Octopus Conference on Cybercrime

4-6 December 2013

Address by Jan Kleijssen

Director of Information Society and Action against Crime Directorate

Dear State Secretary Simona-Maya Teodoroiu, Director General Konrad Kogler, Dear Ministers, Dear former Deputy Secretary General,

Distinguished guests, dear friends,

The Secretary General very much regrets not being with you this morning as he had to leave for Ukraine. He has therefore asked me to open this meeting on his behalf.

Welcome to the 2013 edition of the Octopus Conference on cooperation against cybercrime. I am sure you will all agree that the Octopus conferences on cybercrime since 2004 have been stimulating experiences that helped shape policies and concrete actions on cybercrime. We can again note important progress since

the last conference in June 2012. At that same time, there are also developments that cause concern.

Let us look first at some examples of progress made:

- Legal frameworks are being strengthened in all regions of the world. New laws on cybercrime have been prepared or adopted by many countries in Africa, Asia and the Americas, often using the Budapest Convention on Cybercrime as a guideline.

- More States have joined the Budapest Convention. Since June 2012, seven States[1] have become Parties. Two States have signed it[2]. And five additional States have been invited to accede[3]. Currently, 62 States are members or observers in the Cybercrime Convention Committee. Two weeks ago, Mauritius became the most recent country to accede to the Convention. I call on all States that are signatories or that have been invited to accede to follow the example of Mauritius and become Parties as soon as possible.

[1] Australia, Austria, Belgium, the Czech Republic, the Dominican Republic, Georgia, and Japan.
[2] Andorra and Monaco
[3] Colombia, Israel, Mauritius, Morocco and Panama

- The Cybercrime Convention Committee is now assessing implementation of this treaty by the Parties. And it is issuing Guidance Notes. This enhances the quality of implementation and thus the effectiveness of the Budapest Convention.

- Octopus conferences have been promoting rule of law, human rights and data protection safeguards so that governments not only protect people against crime but also respect the rights of individuals when investigating cybercrime. Respect of human rights is an important condition that must be met, in particular in a Council of Europe context. I therefore welcome very much that States increasingly develop data protection legislation alongside laws on cybercrime. I am also pleased to inform you that the modernisation of data protection convention 108 has reached a new stage with the first meeting of the CAHDATA Committee two weeks ago which is responsible for the negotiation of an Amending Protocol.

- Octopus conferences have always underlined the need for capacity building. International treaties and laws alone will not solve the problem. Through our projects we have demonstrated that capacity building programmes can produce tangible results. I am pleased that the United Nations Crime Commission, in April

this year, reached broad agreement on capacity building as a way ahead, and that the Government of Korea put capacity building high on the agenda of the Seoul Cyberspace Conference a few weeks ago (in October). We will hear more about that conference later on from the distinguished representative of Korea.

- It is good to see that organisations and donors are prepared to invest resources in technical cooperation for capacity building. These include the European Union. On 1 November, the EU and the Council of Europe launched a new joint project on Global Action on Cybercrime that will be of benefit to many of you. Estonia, Monaco, Romania, the United Kingdom and Microsoft have also made voluntary contributions to our ongoing technical assistance activities, and Germany and Japan made special purpose contributions to the present Octopus conference.

- Cooperation with the private sector is essential, not only to prevent and control crime, but also to protect privacy and other fundamental rights. I am very pleased that the partnership with Microsoft that we started in 2006 will continue also in the future. A few days ago we signed a new agreement to this effect. I

encourage other private sector entities to engage in cooperation with the Council of Europe.

- In order to support countries through capacity building programmes we need to enhance our own capacities for the delivery of such programmes. At the Council of Europe we therefore decided to establish a new Cybercrime Programme Office in Bucharest, Romania. I am grateful to the Prime Minister of Romania for his kind offer to host this Office. With this Office we will be able to manage our capacity building programmes more effectively. I am sure State Secretary Teodoroiu will speak more about it.

So, on the one hand I can report good progress. On the other hand, however, I am concerned about certain developments.

The purpose of measures against cybercrime is to protect individuals against crime and to protect their rights. With much of our private and most intimate life taking place on computer systems and stored in the form of digital data, the protection of the confidentiality, integrity and availability of computers is essential to protect our fundamental rights. The protection of human rights, cybersecurity and action on cybercrime are complementary and should go hand in

hand. With the Budapest Convention on Cybercrime we have an international framework for this.

The Budapest Convention is a criminal justice treaty and applies to specified criminal investigations regarding cybercrime and electronic evidence. Some of the law enforcement powers foreseen – for example the interception of content data – interfere with the rights of individuals. A number of conditions and safeguards must therefore be met before a particular measure can be applied in a specific investigation. The more intrusive the measure, the stronger the conditions and safeguards.

Such a criminal justice response to cybercrime is very different from the activities of national security services and the type of mass surveillance reported in the media. The prevention and control of cybercrime does not justify and does not need mass surveillance.

Yes, external and internal security clearly are essential to protect the interests and values of a State. Effective intelligence and security services are necessities for governments. However, national security does not legitimise boundless information gathering and surveillance. In a democratic society, the activities of security

services – in particular those that interfere with the rights of individuals – must also meet a number of conditions to prevent abuse of State power. They must be prescribed by law, and necessary in a democratic society. Those affected must have access to effective remedies, and security services must be subject to effective accountability, oversight and control.

Are we sure that these conditions are met? Or are such activities violating privacy and other fundamental rights? Are they infringing the confidentiality, integrity and availability of computers? If so, wouldn't they undermine efforts on cybercrime and cybersecurity? Wouldn't they undermine the very security, trust and confidence necessary for a flourishing, free and open Internet?

The Ministerial Council of Europe conference of ministers responsible for Media and Information Society held in Belgrade one month ago debated this at length. The ministers reiterated that abuse may undermine or even destroy democracy. They invited the Council of Europe to "examine closely […….] the question of gathering vast amounts of electronic communications data on individuals by security agencies, the deliberate building of flows and

‘backdoors’ in the security system of the Internet or otherwise deliberately weakening encryption systems.”

Dear friends,

Cooperation requires trust. The Cybercrime Convention Committee has underlined on many occasions that the Parties to the Convention need to form a community of trust. I call on you to make use of the Octopus Conference to begin re-building some of the trust that may have been lost in recent months.

Thank you for your attention.