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

136E 67th Street

New York, NY 10065

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

Phone: (212) 861-4900

Fax: (212) 628-0252

517-7427

S T A T E M E N T S

BY HEAD OF THE RUSSIAN INTERAGENCY DELEGATION TO THE FIRST SUBSTANTIVE SESSION OF THE UN OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF ICTS 2021-2025, DEPUTY DIRECTOR OF THE DEPARTMENT OF INTERNATIONAL INFORMATION SECURITY OF THE MINISTRY OF FOREIGN AFFAIRS OF THE RUSSIAN FEDERATION DR. VLADIMIR SHIN

New York, 13-17 December 2021

Unofficial translation

Check against delivery

13 December 2021

On agenda item 3 "Organization of work":

Distinguished Mr. Burhan Gafoor, Chair of the UN Open-ended Working Group,

Distinguished colleagues,

Ladies and gentlemen,

I am sincerely glad to welcome all the participants of the first substantive session of the UN Open-ended Working Group (OEWG) on security of and in the use of ICTs 2021-2025. You know, initially I was going to take the floor a bit later and I was going to say that the outgoing year had become a turning point in the global discussion on information security, since the final reports of the first OEWG and of the Group of Governmental Experts had been agreed upon by consensus, as well as the relevant Russia-US draft resolution had been adopted by the UN General Assembly with a record number of 108 cosponsors without a vote. I was going to say that we expected that these achievements and the overall constructive atmosphere would allow us to have a successful current session. However, in the context of something that looks like a well-orchestrated massive attack aimed at disrupting the start of the work within the Group, I have to react as discussions go and, in response to the statements we heard from distinguished colleagues, I would like to say the following.

Let me start in a roundabout way. We supported the distinguished Mr. Chair who proposed to hold our meetings in a fully in-person mode. In our view, the in-person mode of negotiations enriches our opportunities to find "points of convergence" and opens the way for genuine diplomacy. At the same time I regret to note that considerable part of the Russian interagency delegation did not have an opportunity to come to New York since the authorities of the host country delayed the issuance of visas till the very end, while some members of the delegation did

not obtain them at all. And we know that we are not the only ones who find themselves in such a situation, and some of our foreign colleagues were in the same position.

We regard such a situation as absolutely inadmissible and unacceptable. We will counter any attempts to limit the right of states to participate in the negotiation process within the OEWG. We call on the American side to refrain from projecting our bilateral divergences onto global negotiations, as well as from abusing its status of the country hosting the UN headquarters, employing it as a political leverage. We would appreciate if the UN Secretariat could share its considerations on how to avoid such situations in future, given that the Group will work for five years in accordance with its mandate.

I had to react to the visa situation, inter alia, in the context of the ongoing discussion on stakeholder participation in the Group's work. We presume that ensuring full-scale participation of States in the OEWG negotiation process should be a priority. This is a starting point for our work, and then, as we solve this situation, we can consider other issues including those on interaction between the Group and NGOs.

The Russian Federation presumes that the OEWG work should be based upon its mandate enshrined in the UNGA resolution 75/240 of 31 December 2020 and confirmed by the UNGA resolution 76/19 of 6 December 2021. The Group adopts any decisions solely by consensus. While defining modalities of interaction between the new OEWG and other stakeholders, we believe that it is necessary to strictly follow the para 4 of the operative part of the resolution 75/240 which stipulates that the OEWG *may* – I repeat, *may – decide to interact, as appropriate, with other interested parties*. The OEWG mandate which was enshrined, I repeat, in the 2020 resolution and confirmed by consensus by the 2021 resolution, does not imply stakeholder engagement in the sessions, as well as any obligations to interact with them.

Nevertheless, from the very beginning, since 2018, the Russian Federation presumed the necessity of broadening dialogue between states, as main participants

of our process, and all the other stakeholders which are competent in the issues of ensuring security in the use of ICTs. As you recall, in this context, accordingly to the resolution 73/27 of December 2019, there was a two-day intersessional consultative meeting with stakeholders, and all the interested NGOs could present their initiatives at this event.

We insist that we should, first and foremost, guarantee the integrity and implementation of the OEWG mandate enshrined in the UNGA resolution 75/240. We face a very serious challenge of achieving concrete and tangible results every element of the mandate, and the States bear primary responsibility for the outcomes of our Group. We should focus on realizing this tasks and not on secondary issues. If there is an unlimited access of stakeholders to participation in the OEWG official sessions, the States will simply not have enough time for interventions. The discussion will risk losing its substantive character, and the process can become unmanageable.

According to the UNGA Rules of Procedure, the NGOs willing to intervene within the General Assembly or the Security Council should pass through the silence procedure, and the States are not obliged to explain their decisions on participation of such organizations. The same practice should be applied in the OEWG being a subsidiary body of the UNGA. All the NGOs interested in interstate negotiation process on information security can follow formal OEWG meetings via online broadcast. If they want to express their opinion on any matter of discussion, they can send their written contributions to the Chair which will distribute them for consideration of States, as well as they can present them at intersessional consultative meetings.

As we see, a number of States, inter alia, Australia, Czech Republic, Finland, have already presented their initiatives on holding meetings with participation of other stakeholders on the margins of the first substantive session. We believe that this is quite sufficient level of NGO participation in our work these days. During intersessional activities we could engage other bodies of the UN to work with stakeholders, for instance, the United Nations Institute for Disarmament

Research (UNIDIR). We believe that in this way the UNIDIR could largely contribute in our work.

While considering this topic further, we would like to remind that, as opposed to the first OEWG, the mandate of the current Group does not imply holding intersessional consultative meetings with other stakeholders. However, in the spirit of our constructive approach towards participation in the process, we are ready to support the Chair's proposal to organize the work with NGOs in this format, inter alia, by increasing number of such meetings.

We will express our opinion on this issue further, but now I would like to call on all our colleagues to support the Chair in his vision of modalities of interaction between the OEWG and stakeholders and to start substantive discussions at the first substantive session.

Thank you for your attention.

On agenda item 4 "General exchange of views":

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

We welcome the OEWG Chair's decision to proceed to discussing substantive issues on the agenda of the current session.

The Russian Federation presumes that the mandate of the OEWG enshrined in the UNGA resolution 75/240 of 31 December 2020 and confirmed in the UNGA resolution 76/19 of 6 December 2021 should serve as a basis for its activities. The Russian proposal to ensure the continuity and uninterruptedness of the negotiation process within the universal and democratic OEWG format guaranteed once again an opportunity to participate directly in the decision-making process under the principle of consensus to all the States.

The OEWG mandate defines as a priority further development of rules, norms and principles of responsible behaviour of States and of the ways for their implementation. We presume that this aspect of work requires particular attention, given the growing threats and challenges in information space. This puts on our

agenda the need to gradually move from non-binding, recommendatory norms to developing and agreeing upon clear and equal rules of behaviour for all states in information space and making them legally-binding. We stand ready to make concrete contribution to our work in this area.

During the work of the first OEWG the States presented a considerable number of national proposals and contributions on rules, norms and principles of responsible behaviour of States. Not all of these suggestions were agreed, and part of them were compiled in the Chair's summary under the presumption that their consideration would be continued in the new Group.

As long as the OEWG was established under the auspices of the UNGA First Committee, which is in charge of disarmament and international security issues, it is the aspects of ensuring security in the use of ICTs that should be the Group's focus. A possible significant dimension of our efforts may be the elaboration of legal and practical mechanisms of cooperation that would contribute to creating a system of international information security based on the principles of conflict prevention and promotion of peaceful use of ICTs.

The OEWG should become a platform not just for discussions, but for pragmatic negotiations aimed at achieving tangible results. It is important to provide for an in-depth and thematically specialized discussion to ensure a more thorough consideration of every element of the Group's mandate. We agree with the programme of work at the first substantive session proposed by the Chair and we support its adoption as soon as possible.

Given that the mechanism will function for five years, it should be flexible enough and able to adapt to demands of international community. In order to optimize the process, agreements can be formalized once they are reached, without waiting for the Group's mandate to expire.

I wish to representatives of all states successful and fruitful work. Thank you for your attention.

Within thematic discussion on existing and potential threats:

Distinguished Mr. Chair,

I thank you for the opportunity to address the floor on such an important issue of existing and potential threats in the use of ICTs and possible cooperative measures to prevent and counter such threats.

In our view, some of the acute challenges in the sphere of information security are the threats related to the use of ICTs:

– in military-political and other spheres to undermine (compromise) State sovereignty and violate territorial integrity of States;

– for terrorist and extremist purposes, inter alia, to propagate terrorism and extremism and to recruit new supporters to these activities;

– for criminal purposes, inter alia, to commit crimes in the sphere of computer information, as well as to commit various kinds of fraud;

– for perpetrating computer attacks aimed at information resources of States, inter alia, at critical information infrastructure, as well as unauthorized interference in information resources;

– for interfering in internal affairs of States, violating public order, inciting national, racial and confessional hatred, propagating racist and xenophobic ideas and theories provoking hatred and discrimination, inciting violence and instability, as well as for destabilizing internal political and social and economic situation, for disrupting State governance;

– for disseminating information which is harmful for public, political and socio-economic system, spiritual, moral and cultural environment of States.

Considerable vulnerabilities that were detected in recent years in remote control systems and in settings of parts of server equipment and of support services, enabling amplified computer attacks, prove that individuals and terrorist groups have actually got the tools which are comparable with those of States.

Yet another threat is the use of technological dominance by some States in global information space in order to monopolize the ICT-market, to limit other

States' access to advanced technologies and to increase their technological dependence from States dominating in the area of information and deepen information inequality, also represent a threat. The issue of some States dominating normative and legal regulation of activities of global IT-companies remains unsolved.

The international community should organize a profound discussion and analysis of multiple factors contributing to escalation of threats, including the anonymity of activities in information space.

For the sake of countering existing and potential threats it is necessary to move towards the formation of global system of international information security under the UN auspices based upon the principle of equal security of parties and peaceful resolution of interstate disputes arising from the use of ICTs.

Among particular topics that require attention we would like to highlight the issues of personal and other data protection. Determining and further adopting principles of personal data processing which are common for all the UN Member States will allow us to increase the level of personal data protection during the correspondent transborder exchange and will promote development of legislation in the sphere of personal data protection in States where such legislation is not developed enough or does not exist at all.

Thank you for your attention.

15 December 2021

Within thematic discussion on rules, norms and principles of responsible behaviour of States:

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

In accordance with the OEWG mandate, further development of rules, norms and principles of responsible behaviour of States is the priority aspect of our joint efforts.

It is necessary to continue to develop comprehensive universal list of rules, norms and principles of responsible behaviour of States in information space, since the rules of behaviour agreed in the past are not sufficient for full-scaled regulation of the ICT-sphere, given rapid technological progress and ICT-development.

In this context it is puzzling that some countries insist on preserving exclusively voluntary character of the rules mentioned above. In the current situation, when national security of States depends on global information security, such a proposal is as provocative as if someone would propose to make traffic rules a voluntary matter. This would suit only those driving tanks – in other words, those who advocate "rule of force" and try to legitimize it.

On the contrary, for the moment more and more members of international community, first of all developing countries, touch upon the issue on the necessity to ensure international legal regulation of the ICT-sphere. In their view, international law should be adapted to this particular domain through elaborating a code of clear, equal and obligatory "rules of the game".

In this regard Russia sees a scenario of the Group's work in this dimension as follows. In short-term perspective, we presume that it is reasonable to survey the existing list of norms enshrined in the UNGA resolution 73/27 on the basis of the recommendations from the 2015 GGE report and to undertake further efforts to enlarge this list. It is also important to consider the prospects of universalization and increase of status of rules of responsible behaviour which are voluntary and non-obligatory for the moment. Such a step would allow us to create a basis for regulating activities of State and non-State actors in the use of ICTs.

We presume that on this issue, as well as on other aspects of the mandate, the OEWG will take into account and develop the proposals made in the past years. The annex to the Chair's Summary of the first OEWG contains a number of concrete suggestions of States on rules, norms and principles, and it was recognized that their consideration should be continued. It would be possible to learn from the experience of regional organizations on this matter.

Given the lack of universal international legal regulation of the use of ICTs, the next step in the global discussion is the study of the possibility to develop legally binding norms. Russia has always advocated and continues to advocate developing of binding norms of legal regulation of rules of behaviour in information space. We proposed numerous times to jointly elaborate the content and the format of these norms under the auspices of the UN – moreover, it is reasonable to do it as soon as possible. We presume that multiple will further set the basis for universal international legal instrument – convention on international information security, which would be obligatory and would guarantee the formation of stable and secure system of international information security. In order to contribute to its elaboration, Russia could propose its relevant concept.

In our view, taking concrete measures on implementation of rules of behaviour will not have the expected effect and will not bring aspired results if the list of rules, norms and principles will not have universal and obligatory character.

In the framework of norm-making activities it would be reasonable for the OEWG to elaborate possible ways of regulating activities of IT companies in the digital sphere.

Thank you for your attention.

Within thematic discussion on how international law applies to the use of ICTs by States:

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

Given the absence of a universally agreed understanding of how international law applies to the use of ICTs we believe it would be reasonable for the OEWG to have a thorough discussion of specific issues that remain unsolved:

– how the existing international law, in particular, specific international legal principles of cooperation, apply to the use of ICTs given their characteristics;

– which legal relations in the use of ICTs among subjects of international law still lack regulation and how this regulation may be fulfilled at the global level;

– which particular activities of States in the use of ICTs are considered unlawful from the point of view of international law;

– how and on which basis computer attacks at information resources of States may be qualified from the point of view of international law;

– which international legal mechanisms are required to accomplish the task of deanonymizing information space.

In our view, the principle of cooperation in international law, as applied to the use of ICTs, is also worth discussing, namely by exploring possible ways to elaborate specific international legal mechanisms of interaction, for instance, between and among points of contact on ICT-security or computer incident response teams.

Mindful of all of the existing gaps, as well as of the absence of a universal international legal instrument in the field of security in the use of ICTs, we deem appropriate to raise the issue of developing international legal regulation of ICT-environment and progressively developing international law, taking fully into account the specificities of these technologies. The elaboration a universal convention on ensuring international information security should become our priority.

Given those difficulties that our delegations face on a regular basis when negotiating documents at the UN, as well as in regional and multilateral formats, we consider it important to develop universal terminology with regard to security of and in the use of ICTs. We could start by formulating a list of terms that are used in consensus UN documents, and then proceed to agreeing upon definitions of the basic terms from this list (for example, ICTs, ICT-infrastructure, ICT-environment).

At the current stage, there is no consensus within the international community on the issues of qualifying malicious use of ICTs as armed attack as referred to in Article 51 of the Charter of the United Nations. Therefore, there is no ground to assess the legality of the use of ICTs from the point of view of international humanitarian law. Now, when the existing methods and means of

identifying sources of malicious activities in information space do not allow to identify sources of the malicious activity and their geographic location in a timely and reliable manner, the use of the right for self-defense in response to information attacks may lead to armed escalation.

It would be useful to engage international legal experts and other interested representatives of academia in the discussion on international law within the OEWG for a more thorough consideration of these issues.

Thank you for your attention.

16 December 2021

Within thematic discussion on confidence-building measures:

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

In the area of confidence-building measures we believe it is important to make further steps with a view to implementing the recommendations set out by the first OEWG, in particular creating a rooster of points of contact that would engage in rapid information exchange on crisis events and threats in information space, measures to mitigate them, as well as information exchange on computer incidents and computer attacks perpetrated against states. It is essential to fix the understanding that the amount of information to be shared shall be defined by states themselves.

It is also important to agree upon basic universal principles of confidence-building measures in ICT-environment. The adoption of such measures should not:

– cause harm to security of participating states, as well as that of third states;

– provide advantages to any state or group of states in the military, political, economic or other domain, and in the field of intelligence;

– be used as a tool of interference in internal affairs of states for subjective political assessment of activities and intentions of states in information sphere that further trigger all sorts of punishments, such as sanctions and other response measures.

With a view to enhancing trust and transparency it is important to encourage states to consult on issues related to their activities in information space that may cause concern in order to prevent conflicts and peacefully settle any arising divergences.

As a specific measure we suggest establishing a practice of exchanging national lists of spheres of critical information infrastructure.

Thank you for your attention.

Within thematic discussion on capacity-building:

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

Building on the outcomes of the first OEWG, it is necessary to continue negotiating universal principles of capacity-building.

With a view to bridging the technological gap in the field of information security, we could discuss optimal forms of creating a targeted program / fund for capacity-building in the area of ICT-security for the purposes of providing assistance to developing states (following suit of other UN programs).

In our view, we could engage other interested parties, such as business and NGOs, in these efforts. It seems useful in this context to start exchanging good practices and experience of states in building public-private partnerships in the area of ICT-security at the national level. It is important to elaborate mutually acceptable ways of providing assistance and cooperation between / among states and private actors on the basis of equitable distribution, upon request of each state-recipient and with due regard to its specific needs and characteristics. It is also worth taking further steps to elaborate rules of responsible behavior of business in information space.

Thank you for your attention.

On agenda item 3 "Organization of work":

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

As for the issue of elaborating modalities of interaction between the OEWG and other stakeholders, we would like to share the following considerations.

First of all, we are grateful to you for all your efforts aimed at ensuring success of the OEWG first substantive session.

Despite the fact that some States made a demarche on the first day of our session, threatening to block it under the pretext of immediately solving the issue of stakeholders, thanks to our joint efforts we succeeded to prevent disruption of the event and to proceed with quite exhaustive and truly substantive discussions of issues related directly to the mandate of the OEWG, which are those of ensuring security in the use of ICTs. We are glad that we did this and we thank you for your skillful management of your duties as the Chair.

As for establishing interaction with other stakeholders, we share the opinion expressed by the delegate from South Africa and we believe that it is necessary to stick to a reasonable and balanced approach to this issue, which would take into account the interests of all States as main participants of the format of the OEWG.

If someone is not satisfied with the precedent of the first OEWG, and if we start to resolve the task of elaborating concrete modalities of stakeholder participation in our work, we need to act responsibly on this matter. As for us, we are ready to work on this and we will present our considerations in accordance with the timeline that you proposed.

Thank you for your attention.

Within thematic discussion on regular institutional dialogue:

Distinguished Mr. Chair,

Distinguished ladies and gentlemen, colleagues,

According to one of the recommendations of the OEWG consensus final report, it would be unreasonable to duplicate negotiation efforts in the area of international information security within several bodies. The relevant Russia-US draft resolution, consensually adopted by the UN General Assembly, is also based on this logic. In this regard, we assume that the OEWG should remain the only negotiation mechanism under the UN auspices in this domain.

The OEWG format has already showcased its efficiency and relevance in practice. The first OEWG experience clearly demonstrated that this Group possesses all the necessary features that the international community aspires for at the current stage, namely its universal and democratic nature, openness, transparency, and decision-making based on consensus. As discussions continue and practical results are achieved, we will be able to consider the prospects of the negotiation process on international information security. We do not exclude the possibility of making the OEWG a long-term format or of transforming it into a permanent mechanism, if States deem it necessary.

Within this agenda item we also suggest looking into the prospects of promoting interaction and exchange of experience in the field of ICT-security between the OEWG and regional organizations (in the format of regional consultations, dedicated sessions / intersessional events with participation of representatives / heads of regional organizations).

I would also like to react to the issue touched upon by some States which is the “Programme of Action for advancing responsible behaviour of States in cyberspace”. We presume that this initiative is still at the stage of conceptualization. In our view, there is a need to discuss it substantively and elaborate it further on a universal, open and truly democratic basis, within the framework of the new OEWG. We are ready to work on this at future sessions.

According to the information we have at the moment, the Programme of Action looks more like a mechanism for reviewing norm implementation. Hence, we could discuss this issue within thematic debate on rules, norms and principles of behaviour. At the same time, given the rapid development of ICTs, it is crucial to move beyond what we have already achieved and to make further practical efforts in developing new norms, while considering new initiatives of States in this sphere.

Thank you for your attention.