COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Speech by Maud de Boer-Buquicchio

Deputy Secretary General of the Council of Europe

Octopus Conference on "Co-operation against Cybercrime"

Strasbourg, 23 March 2010

Check against delivery

Ladies and Gentlemen, welcome to the fifth Global Octopus Conference on Cybercrime.

It is encouraging to see that so many experts from all continents, from the public and private sectors, are here again to discuss and look for answers together to the challenges presented to us. The fight against cybercrime is a round-the-clock exercise in shooting at a fast-moving target. Technology is changing fast – and the criminals are also quick to adapt. But I believe that we can – and must – be even quicker.

This Conference will start with an ambitious panel which will address a crucial question: "Security and fundamental rights – what rules for the Internet?".

In order to initiate the debate, and before giving the floor to eminent panelists, here are some introductory remarks:

Let us be very clear: international principles of human rights and the rule of law must apply on-line as well as off-line.

This is also the case for the freedom of expression which is a precondition of any democratic society and which allows individuals to fulfill themselves. The Internet is an extraordinary medium in this respect; it is a space where individuals, including children and young people, can express themselves freely, create, engage in dialogue and prompt action to resolve problems. The case of Anton Abele, a 15 year old Swedish boy, is a striking example. Following the murder of another boy at a party, Anton created a Facebook group called "save us from street violence".

More than 100, 000 people joined the call for action, and a demonstration gathering over 10,000 people in Stockholm was the starting point of a series of concrete actions to stop violence, which I have had the opportunity to discuss with Anton.

The right to freedom of expression and information is not a specific European right for the privileged few, but a universal one, as reflected in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

The same is true for respect of private life.

Privacy and the protection of personal data have become even more crucial today when everything about us is stored on computer systems, mobile phones and other devices and flows across borders to servers somewhere in the "clouds".

These are just examples. The Internet plays such a role that it affects more or less all human rights and rule of law principles. As the Internet has become vital for the full exercise of our rights and freedoms, access to the Internet itself is now increasingly considered a basic right.

While the Internet is a space where people must be able to exercise their fundamental freedoms, the use of information technologies obviously also implies risks. And the more societies rely on such technologies, the more they become vulnerable to threats such as cybercrime. Cybercrime in its many manifestations is a reality.

Cybercrime is a threat to our rights. In 2008, the German Constitutional Court issued a judgment arguing that information about our most intimate life is now stored on computer systems and that therefore people have the basic right to confidentiality, integrity and availability of their computer data. It stated that governments can therefore only intrude into this right under very narrowly defined conditions.

This is an interesting argument, because it also means that an attack against computer systems is a violation of this right. And this is exactly what the Council of Europe Budapest Convention on Cybercrime aims to protect by requiring States in its articles 2 to 6 to criminalise "offences against the confidentiality, integrity and availability of computer data and systems".

A recent judgment of the European Court of Human Rights provides further proof that criminal justice measures and the rule of law help protect fundamental rights on the Internet.

In December 2008, the Court ruled in a case[1] involving the malicious misrepresentation of a 12-year old boy. An unknown person had published intimate details of the boy as well as offers of sexual services on a dating site. The Internet Service Provider refused to provide information on the identity of the person who had posted the information because at that time, there were no legal provisions in place allowing an ISP to disclose subscriber information.

[1] European Court of Human Rights: K.U. v. Finland (application no. 2872/02) of 2 December 2008

The European Court of Human Rights found a violation of Article 8 - Right to Private Life - of the European Convention on Human Rights. The Court underlined that the Government had failed in its positive obligation to protect private life by failing to put criminal law measures in place that would allow effective investigation and prosecution.

While this was not a "cybercrime" in the narrow sense, it was an offence committed through computer systems.

In its judgment, the Court pointed specifically at the Guidelines for co-operation between law enforcement and Internet service providers adopted by the Octopus Conference 2008.

The Court also quoted extensively the procedural law measures of the Budapest Convention on Cybercrime that apply to any offence involving computer systems.

Interesting points for further discussion can be drawn from this:

- Human rights do not only need to be promoted on the Internet but also protected.

- Governments are under a positive obligation to protect the rights of their citizens as well as their security.

- In a State governed by the rule of law, action by government, in particular criminal law action, must be prescribed by law, must pursue a legitimate aim, and must be proportionate.

- Investigative measures, in particular those that intrude into the fundamental rights of people, must be based on procedural law and subject to safeguards and conditions, including independent judicial oversight.

- Full implementation of the Budapest Convention on Cybercrime will help Governments to meet their positive obligation to protect the rights and the security of people.

In this respect, the fact that in recent days Azerbaijan and Montenegro ratified this treaty is highly welcome. I call on other European countries to follow this example and ratify the Budapest Convention as quickly as possible.

However, this treaty has a global vocation and I would therefore encourage countries from all over the world to consider accession. I understand that this question was discussed intensively by the authorities of Argentina in recent months and I look forward to learning more about the outcome in a few minutes.

In conclusion, I should like to emphasise that security and human rights are not mutually exclusive concepts, to the contrary a genuine security needs human rights – and vice versa.

There seems to be a growing consensus in this respect and we experience the construction of a global set of rules and principles that will allow us to ensure both security and fundamental rights on the Internet.

The Council of Europe contributes to this global construction through its human rights and criminal law instruments, including in particular the Budapest Convention as well as the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse which will enter into force on 1 July 2010.

However, this is a shared responsibility. In the globalised online environment, we all need to contribute to a rights-based and safer cyberspace.

We all need to make sure that societies worldwide are able to apply in practice agreed upon rules, and are able to strengthen online security. For that, a global capacity building effort is required that will help countries improve their legislation, train criminal justice authorities, empower and protect children, strengthen public-private co-operation, and co-operate internationally. Such an effort will promote human rights and the rule of law at a global scale.

In a few weeks, the Crime Congress of the United Nations will meet in Brazil. I believe that this event will provide an excellent opportunity to support a global capacity-building effort based on existing tools and instruments.

The UN event will be an opportunity to reinforce our global response to the global threat of cybercrime and cyberterrorism. I think we will have the best chance to succeed if we unite around one international instrument which already exists – namely the Council of Europe Cybercrime Convention. The more countries which join it, the better chance we have to gain ground against cybercriminals. Let us be clear about one thing – they will not give the international community the courtesy to wait if we decided to spend a couple of years discussing how to reinvent the wheel, rather than use – and possibly improve on what is already there. I will stop here. If I sound dramatic, believe me, it is intentional. The problems we face are serious enough.

Thank you.