Octopus Conference on Cybercrime (6-8 June 2012)

Opening session 9h30 – 10h30
(Wednesday, 6 June, Palais, Room 1)

Address by the Secretary General, ca. 9h35-9h50

Dear Dr. Molokomme, Dr. Arzt, Ambassador Szombati, Mr. Harmon,

Distinguished guests, dear friends,

More than 2.3 billion people use the Internet. More people own mobile phones than tooth brushes. Every 60 seconds, 170 million emails are sent, 700 million searches are carried out, 1500 blogs are posted and 70 new domains are registered. But there is a down side to this too:

- every day, more than 2,000 websites harbouring spyware and other malware are identified;
- every day, about 3 million computers are infected by malware;

- every day, children and young people become victims of sexual abuse;
- every day, people become victims of fraud;
- every day, attacks against computer systems and offences using computers are reported around the world.

As we use computers for our daily activities and to exercise our rights, cybercrime is a constant threat to those very same rights.

In November 2011, we met at the last Octopus Conference and celebrated the 10th anniversary of the Budapest Convention on Cybercrime. We noted much progress and impact achieved worldwide in terms of harmonised cybercrime legislation, law enforcement and criminal justice action, and multi-stakeholderco-operation. We also noted that huge challenges still remain.

With so many cybercrime experts gathered here today, we can help societies meet these challenges – if we manage to co-operate effectively.

Let me give you six examples of concrete action taken since we last met:

1. The Cybercrime Convention Committee began to assess the implementation of the Budapest Convention. This will make the treaty more effective.

2. The Committee started to analyse the question of transborder access to data by law enforcement. This could lead to a Protocol to the Budapest Convention, or to the adoption of Guidelines. Workshop 4 at this Octopus Conference will give you the opportunity to express your views and contribute to this work.

3. In March 2012, the Committee of Ministers adopted the Internet Governance Strategy of the Council of Europe for 2012-2015. It includes specific actions against cybercrime, which should also serve to promote rights and freedoms.

4. In March 2012, we adopted a typology report on criminal money on the Internet. This report offers guidance on how to prevent fraud and money laundering and seize crime proceeds on the Internet.

5. Since November, we have organised capacity-building workshops in almost all countries of Eastern and South-eastern Europe, focusing on electronic evidence, financial investigations, high-tech crime units, judicial training and public/private co-operation.

6. In January 2012, we launched Phase 3 of the Global Project on Cybercrime. I would like to thank Estonia, Japan, Romania, the United Kingdom and Microsoft for their voluntary

contributions to this project, and would encourage others to follow their example. This project allowed us to support events in India, Mongolia and other countries. We co-operated with the Government of Costa Rica and the Organisation of American States to promote cybercrime strategies and legislation in Central America. Under this project, we are also organising this Octopus Conference.

As you can see, we have taken up your proposals (from Octopus 2011) and converted them into actions. We will do the same with your proposal resulting from this Octopus 2012 Conference.

We are very much interested in your views, especially on the five following challenges:

1. On the state of cybercrime legislation and how implementation of the Budapest Convention can be accelerated.

2. On how the private sector can share information with the authorities to prevent attacks and prosecute offenders while respecting data protection requirements.

3. On the action to be taken to protect children against sexual abuse in line with decisions taken by Interpol and the Virtual Global Taskforce.

4. On solutions to transborder access to data in the context of cloud computing.

5. How to meet the challenge of cybercrime and at the same time respect human rights and data protection requirements.

I also look forward to learning more about the strategies and measures taken by you, and of your "visions and wish lists" regarding future co-operation against cybercrime.

I should like to reiterate that we at the Council of Europe have taken many measures but we have not taken them alone, but in co-operation with many of you. I strongly believe in multi-stakeholder co-operation as the only way forward.

I very much look forward to your ideas.

I wish you successful deliberations.

Note:

The SG will be making the opening speech.

This will be followed by "setting the scene" panel which is likely to include:

- Ms. Athaliah L. Molokomme, Attorney General, Botswana
- Ms. Sigrid Arzt, Commissioner, Federal Institute for Public Access to Information and Data Protection of Mexico (IFAI)
- Mr. Béla Szombati, Ambassador, Head of Cyber Conference Secretariat, Ministry of Foreign Affairs, Hungary
- Mr. Bill Harmon, Head of Digital Crimes Unit, Microsoft, Redmond, USA

This panel is to run to 10h30, but the SG is free to escape in case he has other commitments.