.coe.int/octopus2012

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Octopus Conference

Cooperation against cybercrime

6 – 8 June 2012

Palais de l'Europe, Council of Europe, Strasbourg, France

Version 11 June 2012

Octopus 2012 – Key messages

Some 280 cybercrime experts from about 80 countries, 15 international organisations and initiatives, and 30 private sector stakeholders and academia met at the Council of Europe in Strasbourg from 6 to 8 June 2012 to further enhance cooperation against cybercrime at all levels.

The Octopus Conference was opened by the Secretary General of the Council of Europe and addressed by the Attorney General of Botswana, the Data Protection Commissioner of Mexico, the Head of the Cyberspace Conference of Hungary, the Head of the Digital Crimes Unit of Microsoft as well as a wide range of public and private sector experts from Africa, the Americas, Asia-Pacific and Europe. It was closed by the Deputy Secretary General of the Council of Europe.

The Conference allowed for free flows of views on complex issues and helped identify ways ahead. Progress since the last Octopus Conference (November 2011) has been noted.

Key messages resulting from plenary and workshop discussions include:

1. Strategies against cybercrime are to be part of broader policies addressing opportunities and challenges of cyberspace. They are linked to cybersecurity strategies and to human rights, the rule of law and the protection of personal data. Technical assistance for capacity building against cybercrime will help societies exploit the potential of information technologies.

2. Multi-stakeholder cooperation remains essential. This includes not only interagency, public/private and international criminal justice cooperation, but also cooperation between international organisations to better serve societies. Each organisation has its own comparative advantage. Participating organisations pledged to reinforce cooperation with each other.

3. The process of global harmonisation of legislation on the basis of the Budapest Convention has been sustained. Progress made in many countries in the adoption of legislation and implementation of this treaty is encouraging. Georgia deposited the instrument of approval of the Convention during the conference and other States are expected to follow in the coming weeks and months.

4. Private/public information sharing will enhance both cybersecurity as well as the prevention and control of cybercrime. Private sector organisations dispose of large amounts of information on incidents. Discussions suggest that it is possible to share such information in line with data protection standards. A working group could be established to document good practices and offer guidance.

5. The Lanzarote and Budapest Conventions contain criminal law benchmarks for online child protection as pointed out in the "legislative engagement strategy" of Interpol and the Virtual Global Taskforce. Adoption of legislation in line with these treaties will allow increased international criminal justice action to identify, rescue and protect child victims of online sexual exploitation and to prosecute offenders. Specific workshops should be organised in different regions to support legislative reform.

6. Transborder law enforcement access to data and electronic evidence is a major issue, in particular in the context of cloud computing. Many countries permit transborder access to data either directly or via service providers under limited circumstances. Common rules and safeguards are needed. The workshop will feed into the efforts of the Cybercrime Convention Committee that is preparing a proposal for an instrument to address this challenge.

7. Governments have the positive obligation to protect people against crime and at the same time to respect the rights of people when enforcing their laws. Conditions and safeguards limiting law enforcement powers are set forth in Article 15 of the Budapest Convention. Good practices have been documented. Data protection standards are reflected in Convention 108 which is open to any country. Legislation in line with this treaty has been adopted in a number of countries of Africa, Asia and Latin America, and these States could seek accession to Convention 108.

8. With regard to the future of cooperation against cybercrime:

- Pursue broad implementation of the Budapest Convention on Cybercrime and related instruments (such as the Lanzarote Convention and Data Protection Convention 108)
- Address emerging issues in a responsive manner through guidelines, dissemination of good practices and soft-law instruments
- Increase the efficiency of international criminal justice cooperation, in particular of mutual legal assistance procedures
- Facilitate information sharing at all levels to address both cybersecurity and cybercrime challenges while respecting rule of law and data protection principles
- Establish, in particular, clearer rules and safeguards regarding access to data and computer systems for measures taken within the national security arena
- Cooperate – just do it and don't chase false problems.

The Octopus Conference is part of the Global Project on Cybercrime and has been made possible by voluntary contributions from Estonia, Japan, Romania, United Kingdom and Microsoft as well as the budget of the Council of Europe (www.coe.int/cybercrime)