The OSCE Secretariat bears no responsibility for the content of this document and circulates it without altering its content. The distribution by OSCE Conference Services of this document is without prejudice to OSCE decisions, as set out in documents agreed by OSCE participating States.

PC.DEL/887/22
16 June 2022

ENGLISH
Original: RUSSIAN

Delegation of the Russian Federation

STATEMENT BY MR. MAXIM BUYAKEVICH, DEPUTY PERMANENT REPRESENTATIVE OF THE RUSSIAN FEDERATION, AT THE 1378th MEETING OF THE OSCE PERMANENT COUNCIL

16 June 2022

On massive cyberattacks against Russia

Mr. Chairperson,

Ever since its appearance in the international arena, the topic of international information security has been a unifying one. The first resolution on this score, adopted in 1998 at the initiative of Russia, drew the international community’s attention to the threats emanating from cyberspace. As proposed by the Russian Government, the first relevant discussion mechanism was set up, namely a United Nations Group of Governmental Experts. The widespread interest shown by countries in issues related to security in the use of information and communication technologies (ICTs) prompted the launching – again at the initiative of Russia – of a United Nations Open-Ended Working Group in 2018, which enabled broader participation by Member States and involved representatives of business and academia in its work. It likewise proved possible to put another idea of ours into practice, namely the establishment of a United Nations special committee tasked with elaborating a universal convention on combating cybercrime. Of course, an important milestone was the development here at the OSCE, as urged by us, of a set of confidence-building measures to enhance inter-State co-operation, transparency and predictability and to reduce the risks of misperception, escalation and conflict that might stem from the use of ICTs. All this allowed the international community to advance towards a common understanding of the rules of behaviour in this field and towards the tackling of emerging threats.

However, more than 20 years later – and this has become especially noticeable in the past few months – it is the position of the Western countries that is the main obstacle to success in international negotiations and to the achievement of real progress in the development of a just international legal framework for the regulation of information space. The United States of America and its allies from the very outset chose the path of asserting the right of the stronger and imposing unilateral rules that are not only not aimed at preventing conflicts and criminal acts but in effect encourage these in every possible way. They did so seeking to conceal their offensive operations and to consolidate, by fair means or foul, their dominance in the field of international information security. Instead of facts and constructive negotiations, the United States has opted for the rhetoric of unfounded accusations backed up by nothing whatsoever, the most blatant falsifications and unilateral sanctions.

Translation by OSCE Language Services

Mr. Chairperson,

We are concerned about the continued exponential rise in cyberattacks against the information infrastructure of Russia carried out from the territory of certain participating States, above all the United States, Ukraine and a number of EU member countries. Systematic work is under way to militarize cyberspace; irresponsible attempts are being undertaken to turn it into an arena of inter-State confrontation, thereby increasing manifoldly the threat of large-scale confrontation which is fraught with unpredictable consequences.

This is being facilitated by the development by Western countries, first and foremost the United States, of tools for conducting cyberattacks against the critical infrastructure of other States. There are, unfortunately, numerous examples of such tools having been put to practical use. Our country was subjected to the most intensive attacks during such landmark events as the Olympic Winter Games in Sochi in 2014 and the 2018 Football World Cup, and during elections – in particular, the 2021 elections to the State Duma of the Russian Federation. According to the information available, the overwhelming majority of these attacks were committed from US territory. It is also important to note that groups of hackers from other countries were enlisted to participate in these illegal and dangerous campaigns as well.

Since February 2022, massive co-ordinated distributed denial of service attacks have been carried out against Russia, in which more than 65,000 “home-grown hackers” from the United States, Ukraine, Poland, Germany, Georgia and other countries regularly take part. Twenty-two hacker groups are involved in these illegal operations, the most active being the IT Army of Ukraine (Ukraine), GhostClan (United States), GNG (Georgia) and Squad 303 (Poland). The software installed on the servers of the cloud providers Hetzner (Germany) and DigitalOcean (United States), the specialized platforms War.Apexi.Tech and Ban-Dera.com and the online capabilities of the IPStress.in and Google servers are being actively used for these purposes. It is not only the information resources of Russian government agencies that have been hit but also those of numerous Russian companies, including Yandex, Sberbank, Gazprom, Lukoil and the airlines Rossiya, Aurora, Yamal, NordStar, Smartavia and Yakutia.

Separate mention should be made of a recent pronouncement by the Deputy Prime Minister and Minister of Digital Transformation of Ukraine, Mykhailo Fedorov, in an interview with the Spanish newspaper *El País*. He announced with great fanfare the creation of “a cyberarmy numbering 300,000 hackers”, a world first. In other words, a mass mobilization of cybercriminals is under way for the purpose of undermining the operation of Russian critical and social infrastructure. “Digital interventions” of this kind can disrupt the functioning of government agencies and healthcare, transport, financial and energy sector enterprises, and have detrimental consequences for the citizens of our country. This is effectively a question of encouraging “technological terrorism”. We are convinced that there is no way that such a “cyberfront” could have been opened by Ukraine at short notice and using its own resources. It is evident that preparations for it, involving external technical assistance, had been going on for a long time before. There can be no doubt that it will not be possible to order these hackers to demobilize and that the skills they acquire in the use of ICTs for combat purposes will lead to even greater destabilization and multiplication of hacker threats in Europe and throughout the world.

In closing, we should like to recall that we advocate the preservation of peace and security in the information space in complete conformity with the generally recognized principles and norms of international law enshrined in the Charter of the United Nations – in particular, the non-use of force or the threat of force, non-interference in the internal affairs of other States and respect for national sovereignty, among others. As before, we consider it important to develop rules, norms and principles for responsible behaviour by States in the use of ICTs and to endow these with a legally binding status so as to prevent inter-State conflicts in the digital sphere. It is necessary to make more active use of the OSCE’s existing toolbox of confidence-building measures to eliminate emerging threats – even in a context where such confidence has been heavily eroded through the efforts of certain Western countries.

Thank you for your attention.