

**Постоянное
представительство
Российской Федерации
при Организации
Объединенных Наций**



**Permanent Mission
of the Russian Federation
to the United Nations**

136E 67th Street

New York, NY 10065

Phone: (212) 861-4900

Fax: (212) 628-0252

517-7427

S T A T E M E N T

**BY AMB. ANDREY KRUTSKIKH,
SPECIAL REPRESENTATIVE OF THE PRESIDENT
OF THE RUSSIAN FEDERATION FOR INTERNATIONAL
COOPERATION IN THE FIELD OF INFORMATION SECURITY
AT THE FIRST SESSION OF THE UN OPEN-ENDED WORKING
GROUP ON DEVELOPMENTS IN THE FIELD OF INFORMATION
AND TELECOMMUNICATIONS IN THE CONTEXT
OF INTERNATIONAL SECURITY**

New York, 3-4 June 2019

Unofficial translation

Check against delivery

Distinguished colleagues,

I would like to congratulate everyone on the opening of the first-ever session of the UN Open-ended Working Group (OEWG) on International Information Security (IIS) and express gratitude to the UN Office for Disarmament Affairs and, personally, to Under-Secretary-General and High Representative for Disarmament Affairs Ms. Izumi Nakamitsu for its organization.

We congratulate Switzerland on its election as the Group's Chair. This places an important and responsible burden on its shoulders. Switzerland will undoubtedly leave its mark in the history of the United Nations as a country that led the work of the first OEWG. Russia wishes the Chair success in this challenging work and expresses its full readiness to contribute to the effectiveness of the Group's activities.

I regret to note that, while the international community is trying to establish an effective dialogue on IIS within the United Nations, the situation in the use of the information and communication technologies (ICTs) is becoming more and more tense.

Malicious use of ICTs poses a threat of violation of states' sovereignty and interference into their internal affairs.

The greatest danger is that incidents online can lead to a full-scale war offline. The doctrine of so-called preventive cyber strikes promoted by a number of countries poses a real threat to international peace and security. This doctrine considers the use of force a legitimate response to potential cyberattacks. In our view, such an approach is inadmissible. We need to avoid the situations when a state independently and without any evidence determines a potential source of threats stemming from the use of ICTs and carries out a devastating punitive strike as it deems fit.

Unfortunately, some states have already put this concept into practice. They do so without appropriate authorization of the UN Security Council, bypassing the UN Charter. The accused party has no chance to protect its rights through legal action. Is this what the applicability of international law to information space is about? ~~On the contrary, such steps lead to the establishment of a dictate and rule of force in digital field and undermine trust between states.~~

Today the social and economic progress is totally dependent on the ICTs. They set the pace for the development of almost all innovative industries: digital economy, artificial intelligence, the Internet of Things, unmanned vehicles, smart cities, telemedicine and other products of the technological revolution. However, all of these achievements are nowadays critically vulnerable in the face of IIS threats and remain hostage to this unsolved political problem.

Yet these days technological progress in the field of ICTs is a privilege of the developed countries. Others get not its profits but its residue. For instance, developed countries, concerned about their environment, take their electronic waste to the developing countries for disposal, instead of rendering them real assistance in building their own digital potential. Thus, the developing states basically become hostage to the cyber neocolonialism policy. At the end of the day, this limits their capacity to protect their citizens, businesses and sovereignty as a whole.

The use of ICTs for criminal purposes is another acute problem. According to UN Secretary-General António Guterres, in 2017 the world economy's official losses resulting from actions of carried out by criminals with the use of ICTs amounted to 1.5 trillion US dollars. As estimated by the World Economic Forum, by 2022 this figure could reach 8 trillion US dollars and exceed the total income from the use of the Internet.

We believe that the above-mentioned challenges should be addressed under the UN auspices with an active involvement of all members of international community. Thanks to the efforts of more than 100 countries, today we have a real

chance to bring the IIS negotiation process within the UN to a qualitatively new level.

We welcome the fact that, starting from this year, the IIS discussion within the UN will be held in two formats instead of one. We see no obstacles to the ~~OEWG and GGE productively working in parallel.~~

It is important to ensure that this process is complementary, non-confrontational, constructive and based on cooperation. We think it is necessary to harmonize the efforts on the two platforms. To achieve this, discussions should be pragmatic, non-politicized and produce results that would be mutually reinforcing rather than conflicting. We would like to underline that we are looking forward to a fruitful and peaceful dialogue.

We approached the American side with these proposals as early as last autumn. And though there has been no response thus far, we hope that the US share our vision on constructive collaboration between the OEWG and the GGE.

As for the OEWG, it has an extensive agenda to work on. The Group's mandate encompasses more issues than have ever been included in the traditional mandate of the UN GGE on IIS. Some of them will be addressed within the UN for the first time ever. Though the essential feature of the OEWG is that it is not just a forum for an expert exchange of views but a General Assembly body for achieving concrete solutions. Besides, it is currently the most representative IIS mechanism within the UN.

This entails particular responsibility for the Group. If it proves incapability to reach an agreement on fundamental issues related to ensuring IIS, demonstrates its passive position or limits itself to strictly formal approach to its mandate, this will mean a failure not just for individual countries but for the entire international community.

One should not cherish hope that they can wait out the storm in their safe harbor, which will be unaffected by global IIS challenges. This is but a dangerous illusion. Unlike traditional security challenges, IIS threats are "the great equalizer", which makes all international players equally vulnerable, regardless of their

political stance and level of technological development. We call on all states to exercise their sovereign right and most actively engage in the OEWG-led negotiations, adopting a constructive approach and showing commitment to reaching a compromise.

~~I would like to elaborate on the OEWG priorities as we see them. The~~ Group will launch its discussion on IIS issues not from scratch; therefore, it will undoubtedly have to consider the results of previous pertinent GGE efforts. Russia, when submitting the draft resolution together with other co-sponsors last year, proposed to focus the OEWG mandate on the issues that had already been discussed by the GGE, and suggested that all countries which had never participated in the GGE would be invited to join the discussion.

I am talking of four traditional issues.

1. Rules/norms of responsible behavior of states in information space.

This is an absolute priority on the international agenda. Last year, the General Assembly for the first time approved by a vast majority the initial list of such rules/norms. This is a real breakthrough for the international community. Nothing like that has ever been approved anywhere. The list provides for measures to prevent conflicts in the digital sphere and enshrines the principles of the non-use of force, respect for state sovereignty, non-interference in internal affairs of other states, and fundamental human rights and freedoms. Once again, these rules/norms have been supported by the majority of UN Member States.

We believe that as a next step in line with the OEWG mandate we should continue our work on this list so as to make it comprehensive and search for ways to put it into practice. This would allow us to make these rules/norms universal. We seek for reaching consensus while discussing these issues consequently adopting a UNGA resolution on IIS in 2020.

2. Confidence-building measures in the digital sphere. Drawing on the regional experience, particularly that of the OSCE and the ASEAN Regional Forum (ARF) on security issues, the Group could consider ways to develop a global set of such measures. We may also wish to think about unifying under the

UN umbrella the confidence building measures agreed at the regional level and adopt universal criteria for their further elaboration.

3. Future discussions on IIS within the UN. Today, it is clear that this issue has become an integral part of the UN agenda. It is high time we discussed ~~ways of giving it a new status — as an idea, establishing a permanent entity under~~ the UN auspices.

4. Digital capacity building. By failing to provide necessary support to countries affected by the digital divide, we basically leave them to stand against IIS challenges on their own. How can we expect them to engage in resolving global IIS issues to the same extent as other, more technologically advanced states? Issues of technical assistance should become a priority in our discussions.

More specifically, Russia proposes the following concept for the OEWG's work.

It should focus on preparing a substantive final report containing recommendations to the UN Member States with regard to the above issues and reflecting all opinions expressed in the course of discussions within the OEWG.

In order to make these recommendations universal, consensual and politically meaningful, we propose to draw up on their basis an updated UNGA draft resolution on IIS as an annex to the report that will be recommended for adoption by the General Assembly at its 75th session in 2020.

The basis for these documents is already in place, including the GGE's reports on IIS for 2010, 2013 and 2015, as well as annual UNGA resolutions ("Developments in the field of information and telecommunications in the context of international security"). Regional platforms (OSCE, ARF) can also provide valuable inputs.

To implement these objectives, we should launch an intensive negotiation process to be completed within a short timeframe.

We propose that, at its second session in September 2019, the OEWG hold a general discussion on issues that fall within its mandate.

We believe it advisable to distribute a zero draft of the report, including the abovementioned draft resolution, on behalf of the Chair of the OEWG by October 2019. It will allow Member States to work on these drafts in between sessions (between the 2nd and the 3rd sessions of the OEWG) to finalize the text at the ~~Group's third session in February 2020 and "polish it" and to sum up the results of the meeting at its last session in July 2020.~~

If we follow this scenario, in the fall of 2020, the Chair of the OEWG, on behalf of the Group's member states, could present the report and the draft resolution for adoption at the 75th session of the UN General Assembly.

We believe that such tactics will allow us to take into account the experience of previous GGEs on IIS and the UN General Assembly First Committee, where there were too many disagreements and too little time to find consensus and get to working on the text.

By doing so, the OEWG will be able to demonstrate tangible practical results of its work. This will not only provide basis for the General Assembly to adopt universal decisions in this field but, in fact, launch a continuous negotiation process on IIS within the United Nations.

Certainly, the proposed tactics will require great effort on the part of all participants, especially the Chair. But we should walk this path if we really want to achieve results. For our part, we are ready to do everything possible to facilitate this work.

Thank you.