

Annex 3. Impact of ICT on the Level of Strategic Stability: A New Format

Natalia P. Romashkina*

After the meeting of the presidents of Russia and the United States in June 2021 in Geneva, consultations on strategic stability began at the interdepartmental level under the auspices of the Russian Ministry of Foreign Affairs and the U.S. Department of State. The Russian interdepartmental delegation is headed by the Deputy Minister of Foreign Affairs of the Russian Federation Sergey Ryabkov and the American delegation by Deputy Secretary of State Wendy Sherman. At the regular meeting, it was decided to form two working groups: the Working Group on Principles and Objectives for Future Arms Control, and the Working Group on Capabilities and Actions with Strategic Effects. After the meetings of these groups, a third plenary session is scheduled. Fundamentally new is the fact that, as part of this comprehensive dialogue, expert consultations on cybersecurity under the auspices of the Russian Security Council and U.S. National Security Council are being held in Geneva.

Introduction

Not so long ago, skeptics suggested that it was inexpedient to discuss, even at the expert level, the issues of linking nuclear and cyber problems in the military field, that no agreements in this area were possible, and so on. However, the natural process of development of scientific and technological progress, primarily in the field of information and communication technologies (ICT), has led to the creation of new capabilities for both offensive and defensive weapons. At the same time, natural awareness of the vulnerability arising from accelerated growth in the likelihood of malicious ICT being used in the military sphere led to a new format for this topic. And today, despite the opinions of pessimists, not only is the problem of ICT influence on the level of strategic stability recognized at the highest level in the great powers, but interstate dialogue on this issue has resumed.

The transition of the problem of ICT influence on the level of strategic stability to a new format is taking place against the background, throughout 2021, of important breakthrough events in the development of the system of international information security and Russia's participation in this process.

In March 2021, at a meeting of the Russian Security Council, the international information security problem was discussed for the first time. In April 2021, Russian President Vladimir Putin approved a

* Head of the Division of Issues of Information Security, IMEMO RAS, Professor, Correspondent Member of the Academy of Military Sciences of the Russian Federation, PhD (Political Sciences).

new edition of one of the fundamental documents in this area, “Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security.”¹⁶

In addition, important positive changes have taken place at the international level. The UN adopted the final reports of the Open-ended Working Group (OEWG) and the Group of Governmental Experts (GGE) in the field of international information security. Thus, the “Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,” adopted by consensus in June 2021, can be seen as the beginning of the process of transforming the rules of responsible behavior into a system of norms of “soft” international law. Russia especially notes the position of the GGE Report on the parallel existence of the norms of responsible behavior of states in the ICT environment and international law, which reflects the awareness of cyberspace as a new area of international cooperation, significantly different from traditional spaces.¹⁷

In October 2021, the UN First Committee decided by consensus to merge the two parallel international information security platforms that existed from 2019 to 2021 — the OEWG and the GGE, created at the initiative of Russia and the United States, respectively. This will undoubtedly help to increase the effectiveness of countering existing and potential threats to international security in the ICT environment.

On December 6, 2021, the UN General Assembly by consensus adopted the Russian-American draft resolution “Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies,” put forward at the initiative of Russia.¹⁸

All this allows us to speak about the positive dynamics in the creation of an international information security system process.

Russia’s Cyber Stability Policy

After the Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring Russia-U.S. cooperation in the field of international information security on September 25, 2020, as well as his proposals in 2020-2021 on the need to sign bilateral documents between the

¹⁶ “Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security” (in Russian), April 12, 2021, <http://www.kremlin.ru/acts/bank/46614>.

¹⁷ United Nations, “Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security,” July 14, 2021, <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>.

¹⁸ United Nations, “Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behavior in the use of information and communications technologies,” A/76/439, November 12, 2021, <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/336/94/PDF/N2133694.pdf?OpenElement>.

Russian Federation and the United States — in particular, the Bilateral Intergovernmental Agreement on the Prevention of Incidents in the Information Space, as well as universal international legal agreements aimed at preventing conflicts and building a mutually beneficial partnership in the global information space¹⁹ — this problem has found a real embodiment.

At a briefing for foreign military attachés on December 24, 2020, Chief of the General Staff of the RF Armed Forces, General of the Army Valery Gerasimov noted: “The military confrontation extends to cyberspace and outer space, as a result, the risks of incidents due to interference in the functioning of control systems and ensuring the use of nuclear weapons increase. . . . In these conditions, nuclear deterrence remains a key element of ensuring the military security of the Russian Federation.”²⁰

The problem of the impact of ICT on the level of international security and strategic stability was also sounded in many speeches and at the annual Moscow conference on international security of the Russian Ministry of Defense in June 2021.

In his report at the opening of the Conference, the Minister of Defense of the Russian Federation Sergey Shoigu, speaking about topical issues of international security, said:

Hypersonic, digitalization and robotization come to the fore in the development of new weapons. Space and cyberspace are increasingly involved in military confrontation. As part of the armed forces of a number of countries, space and cyber commands are being created, the main task of which is not defense, but the planning and conduct of offensive operations in the relevant areas. A careful attitude towards international obligations is replaced by unilateral sanctions and the introduction of a certain order based on rules invented by someone unknown. The world is rapidly plunging into a new confrontation, much more dangerous than during the Cold War.²¹

It is logical that during the military exercises of the militarily advanced states, this problem is already being taken into account. In Russia, according to the Ministry of Defense, similar tasks were solved during an exercise in the Kemerovo region in September 2021: signalmen of the combined-arms formation of the Central Military District repelled a simulated enemy’s cyberattack on secret communication channels and ensured covert command and control of troops. According to the concept of the exercise, one of the currently topical scenarios for the malicious use of ICT was worked out: A conditional adversary attempted a network attack on secret communication channels

¹⁹ “Statement by President of Russia Vladimir Putin on a comprehensive program of measures for restoring the Russia–US cooperation in the field of international information security,” September 25, 2020, President of Russia (website), <http://en.kremlin.ru/events/president/transcripts/statements/64086>.

²⁰ “General of the Army Valery Gerasimov, Chief of the General Staff of the RF Armed Forces, gave a briefing for foreign military attachés,” Ministry of Defense of the Russian Federation (website; in Russian), December 24, 2020, https://function.mil.ru/news_page/country/more.htm?id=12331668@egNews.

²¹ “The Minister of Defense of the Russian Federation opened the IX Moscow Conference on International Security,” Ministry of Defense of the Russian Federation (website; in Russian), June 22–24, 2021, <https://mil.ru/mcis/news/more.htm?id=12368274@egNews>.<https://mil.ru/mcis/news/more.htm?id=12368274@egNews>

for command and control of troops in order to distort and substitute transmitted information. In response to these actions, continuous monitoring of equipment performance was organized, and a special technological barrier was created to prevent a network attack. Receiving information about the next cyberattack attempt, the operators manually blocked the attacked communication channel and switched to backup wire and satellite communication channels.²²

Strategic Stability and Cybersecurity – Towards New Agreements?

A key factor in determining the stepping up of this issue to a new format was the announcement of the launch of the Russian-American dialogue on strategic stability following the Putin-Biden meeting in Geneva on June 16, 2021. The Joint Statement of the Presidents of Russia and the United States on Strategic Stability indicated that Russia and the United States would participate in an “integrated bilateral Strategic Stability Dialogue,” the purpose of which “to lay the groundwork for future arms control and risk reduction measures.”²³

An important result of the meeting between the leaders of Russia and the United States was the first reaffirmation of adherence to the “principle that a nuclear war cannot be won and must never be fought” since the key Russian-American statement of 1985. This is notable in itself in modern conditions, when irresponsible calls for the use of nuclear weapons are heard in the West more and more often, when society purposefully minimizes the threat and consequences of nuclear war. After the end of the summit, Putin called the decision to start bilateral consultations on cybersecurity “extremely important” — both for Moscow and Washington and for the whole world.

On July 28 and September 30, 2021, two rounds of interagency consultations on strategic stability were held in Geneva under the auspices of the Russian Ministry of Foreign Affairs and the U.S. Department of State.²⁴ According to Deputy Minister Ryabkov, the future agreements on strategic stability should be based on a new “security equation” that would take into account all factors affecting this area, including strategic defensive and offensive weapons in their interconnection, as well as strategic offensive weapons in non-nuclear equipment — that is, systems that allow, without the use of nuclear warheads, the solving of strategic tasks in terms of hitting targets on the territory of the other side. Russian statements that this new “security equation” should take into account the

²² “The military police of the Central Military District at a special exercise repulsed the attack of the mock enemy on the convoy with humanitarian aid,” Ministry of Defense of the Russian Federation (website; in Russian), September 20, 2021, https://function.mil.ru/news_page/country/more.htm?id=12384785@egNews.

²³ U.S.–Russia Presidential Joint Statement on Strategic Stability, June 16, 2021, President of Russia (website), <http://en.kremlin.ru/supplement/5658>.

²⁴ Joint statement on the meeting in the framework of the Russian-American dialogue on strategic stability in Geneva, (in Russian), September 30, 2021, Joint statement on the meeting in the framework of the Russian-American dialogue on strategic stability in Geneva, September 30, 2021, https://www.mid.ru/ru/foreign_policy/news/1777978/?lang=en.

situation in outer space, where the danger of an arms race is growing, as well as the problems of cybersecurity, are of paramount importance.²⁵

Thus, negotiations on strategic stability are aimed not only at reaching a new treaty on the limitation of strategic nuclear weapons in the future. Discussions will focus on transparency and risk mitigation measures for unintentional or deliberate escalation of nuclear weapons use during a crisis or conflict. In addition, work is planned to analyze the proposed doctrines that could exacerbate tensions or complicate the management of emerging crisis.

Both sides once again emphasized the importance of the dialogue between Russia and the United States on information security issues during the lengthy conversation of Putin and Biden via videoconference on December 7, 2021. Leaders of the states expressed their readiness to continue working together on practical matters related to combating cybercrime through the criminal justice process, as well as using technical intelligence. Noting the unsatisfactory state of bilateral cooperation between Russia and the United States, the presidents nevertheless noted the importance of the process of implementing the results of the June 2021 Geneva summit, consistent implementation of the agreements reached at the highest level, and preservation of the “spirit of Geneva” when problems arise between Russia and the U.S.²⁶

Strategic Cyber Instability Issues

However, a huge number of problems make dialogue difficult. The very term “strategic stability” has no common understanding, which could have been foreseen after a long vacuum — in fact more than 20 years — of a constructive dialogue between the Russian Federation and the United States on this issue. It is logical that in such conditions, Russia and the United States propose different concepts and therefore have different priorities in relation to the newly emerging dialogue. As expected, controversial and difficult to reach a compromise on are the issues of missile defense of the United States and its allies; inclusion in the dialogue of all types of weapons systems with a possible strategic effect, both nuclear and non-nuclear; strategic systems for the delivery of medium and intercontinental nuclear weapons; tactical nuclear weapons; the destructive influence of ICT on military-political processes, etc.²⁷

Therefore, the discussion of cybersecurity issues within the framework of this complex dialogue in Geneva is of the utmost importance. A very wide range of issues have emerged over a long period of absence of dialogue. In particular, these include Russia’s concerns about U.S. missile defense plans,

²⁵ “Ryabkov: The new ‘security equation’ with the United States should take into account the topic of cybersecurity” (in Russian), Russian News Agency TASS, June 2, 2021, <https://tass.ru/politika/11535921>.

²⁶ Meeting with US President Joseph Biden, December 7, 2021, President of Russia (website), <http://en.kremlin.ru/events/president/news/67315>.

²⁷ N. P. Romashkina, A. S. Markov, and D. V. Stefanovich, *International Security, Strategic Stability and Information Technologies* (in Russian) (Moscow: IMEMO, 2020), <https://www.imemo.ru/files/File/ru/publ/2020/2020-017.pdf>.

increasing threats from harmful ICTs; the growing risks of militarization of outer space and interest in new types of anti-satellite weapons; interference in the internal affairs of sovereign states, etc.

There have already been five main and intermediate consultations between the Russian Federation and the United States on cybersecurity issues. In addition, contact has continued by videoconferencing at the level of experts and the exchange of messages and signals at the level of embassies.

The very beginning of the Russian-American dialogue on these most urgent and vital issues can be considered the most important result of this work. In addition, according to the parties, the format of the participants and the practice of exchanging views have already been worked out, in addition to holding online meetings via a closed channel. New contacts are planned for the coming period. According to the statement of the Russian Ambassador to Washington, Anatoly Antonov, “There are small but concrete results in the area of suppressing hacker activity. We are responding to all the concerns that Washington communicates to us through established channels.”²⁸

However, the American side, trying to achieve unilateral advantages, seeks to focus all work in negotiations on cybersecurity exclusively on the interests of the United States, ignoring Russia’s concerns in this area. Russia is ready to discuss with Americans topics of their primary interest (currently, first of all the suppression of the activities of hacker groups attacking objects in the United States with the help of ransomware viruses), but believes that the conversation on this topic should include not only discussion of an attack by some groups on, for example, a meat processing plant with the aim of obtaining a ransom, but also many other aspects: “With all the importance that the American side attaches to what it considers to be hacker attacks by cyber fraudsters, we must look at [cybersecurity] from the point of view of a more direct link with the task of strengthening strategic stability in general.”²⁹ Russia, in particular, considers it important to discuss the risks of cyberattacks on elements of the armed forces command and control system.

Expanding the topic and agenda, taking into account the interests of Russia, is still the most important task for professionals from various fields, but at this stage, first of all, for Russian diplomacy. There are some shifts in this direction, but they are not sufficient. According to the Russian Foreign Ministry, it is still premature to talk about any binding agreements in this area, since there is no experience in developing binding agreements in this area in connection with the task of strengthening strategic stability.³⁰

²⁸ “Ambassador Antonov spoke about the results of the dialogue with the United States on cybersecurity” (in Russian), RIA News, October 12, 2021, <https://ria.ru/20211012/kiberbezopasnost-1754295082.html>.

²⁹ “Ryabkov: Russia and the United States have already held four rounds of consultations on cybersecurity” (in Russian), Kommersant, July 22, 2021, https://www.kommersant.ru/doc/4910861?utm_source=yxnews&utm_medium=desktop.

³⁰ “We are waiting for a ‘Subject reaction’. Ryabkov assessed the talks with the United States in Geneva” (in Russian), RIA News, July 28, 2021,

Indeed, the problems of developing measures of transparency, trust, and predictability, agreeing and verifying with regard to restrictions or abandoning cyber weapons, now may seem insoluble, but today one can and should make every effort to develop a dialogue between the Russian Federation and the United States, ultimately aimed at developing and signing a document that politically obliges states to abandon cyberattacks on each other's strategic control systems to prevent an unintended exchange of nuclear strikes.

Russia expects dialogue with the United States on cybersecurity to become regular if a broad agenda is discussed.

In the context of the new format of the problem of ICT's impact on the level of strategic stability, the question of the prospects for signing legally binding documents is currently quite acute. This is due to the following problem. On the one hand, at present, the latest weapons systems and military technologies, including ICT, create difficulties for the development of control and restrictive regimes in relation to strategic stability. On the other hand, new ICT capabilities objectively add uncertainty and, consequently, increase the risks of starting a nuclear war. This means that in the future they contribute to the awareness of this threat, the awareness of equal vulnerability for all players of strategic stability. In addition, as history proves, this leads as a result to the achievement of a compromise, which is necessary and inevitable in order to reduce the number of conflicts with a high probability of escalation to a large-scale nuclear war.

This problem has largely become one of the reasons for the emergence of the theory that changes in the world order and revolutionary military technologies require the abolition of negotiations and treaties on arms limitation, including cybernetic ones. Instead, these would be replaced with multilateral forums of states and broadly focused experts — in order to agree on a common philosophy of stability. In addition, there are arguments for the complete abandonment of control and restrictive treaties in favor of military rivalry without rules — in order to achieve strategic superiority. And this is a direct path to disaster.

At present, the awareness of the importance of arms control — the desire and ability to consistently seek agreements in this area, relying on the half-century experience of its predecessors — plays a global role. As a result, the world will be able to avoid new cycles of the arms race, further proliferation of nuclear weapons, and an increase in the number of conflicts with a high probability of escalation to a large-scale nuclear war. Awareness of the need to preserve and develop the arms control system, its adaptation to new destabilizing factors, including the use of ICT for harmful military-political purposes, plays a global role. Of course, on the way to new agreements, it is advisable to productively use the many years of experience of Russia (USSR) and the United States to consistently and professionally seek agreements.

With the political will of the parties, the system of limiting and non-proliferation of weapons can be preserved and adapted to cover many of the latest destabilizing weapons. As happened in the past, not

https://radiosputnik.ria.ru/20210728/ryabkov-1743345002.html?chat_room_id=1743345002.

all innovative technologies can be taken under control now or tomorrow. However, the continuation of the productive negotiation process — with the leading role of Russia and the United States — is an indispensable condition for the subsequent inclusion of the latest weapons and technologies in the legal regimes. This is necessary for the future restructuring of the arms control system from bilateral to multilateral formats, and for creating a base to ensure the necessary and sufficient level of strategic stability.

In a recent interview, speaking about the problem of cybersecurity, Director of the Russian Foreign Intelligence Service Sergey Naryshkin noted: “Of course, we are following development in this area, because we must not lag behind, and we must ensure national security, including cybersecurity. . . . We see how our partners are building up their offensive cyber capabilities both in the United States and NATO member states, but I can assure that Russia is capable of and will ensure information security. Russia is making its contribution to the creation of a global security system in the cyber-sphere.”³¹

It is logical to assume that one of the most important tasks in this case is the international legal support of strategic stability, taking into account ICT threats.

³¹ Dumb intelligence? Sergey Naryshkin, director of the Russian Foreign Intelligence Service, September 26, 2021, RT.com (television network), <https://www.rt.com/shows/worlds-apart-oksana-boyko/535830-intelligence-information-dumb-naryshkin/>.