PC.DEL/420/11
9 May 2011

ENGLISH only

**EUROPEAN UNION**

**OSCE CONFERENCE ON A COMPREHENSIVE APPROACH TO CYBER SECURITY: EXPLORING THE FUTURE OSCE ROLE**
**Vienna, 9-10 May 2011**

# EU statement on OSCE Conference on a Comprehensive Approach to Cyber Security: Exploring the Future OSCE Role (Opening Session)

The Astana Summit called on the OSCE to achieve greater unity of purpose and action in facing emerging transnational threats. Against this background, the European Union welcomes the initiative by the Chairmanship in Office to convene this conference on a comprehensive approach to Cyber Security and exploring the future OSCE role.

Ensuring the security of cyber space and fighting Cybercrime are priority objectives for the EU. As regards Cyber security, this is underlined notably in, among other initiatives, the Digital Agenda for Europe of 2010 as well as in the 2011 Communication on Critical Information Infrastructure Protection ("Achievements and next steps: towards global cyber-security"). Priorities regarding the fight against Cybercrime have been highlighted in the Stockholm Programme and further reaffirmed in the Commission Communication on the “EU Internal Security Strategy in Action: Five steps towards a more secure Europe” adopted in November 2010. Cyber threats may be natural and accidental (e.g. technical failures) or voluntary and man-made (e.g. attacks). The EU shares the international community’s concern about the increasing threat from cyber

space including Cybercrime, where effective international co-operation is vital. In this respect, the efforts at international level should be primarily focused on the actual implementation of existing tools and instruments, while providing for consolidated approach in capacity building and technical assistance in developing countries.

Cyberspace has become essential for the economic, social and political health of all States. It underpins many of our daily activities, both professionally and in our personal lives, and also fundamentally supports much of a States' national infrastructure. This growing dependency exposes us to new vulnerabilities.

The European Union has been tackling this issue actively over recent years. Already in 2004 the EU established ENISA – the European Network and Information Security Agency, which contributes to achieving a high and effective level of Network and Information Security within the European Union. On 30 September 2010, the EU Commission presented a proposal to modernise and revitalise ENISA and to extend its mandate for a further five years, until 2017. Furthermore, in 2006, the EU adopted a Strategy for a Secure Information Society. The 2008 Report on the Implementation of the European Security Strategy includes cyber security as one of the global challenges and key threats, alongside Proliferation of Weapons of Mass Destruction, Terrorism and Organised Crime, Energy Security and Climate Change.

In 2009, the Commission adopted a Communication on Critical Information Infrastructure Protection (CIIP) **"**Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", setting out a plan (the 'CIIP action plan') to strengthen the security and resilience of vital Information and Communication Technology (ICT) infrastructures. The aim was to stimulate and support

the development of a high level of preparedness, security and resilience capabilities both at national and European level.

In March 2010, the European Council adopted the European Union's Internal Security Strategy. It describes cyber-crime as a global, technical, cross-border, anonymous threat to our information systems which poses many additional challenges for the law-enforcement agencies in the EU. Later the same year the European Commission adopted a Communication on the Internal Security Strategy which includes action oriented proposals. Further concrete steps are foreseen within the context of the EU Stockholm Programme 2010-2014.

The EU Presidency has organised, in co-operation with the EU Commission, a Ministerial Conference on Critical Information Infrastructure Protection in Balatonfüred on 14-15 April 2011.

The EU Presidency has recently organised a conference "Cyber-security: Challenges and Policies" in Budapest on 2 May 2011. The event's objective was to examine cyber security and defence as a comprehensive security policy challenge, analysing present problems and solutions as well as future trends, with special regard to opportunities for co-operation with other international organisation.

Threats to Cyber security are both transnational and cross dimensional. Addressing these challenges requires a coordinated response drawing on internal, foreign and defence policies. The OSCE's unique cross-dimensional approach to security can provide an excellent foundation to meet this challenge.

We have noted that the Report by the Secretary General on the implementation of the Athens Ministerial Council Decision 02/09 on Further OSCE Efforts to Address Transnational Threats and Challenges

to Security and Stability includes cyber security among the topics requiring further co-operation between the various members of the OSCE family. We look forward to further strengthening programmatic coordination between OSCE executive structures. Based on the consensus achieved in Astana, meaningful and visible steps should be undertaken by the time of the OSCE Ministerial Council in Vilnius to adjust and further develop OSCE mandates on TNT-related programmes while gradually strengthening programmatic coordination in this area of activities. Both goals should be pursued in parallel and in a complementary manner.

In this regard, the issue of a comprehensive and multidimensional approach to cyber security is particularly relevant. In the framework of the Corfu process, the EU has proposed to examine the need for an OSCE Strategy for Cyber Security. In this area, we must build on existing OSCE capacities and expertise on antiterrorism, organised crime, drug and human trafficking and police-related activities. Furthermore, it will be essential to identify where the OSCE can complement and add value to international efforts, in close collaboration and coordination with the UN, the European Union, the Council of Europe and other international organisation and fora that pursue relevant activities in this field.

The candidate countries TURKEY, CROATIA*, the FORMER YUGOSLAV REPUBLIC OF MACEDONIA*, MONTENEGRO* and ICELAND**, the countries of the Stabilisation and Association Process and potential candidate countries ALBANIA, BOSNIA AND HERZEGOVINA and SERBIA, the European Free Trade Association country NORWAY, member of the European Economic Area, as well as UKRAINE, ARMENIA, GEORGIA and ANDORRA align themselves with this statement.

*Croatia, the Former Yugoslav Republic of Macedonia and Montenegro continue to be part of the Stabilisation and Association Process.

**Iceland continues to be a member of the EFTA and the European Economic Area.