Opening remarks of the Leader of the Russian delegation Mr.Nikolay R.Kudashev

We are grateful to Korean organizers for hospitality and excellent logistics of the event which we regard to be a joint Korean-Russia initiative.

The substantial expert presence, with our team incorporating information security professionals from the FSS, FPS and Home Affairs Ministry testifies to the importance we attach to this event.

We are absolutely convinced in the specific urgency of the main theme of our today's seminar since cyberterror and cybercrime would not only constitute an independent and extremely dangerous dimension of new challenges and threats to secure trade and sustainable development in the APEC region. But due to accessibility and transboundary nature of the information and communication technologies this threat would rather culminate the dangers of terrorist and criminal activity to political existence of APEC economics.

We began working upon the issues of cybercrime quite a long time ago, accumulated substantial experience. Our professionals are ready to share this experience with You.

We attach utmost importance to the UN-platform where we initiated discussions upon international information security issues and where several important documents put forward by the Russian Federation were adopted.

Among them the UNGA Resolution № 53/70 of 4 January 1999 "Developments in the field of information and telecommunications in the context of international security", draft document "Principles of international information security" of 2000. Russia is very active in the ITU. A resolution №130 upon "Strengthening the role of ITU in building confidence and security in the iuse of information and communication technologies" was adopted in 2006. In November 2009 in Geneva the first meeting of the Group of Governmental Experts on

developments in the Field of Information and Telecommunications in the Context of International Security will be held under Russia's chairmanship.

Lots of effort is being invested in fighting cyberterrorism and cybercrime on the platform of G8, OSCE, CE, CSTO, CIS and EAG.

Serious breakthrough was achieved at the SCO platform where in June 2009 at the Ekaterinburg summit under the Russian chairmanship a Treaty upon cooperation in securing international information security was done meant to be opened to other countries.

Naturally, we highly value the contribution of other countries in raising public awareness and developing the mechanisms of response to cyberthreats. Our today's seminar testifies to this.

Let me now brief You upon our present understanding of the nature and scale of cyberterror and cybercrime threats.

Cyberterrorism = sources – organizations and persons involved in terrorist activities.

Features – the use of information networks for terrorist activity and recruitment; destructive influence upon information resources; undermining the channels of mass communications; abuse of Internet for propaganda of terrorism, creating the atmosphere of fear and panic.

Information crime = sources – persons and organizations involved in illegal use of information resources for criminal purposes.

Features - deliberate intrusion into information systems to undermine their confidentiality; producing and disseminating of viruses; undertaking DOS-attacks; deliberate damaging of information resources; abuse of information resources for criminal purposes (fishing, stealing, extortion, trafficking, child pornography).

We believe cyberterror and cybercrime to be among the most serious challenges to secure and sustainable development of APEC economies. We understand that there could be differing perceptions of their substance, nature and composition. We expect productive exchange of views upon these issues to try to

establish a draft APEC-wide scale of cyberterror and cybercrime threats to secure trade.

Up to now it was mostly different political fora to deal with the issues of cyberterror and cybercrime. Purely economic bodies like the APEC were seldom involved which would not meet the interests of sustainable development and secure trade on the grounds of our Forum.

That's why Russia proposes to continue with the productive exchange of views upon these issue within APEC, work upon the economic dimension of cyberthreats, compare our evaluations of the level and nature of these threats, explore the possibility of establishing within APEC a secure portal for real-time contacts of cyberterrorism experts and monitoring of the situation.

Thus could we call the attention of political fora to the seriousness of cyberthreats to APEC business environment, paving the way for adoption of a comprehensive set of principles for international information security and continuation of discussions on the UN platform for a larger universal treaty to cover the issues of cyberterrorism.

We are most interested to solicite your views upon the points of agenda of the seminar as well as Russia's proposals and would be ready to support the Korean effort and to discuss the possibility of conducting a seminar in Russia on the issues of cyberterror and cybercrime should Your response be positive.