Speech by Mr Rudolf Peter ROY,
Head of division for Security Policy and Sanctions of the European External Action Service, at the L COSAC Meeting
29 October 2013, Vilnius

Honourable members of the National Parliaments of the EU member states and candidate countries,

Honourable members of the European Parliament,
Ladies and Gentlemen,

It is for me a great honour to speak to the 50th Conference of COSAC. The issue I like to address today are challenges and perspectives of Cyber Security.

Information and Communication technology (ICT) related activities accounted for more than 20 percent of GDP growth in the world's major economies over the last five years. According to relevant studies, the Internet is already contributing up to 8 percent to GDP in some of the G-20 economies.

If it were a national economy, the Internet economy would rank in the world's top five – and its significance just keeps growing. **But:** The benefits of the Internet go obviously far beyond its direct economic benefits.

In simplified terms Cyber space helps us to achieve a better future. It provides access to education, promotes freedom of speech; it connects people worldwide and enables essential services. It works as a crucial catalyst for achieving the Millennium development goals.

Technology also acts as a great global equalizer. Cyberspace empowers people in all corners of the world, young and old, rich and poor. In the spring of 2011 it helped the people in North Africa to stand up for their rights.

In 2013, we have 2,4 billion Internet users. This number will double by 2020. To fulfill the vision of a better future for billions, we need a cyberspace that is open, undivided, unfragmented and not controlled by any single entity. Today, more than ever before, we also need trust, reliability and increased capacity in this manmade domain.

Recent years have seen that while the digital world brings enormous benefits, it is also vulnerable. Cyber security incidents, be it intentional or accidental, are increasing at an alarming pace: Such incidents can disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile

services. Threats can have different origins including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.

What is the EU approach on all this?

On 5 February, the College of Commissioners adopted the EU Cyber Security Strategy. The Strategy was prepared jointly by the High Representative of the Union for Foreign Affairs and Security Policy Catherine Ashton, Commissioner for Communications Networks, Content and Technology Neelie Kroes and Commissioner for Home Affairs Cecilia Malmström.

The Strategy focuses on an imminent need to step up EU-wide preventive efforts in area of cyber security. It comprises internal market, home affairs and Common Foreign Security Policy angle of cyberspace issues.

The strategy addresses the issue how the Member States can streamline their efforts in this field, and what the EU institutions and agencies can do in order to assist them.

It also seeks to improve horizontal cooperation between different policy areas in the EU: strengthening cyber resilience, fighting with cybercrime, advancing EU international cyberspace policy and dealing with CSDP related cyber issues. By doing so it brings different Cyber communities together and provides for the needed holistic approach.

The strategy stresses that for cyberspace to remain open and free, the EU core values, norms, and principles that we uphold offline must also apply online. Fundamental rights, democracy and the rule of law need to be protected in cyberspace globally.
The Strategy is accompanied by the legislative proposal that aims to strengthen IT risk management as well as advance security of networks and information systems in the EU. It also will contribute to creating a level playing field in cyber security among the EU Member States. When it comes to national cyber preparedness, we have still homework to do in order to achieve EU wide cyber resilience.

The European Parliament in its resolution **of 12 September 2013 has welcomed this strategy . In this resolution it was stressed that** the internet, and cyberspace, has increasing and paramount importance for political, economic,

and societal transactions, not only within the Union but also in in relation to other actors around the world.

And that brings me to the external dimension of the strategy. I like to elaborate on three key issues.

The first element and a priority for EU international engagement in cyber issues will be to uphold our core values in cyber space, in particular the principle of freedom and openness: This is an important element that was outlined in the EU Cyber Security Strategy. We will promote cyberspace as an area of freedom and fundamental rights.

Access to information is easier in the cyber era than ever before. Nevertheless, this access is not always granted in all parts of the world.

Expanding access to the Internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU will implement the number of instruments to achieve this objective. We will work towards the goal of everyone being able to have access to the Internet. We believe that increased global connectivity will advance democratic reforms worldwide.

There is some discussion if and how far the NSA allegations have an impact on this. Let me allow a few words; even if we think these incidents are not strictly speaking a question of cyber security. It is also obvious that we still do not have the full story.

First on the question of surveillance of mass data flow: As you know the EU and the US side are conducting expert meetings in order to discuss the related data protection issues. These continuous consultations will hopefully result in how better to protect privacy in digital age.

Second, the allegations of spying on the diplomatic premises or officials of the EU and its MS raise an issue of trust. On both aspects, the Heads of State and Government of the EU delivered a clear message, in a statement annexed to the Conclusions of the 24-25 October European Council.

I personally do hope that the discussion around these issues will lead at the end to more awareness and transparency.

I think it also shows already now that the EU approach on Cyber security is the right one.

- We have to enhance the awareness of internet users,
- we should further work on network security issues and we
- should stick –may be promote even more- the European approach on privacy and data protection.

Furthermore it is obvious that cyberspace will provide us with a platform to achieve development goals. To reach these goals we have to work together with all actors in cyberspace - companies, governments and civil society, to be able to fully exploit the benefits of technology. We need continued collaboration between all these stakeholders, as well as a transparent and accountable model for undivided Internet.

Second element I like to highlight is that all of us in international society have a **responsibility to preserve cyberspace** as we know it now.

Imposing responsibility is usually easier with recognized actors, so I suggest that states as responsible actors in this new domain, should start by agreeing themselves which actions are allowed and which not, in cyberspace.

For this, the recent initiatives to develop Confidence Building Measures in cyber security offer a valuable set of norms how states will guide their behaviour. States should know whether a cyber-incident was launched accidentally to avoid the threat of miscalculations when retaliating.

For this they should establish cyber communication lines, similar to current nuclear crisis procedures. They should also establish regular exchanges at the policy level and technical level. Trust building and cooperation between all major cyber countries could be complemented by regular cyber talks at the regional and international security forums.

In addition to Confidence Building Measures that aim at increasing general trust, we also should take seriously the commitments that the international society has worked on over the last 150 years.

If conflicts extend to cyberspace, the principles enshrined in International Humanitarian Law should apply.

And **this leads to me third element**. Trust and confidence on ICT depends on knowledge and capacity.

Not all the countries in the world have an equal technical capability, preparedness and legal frameworks to address cyber threats. Many policy-

makers are looking for models for how to structure capacity building efforts, what methods to use and how to measure their efficiency.

Capacity building means constructing safer and more reliable communication networks worldwide. The aim should be to include resilience already in the package when extending communication networks into new markets. Reliable and secure global cyber infrastructure requires also private sector leadership and corporate social responsibility.

The EU intends to engage with international partners and organisations, the private sector and civil society to find the right model to support capacity-building. Cyber resilience in a country depends on preparedness, awareness and cooperation of many players.

All nations should develop a national model, where private and public sector will work together, law enforcement agencies will link up with the incident response community, policymakers and the technical community will elaborate common goals.

The key issue for everyone is investment into training and education. A better cyber future depends on a broad base of e-skills of the public, on computer security knowledge in companies, on special training of IT professionals.

Equally important is to have a proper legal framework in place. An essential part of any national cyber effort is updated legislation to address cybercrime. This includes measures to criminalise offences related to computer crime, and to harmonise minimum penalties with general international practice, while of course ensuring that core values are respected. The Budapest Convention on Cybercrime provides an excellent model that includes all necessary safeguards and conditions for successful cybercrime investigation.

The EU is already engaged in global capacity-building that focuses on enhancing criminal justice and incident response. Together with the Council of Europe we have just started a new global project to build judicial and law enforcement capacity. In next five years, we will increase considerably our financing on capacity building.

And let me now conclude with indicating some elements for a possible way forward. In future capacity building, we need a better coordination of efforts, as well as a sufficient overview on existing initiatives. We also need to bring together the development aid and cyber communities, the public and private sector, technologically advanced and less advanced countries.

The EU will work on a model for how to leverage best practices of countries and the private sector for global cyber security capacity building. We should also look for synergies across many development areas to improve governance, ensure respect of human rights, build infrastructure and provide basic education.

With outlining the EU's global approach to cyber issues, I conclude my remarks today. I will be glad to answer possible questions.

Thank you very much