PC.DEL/956/18
12 July 2018

ENGLISH
Original: RUSSIAN

Delegation of the Russian Federation

STATEMENT BY MR. ALEXANDER LUKASHEVICH, PERMANENT REPRESENTATIVE OF THE RUSSIAN FEDERATION, AT THE 1192nd MEETING OF THE OSCE PERMANENT COUNCIL

12 July 2018

On the Digital Geneva Convention

Mr. Chairperson,

We have listened with interest to the report by the Vice President of the Microsoft Corporation, Mr. John Frank, on the work undertaken to elaborate the Digital Geneva Convention. The signing of an agreement by 40 leading high-tech companies is without a doubt an important step towards the finalization of that document. Unfortunately, Russian companies were not involved. We should like to remind you of the Information Security Charter drawn up by the Nornickel company and presented at the 12th International Forum "Partnership of State Authorities, Civil Society and the Business Community in Ensuring International Information Security" held in Garmisch-Partenkirchen from 16 to 19 April this year and supported by the participants. That document presents a code of business conduct specially for corporations and the private sector.

A number of questions arise in this connection. How and on what platform does Microsoft intend to proceed in future with its convention and what status does it expect it to have? We trust that this initiative is not an attempt to establish a non-proliferation regime for cyberweapons, similar to the Treaty on the Non-Proliferation of Nuclear Weapons, in which a designated group of States would not have the right to develop and use cyberweapons, which in effect would sanction the start of an era of cyberwarfare. We would remind you that only the United Nations Security Council has the authority to qualify a particular situation as a threat to international peace and security.

Safeguarding international information security is one of the key priorities of the Russian Federation in the field of inter-State co-operation. The influence of information and communication technology (ICT) on all aspects of the life of people, society and the State cannot be overestimated. Apart from the obvious positive aspects, the active use of digital technologies carries new risks for national and international security.

Cybersecurity is becoming an increasingly acute problem on a global scale. Not only individuals and legal entities but also entire States can become the victims of incidents in the digital environment.

According to the World Economic Forum, damage to the global economy as a result of cybercrime in 2017 amounted to over 1 trillion US dollars and by 2022, if effective and impactful measures are not taken, this figure could reach 8 trillion.

These massive threats can be neutralized only by pooling the efforts of the international community as a whole. Combating these threats is the task of States and its success is contingent on combining the efforts of law enforcement authorities, the business community and non-governmental organizations. It would be a mistake to make it the responsibility of private companies alone. The State and its competent authorities are responsible for security.

It is important to elaborate a single set of rules of the game and common international standards that would take maximum account of the rights and interests of all States and would be universal and accepted by all.

We believe that the universal rules should be drafted within the framework of the United Nations in accordance with its central and co-ordinating role in this process, with existing international law being adapted at the same time with account taken of the specific aspects of cyberspace. The application of existing norms to the new situation would be counter-productive. There is a need for new concepts and a clear definition of the threats and ways of combating them.

We have consistently called on international platforms for a concept for preventing politico-military conflicts in cyberspace, the non-use of force in this area, and respect for the principles of national sovereignty and non-interference in internal affairs.

Russia is already planning to present a draft resolution in the First Committee of the 73rd Session of the United Nations General Assembly to strengthen the code of conduct of States in cyberspace. The preamble includes an initial list of rules of responsible behaviour by States in cyberspace elaborated on the basis of corresponding recommendations from the consensus-based reports by the United Nations Group of Governmental Experts (GGE) on International Cybersecurity in 2010, 2013 and 2015.

It sets forth a whole set of fundamentally important rules of behaviour for States in cyberspace, including the following commitments:

– Use of ICT exclusively for peaceful purposes;

– Alignment of international efforts to prevent conflicts in this area;

– Observance of the principles of the Charter of the United Nations, including the sovereign equality of States, the non-use of force or threat of force, and non-interference in the internal affairs of States;

– Avoidance of unfounded accusations of malicious use of ICT and provision of evidence to support any accusations;

– Non-use of intermediaries for cyberattacks;

– Prevention of the spread of malware and malicious hidden functions ("backdoor components").

Our aim is to have these proposals made universal through approval by the UN General Assembly, which would make it possible to establish a basis for regulating the action of States in cyberspace in the form of "soft" legal norms.

There is provision in the operative part of the resolution for the creation of a new GGE in 2019 to draft, correct and enlarge this initial list of norms of behaviour. Its mandate also provides for studying the possibility of organizing regular institutional dialogue on cybersecurity under the aegis of the UN with participation of a wide range of States. This will permit the definition of the best negotiating format for future discussions of this issue in the UN.

We are also convinced of the usefulness of co-operation on safeguarding international cybersecurity at the regional level. We call for the OSCE's role in preventing security incidents involving ICT to be strengthened. The Organization could provide a platform for direct dialogue with a view to preventing incidents from developing into direct confrontation.

We see the adoption of ICT confidence-building measures within the OSCE as playing a special role.

We attach great importance to co-operation with the business community in the area of cybersecurity. The International Cybersecurity Congress organized by Sberbank Russia was held in Moscow on 5 and 6 July and attended by over 2,000 delegates from 51 countries. The meeting was opened by Vladimir Putin, President of the Russian Federation, who outlined Russia's basic approaches to ICT.

At the national level, we are seeking to devise comprehensive solutions to prevent and put an end to cybercrime directed at citizens, to implement business initiatives to create a system for the automated exchange of information on threats in cyberspace, develop home-grown technologies, and improve the system of international exchange of information on cyberthreats.

In conclusion, I should like to stress that the Russian Federation intends to continue contributing to safeguarding cybersecurity. We are willing to participate in constructive dialogue in international and regional formats and at the bilateral level.

Thank you for your attention.