

FSC-PC.DEL/31/10  
10 June 2010

ENGLISH  
Original: RUSSIAN

Delegation of the Russian Federation

**STATEMENT BY MR. S. SHESTAKOV,  
REPRESENTATIVE OF THE RUSSIAN FEDERATION, AT THE  
JOINT MEETING OF THE OSCE FORUM FOR SECURITY  
CO-OPERATION AND THE OSCE PERMANENT COUNCIL**

2 June 2010

Mr. Chairperson of the Permanent Council,  
Mr. Chairperson of the Forum,

I should like first of all to thank the organizers of today's meeting for the attention they are paying to a comprehensive approach to enhancing cyber security.

We do not doubt the importance of this problem and believe that as many countries and organizations as possible should be involved in solving it.

As you are aware, a significant step has already been made. The main work in this area is being undertaken within the United Nations. The 63rd session of the United Nations General Assembly adopted resolution 63/37 "Developments in the field of information and telecommunications in the context of international security", in accordance with which the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security began its work. The Secretary-General's report for the 65th session of the General Assembly in 2010 is to be prepared on the basis of the results of the Group's work. This resolution was adopted by consensus in 2009.

In this connection, I should like once again to set out the basic approaches of the Russian Federation as regards the formation of an international information security system.

The possibility of information and communication technologies (ICT) being used for purposes that have nothing to do with ensuring international stability and security is our main concern when it comes to ensuring international information security. A most important task in this respect is limiting the threat of information weapons being used against critical State structures (the damage is on a par with a military attack) and the hostile use of ICT as a means of inter-State confrontation for both political and military purposes as well as the threat of criminal and terrorist activities in the information sphere.

From this point of view, cyber security is an important component of a more general concept – information security, meaning the protection of the interests of States and international organizations associated with the use of modern ICT.

Faced with the dishonest use of ICT, we firmly believe that in dealing with the problem of international information security we need to counter three main threats – of a politico-military, criminal and terrorist nature.

At the same time, priority should be given for now to the discussion of the problems involved in countering the politico-military threat from the use of ICT to achieve political goals by applying pressure on the leadership of other countries.

ICT is acquiring the attributes of a weapon. Its specific feature is its ability to be used across borders.

Without referring to specific examples, we can conclude that the use of ICT to exert forceful pressure can give rise to situations that could threaten international peace and security.

The specific feature of this threat is the hidden and anonymous nature of the preparation and conduct of hostile activities, and the difficulty in preventing and responding appropriately to such actions.

In this regard there is an objective need for the peaceful processes involved in civilian and military information technology to be regulated by international law and for an agreed international platform to be developed with respect to information security. We need to begin the process of moving the international community towards the joint elaboration of a genuinely universal document under international law, noting the existence of a whole range of threats in the area of information security and providing for appropriate measures to restrict and combat them through joint efforts.

The results of the work of the 12th United Nations Congress on Crime Prevention and Criminal Justice held in the Brazilian city of Salvador from 12 to 19 April 2010 were significant in this regard. Most countries are working towards the drafting of a universal international convention with the participation of all interested States. A universal document of this kind could resolve quite a number of fundamental questions that have not been properly reflected in the Council of Europe Convention, notably safeguarding the national sovereignty of participating States and the observance of the rights of their citizens while simultaneously guaranteeing the effectiveness of international co-operation in preventing and suppressing ICT-related crime. The convention should cover all the possible constituent elements of such crimes, provide for adaptation to new forms of crime in cyberspace and meet the expectations of developing countries in terms of providing them with technical assistance in the development of equipment and methods for combating what is for them a new criminal threat.

The convention might also spell out commitments on the part of the private sector and companies involved in ICT with access to massive databases and playing an increasingly important role in protecting their clients against attacks on their personal data, property and private life.

Ensuring international information security has a firm place on the agenda of a number of prestigious international forums, including the Collective Security Treaty

Organization (CSTO), the Council of Europe, the G8, the International Telecommunication Union and the Internet Governance Forum.

The problem of international information security has also been mentioned in the Forum for Security Co-operation and Permanent Council of the Organization for Security and Co-operation in Europe.

The most significant recent development for us was the signing on 16 June 2009 at the Shanghai Co-operation Organization (SCO) summit in Yekaterinburg of an agreement between the governments of the SCO Member States on co-operation in ensuring international information security. The purpose of this agreement is to create the political, legal and organizational foundations for strengthening confidence and developing co-operation among the parties and relevant national agencies concerned with international information security. The agreement identifies the existence and essence of specific threats with respect to international information security as well as the basic areas, principles, forms and mechanisms of co-operation among the parties in this field. It is open to accession by other States.

Expanding the basis under international law for co-operation among States in this area, Russia and Brazil signed an agreement on co-operation on international information security this May.

There is no doubt that we should continue joint work to assist the international community in its efforts to establish an international information security system.

It is essential that we discuss the existing problems in a common language. I am referring here to the terminology used. We already have positive experience within the SCO and the CSTO. We are looking forward to the results of the work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

In our view, it is also important to step up international co-operation with a view to strengthening Internet security. We believe it is necessary to internationalize Internet governance, to ensure that States are equally involved in the governance of this global information network and that they exercise their sovereign right to independent governance of the Internet at the national level, to increase the role of the International Telecommunication Union in Internet governance and to guarantee the continuity, security and stability of its functioning. We believe that the Internet Governance Forum will continue to play a positive role in this process.

In conclusion, I should like once again to draw attention to the importance of a comprehensive approach to the problems under discussion and to thank all those present for their attention.