Statement made by the representative of the Russian Federation
at the Facilitation Meeting on WSIS Action Line C5:
Building Confidence and Security in the Use of ICTs
“Partnerships for Global Cybersecurity”

16 May 2006

Mr. Chair, Mr. Secretary,

Confidence and security are acknowledged to be among the main pillars of the Information Society. ICTs are effective tools to promote development, technological progress, peace, security and stability. At the same time, they can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security. Therefore, in accordance with subparagraph “a)” of C5 of Action Line, governments with all stakeholders should consider existing and potential threats to ICTs while addressing information security issues.

In doing so, it is important to examine the issue of international information security, which encompasses, *inter alia*, such interrelated topics as spam, cybercrime, cybersecurity, hostile use of ICTs by states or governments that undermine stability and security of the Internet.

Spam impedes the normal functioning of the Internet, disrupting one of its most important applications – e-mail. It results in significant financial losses, increased time needed to transmit and receive information, decreased capacity, disruption and even blocking of Internet channels. Spam could be used by different actors, such as criminals, terrorists, states and governments as one of the means of hostile activities. Thus, not only the technical characteristics of threats but also their source should be taken into account while considering the implementation of protective measures.

Cybercrime is, in most instances, economically motivated. Every year it brings multibillion-dollar losses. At the same time, some hacker groups have overt political interests and are often found to be related to organized crime and terrorism. Furthermore, hackers may be employed by states or governments to attack other states, including their critical infrastructures.

Cyberterrorism is an extremely dangerous type of terrorism. Terrorists use the Internet as a communication means to identify and recruit potential members of terrorist groups, to collect and transfer funds, to incite, prepare and organize terrorist acts. Telecommunication networks and information systems, which are broadly used today in all areas of life of the society, are an attractive target for terrorists.

Serious concerns are caused by the potential to use Internet means and resources by states or governments to exert hostile military and political influence on other countries. Such potential is a grave threat to international security and stability.

Therefore, in the context of “building confidence and security in the use of ICTs”, we propose to examine the topic of international information security in a comprehensive manner, including the issues of cybersecurity, spam, the threats of cybercrime, cyberterrorism, and hostile use of the Internet infrastructure and potential by states or governments.