New Technologies: Challenges to International Security and Stability

Nataliya P. Romashkina
International Security Center
Primakov National Research Institute of World Economy and International Relations (IMEMO)
Moscow, Russia
Romachkinan@yandex.ru

***Abstract*—Article presents comprehensive analysis of the most relevant threats in informational sphere, which represent the danger for international peace and carry global and strategical nature. Author underlines that existence of these threats requires immediate development of mechanisms for international administration and control. Currently many states consider military confrontation as a resistance taking place not only within four standard domains: earth, naval, air and near-earth space, but also in informational and cyber space. It raises the problem of application of informational and communicational technologies (ICTs) for military and political purposes to perform hostile actions and acts of aggression. Indications of such problem were identified in the article along with military means, which contribute to conduction of informational and cyber operations. Cyberwarfare adds unpredictability and uncertainty to international military and political relations and reduces the level of strategic stability. The article describes the main factors of global effect of information and communication technologies on strategic stability. The analysis of modern approaches to define the concept of strategic stability in the ICT era as well as new characteristics of instability of the modern international politico-military system are presented. Arguments underlying the need to develop mechanisms of international governance in this area are provided. Suggested specific international actions performed together with Russia in response to current global challenges to international security and strategic stability may become one of such instruments.**

***Keywords*—information security; information and communication technology (ICT); strategic stability; information weapons; information threat; cyber threat; cyber attack; cyber-electromagnetic activity; cyber warfare; cyber war; nuclear weapons.**

I. Introduction

In the 21st century, information revolution has posed fundamentally new questions to humanity that have already attained international and global importance. Along with unique capabilities, rapidly developing information and communication technologies (ICTs) pose global challenges and threats. Information sabotage in the ICT space has become a new tool for non-state collective and individual subjects. Methods using ICT are turning into an important element of the politico-military potential of states complementing and sometimes even replacing traditional political and diplomatic means and weapons.

The information and cyber warfare of some states against the others may lead to similar level of destruction compared to traditional wars, and new information and communication technologies can become a detonator for unleashing an interstate military conflict using strategic and even nuclear weapons. Currently new ICTs are already actively used in the military organization and infrastructure, and this creates new objective problems. The most important of ICT threats are those in field of strategic and, in particular, nuclear weapons. Thus, ICTs are already affecting the level of strategic stability. Therefore, ensuring international security and strategic stability becomes one of the most important and urgent tasks of the world community in the modern digital era. It requires the development and modernization of international governance and control mechanisms. At the same time, one does not need to fundamentally change the basic principles of international governance, because ICT threats exacerbate, complicate, deepen, reinforce and modify the problems existing in this area.

No single country in the world can consider itself protected from such cross-border information and cyber threats and is able to solve global information security problems alone.

II. Application of Informational and Communicational Technologies for Military and Political Purposes to Perform Hostile Actions and Acts of Aggression

Information and cyber operations provide unique opportunities for creating a destructive effect in the modern world. Military means for these operations include strategic communications, interagency coordination groups, cyber and space operations, information support, intelligence, special technical procedures, etc. [1].

The United States has been the undisputed world leader in this area for many years. According to famous American scientists, “In today's global information age, victory may sometimes depend not on whose army wins, but on whose story wins” [2]; cyber technology “can be a decisive force multiplier if employed carefully, discriminately, and at precisely the right time” [3]; “The soft power of attraction becomes an even more vital power resource than in the past, but so does the hard, sharp power of information warfare” [4]. Moreover, the strategy of information superiority attainment, which is defined in the US as the ability to collect, process and spread a continuous flow of information, depriving the adversary of the ability to carry out such actions, has been under development for several decades, which has been reflected in doctrinal documents and in practice by running information operations. This situation has created a trend to increase additional global risks and is directly related to the problem of strategic stability maintenance. Therefore, it requires special attention from specialists. Another crucial and relevant trend in the development of ICT space is associated with the problem of security of ICT systems, which are of strategic importance for most countries around the world. These systems have become an important factor ensuring sovereignty, defense and security of the state. Moreover, today one considers a threat to the development of so-called information and cybernetic weapons. According to some estimates, more than 30 states already have offensive cyber weapons. ICTs can provoke the interstate military conflict, primarily because of the possibility of disproportionate use of methods responding to threats and attacks. For example, the injured party can use real weapons in response to the use of cyber weapons. In addition, a conflict may occur by mistake, as there is no universal methodology for identifying violators, and criteria for classifying cyber attacks as an armed aggression have not yet been developed together with universal principles for investigating such incidents. To date, a wide range of ICTs has been created that can be used in the military field. They include:

• *Warfare with Command and Control System*, being a military strategy using information environment on the battlefield to physically destroy the enemy command structure,

• *Intelligence warfare*, being offensive and defensive operations using automated systems, which, in turn, are potential targets of cyberattacks,

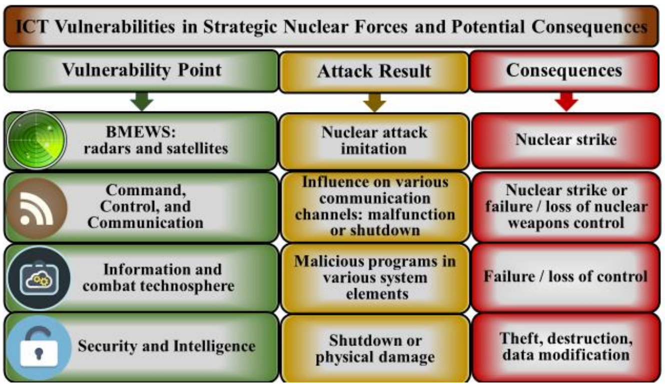
• *Electronic warfare*, being military operations using electromagnetic and directed energy to control the enemy. These include three units: electronic attack, electronic defense and support for electronic warfare,

• *Military means to facilitate information operations*, such as those including strategic communications, interventions in cyberspace and space, military support of information, intelligence, joint operations of the electromagnetic spectrum, etc. [5].

The problems associated with these opportunities can be attributed to various elements of the military organization and infrastructure. However, the most important of them is certainly the group of ICT threats in the field of nuclear weapons (Fig. 1). Today there are different opinions regarding the likelihood and consequences of the harmful effects of ICTs on the system of command and control of nuclear weapons, from complete denial to arguments for a sharp increase in such probability. However, both in general science and in military strategy, in particular, one needs to consider the worst-case scenarios. Therefore, this problem should be in the focus of attention of scientists and practitioners, primarily from the states with the nuclear weapons. However, one does not need to fundamentally change the base principles of international governance. ICT threats exacerbate, complicate, deepen, amplify and modify those problems, which have always existed in maintenance of the nuclear weapons security.

Thus, the threats of the application of new technologies are caused by the development of cyber weapons, use of ICTs to interfere in the internal affairs of states, and development of ICTs for harmful influence on military-industrial complex objects. The international security threats are further enhanced with the development of *remote-controlled military combat robot systems* [6], *military-grade artificial intelligence* [7], machine learning, the autonomous operation of various systems and subsystems, automated decision-making systems, etc., that may be exposed to ICT attacks, as well as means of *cyber-electromagnetic activity*, which is actively developed in the USA. *Cyber electromagnetic activities* are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. CEMA consist of cyberspace operations (CO), electronic warfare (EW), and spectrum management operations (SMO) [8].

In addition to technological characteristics, there is also a psychological one, which can be formulated as the loss of fear of a nuclear war among society and political elites of the West countries. This can significantly lower the threshold for the use of the weapons. Moreover, the most dangerous belief seems to be a conviction that a local "small" nuclear war is possible and the victory can be reached there. The tendency to spread such views has arisen with the help of modern ICTs, allowing affecting a huge audience in a relatively short time with no substantial economic costs. At the same time, damage assessment and development of counteractions are significantly complicated due to the “intangibility” of ICTs and wide range of sources of possible malicious technologies, including state and non-state actors, and single hackers. All of these factors increase the level of uncertainty and instability. Therefore, one of the most crucial and relevant threats related to ICT in the field of international security appears to be the decrease in the level of strategic stability.



ICT Vulnerabilities in Strategic Nuclear Forces and Potential Consequences

Vulnerability Point	Attack Result	Consequences
BMEWS: radars and satellites	Nuclear attack imitation	Nuclear strike
Command, Control, and Communication	Influence on various communication channels: malfunction or shutdown	Nuclear strike or failure / loss of nuclear weapons control
Information and combat technosphere	Malicious programs in various system elements	Failure / loss of control
Security and Intelligence	Shutdown or physical damage	Theft, destruction, data modification

Fig. 1. Strategic nuclear weapons: some ICT vulnerabilities and potential consequences.

III. The Effect of Informational and Communicational Technologies on the Level of Strategic Stability

Today, the problems of strategic stability become a main topic of international relations once again. This is primarily because of the gradual destruction of the regime associated with limited and reduced strategic missile and nuclear weapons, after the withdrawal of the US from the Anti-Ballistic Missile Treaty (ABM Treaty), the Intermediate-Range Nuclear Forces Treaty (INF Treaty) and in the absence of negotiations on the limitation and reduction of nuclear weapons at the end of the Strategic Arms Reduction Treaty (START-3, New START) [9]. Another factor is the accelerated development of ICTs that have a global impact on military and political relations in the 21st century. Is it possible to provide the required and sufficient level of strategic stability in the modern conditions of the new technological revolution? Or will the instability, including global and strategic one, become a new trend? Currently, this situation can be considered as a crisis.

Moreover, today one considers two approaches or even a split between supporters of the classical view on strategic stability being developed during the bipolarity when this term was born, and supporters of a completely new view on challenges and ways to ensure strategic stability in modern conditions. Probably the truth is somewhere in between. It would be a mistake to abandon the experience of strategic stability maintenance accumulated during the Cold War, which helped to avoid a large-scale war in conditions of deep confrontation extended for decades. At the same time, one has to take into account modern political and technological fundamental changes. Thus, during the bipolarity period, *the concept of "strategic stability"* applied to nuclear-weapon states was defined as *the state of their relationship, in which the incentives to launch the first nuclear strike are removed* [10]. As nuclear weapons continue to exist and their destructive capabilities are constantly being improved, this understanding of strategic stability is still relevant today, similarly to the period of Cold War when this view was formed. However, the situation has become much more complicated over the past three decades, and the ideas about the methods and mechanisms to prevent nuclear war developed during the bipolarity, have ceased to reflect modern geopolitical realities and the level of technological development. These significant changes in international military and political relations require taking into account not only the nuclear component of this concept but also other indicators and characteristics, while preserving the traditional essence at the same time. In addition, today one does not consider two global poles of confrontation examined during the bipolarity period, but observes an increase in the number of entities affecting the strategic stability level. Therefore, it is necessary to assess the capabilities and characteristics of the politico-military system.

The strategic stability of the politico-military system is the state of the peace (absence of a large-scale war) within the framework of this system, which is maintained even in response to constantly acting disturbances (destabilizing factors) for a certain (given) period of time [11].

Therefore, on a professional level, one should speak not strategic stability "maintenance" and its "consolidation", but about the need to *ensure strategic stability*, the need to develop new approaches to assess the level of strategic stability based on the existing experience. This is about the development of general qualitative, and most importantly, quantitative metrics of this level. Therefore, one has to agree on common evaluation criteria. Initiated by the US, the process of discussing such criteria was ceased at the RF-USA bilateral level during 1990s. This has resulted into a global problem, because the decrease in the level of strategic stability below the required and sufficient threshold is extremely dangerous for all states with no exceptions. Therefore, all countries over the world seem to be interested in ensuring such level. However, the responsibilities of different states appear to be different, with the nuclear-weapon states still bearing the greatest responsibility. What are the new emerged characteristics of the system, within which it is vital to provide the required and sufficient level of stability?

- *Increase in the number of local wars and armed conflicts*, and more significant effect of ICTs on their outbreak and waging.
- *Change in the system of international relations after periods of bipolarity and monopolarity*, led by the United States. This is primarily due to changes in the military and -strategic relations between Russia and the United States, as well as the emergence of a new global center of power being– China, which is not involved in the nuclear disarmament process.
- *Gradual destruction of the regime of limitation and reduction of strategic arms* after the withdrawal of the US from the ABM Treaty, the INF Treaty and in the absence of negotiations on the restriction and reduction of nuclear weapons at the end of the New START [12].
- *Nuclear-missile multipolarity*, which is associated with increase in the number of states with nuclear missile weapons, as well as with increase in probability of their subsequent proliferation.
- *Trends of doctrinal changes in the nuclear-weapon states*, which are formally designed to consolidate deterrence but in fact weaken a threshold of nuclear weapons use, increasing the chances of limited nuclear wars.
- *US large-scale missile defense system*, which significantly changes the balance of strategic forces and increases the level of uncertainty in strategic planning [13].
- *Increasing role and power of non-nuclear (precision and smart) types of weapons in strategic planning*, which create a theoretical threat of a disarming strike against strategic nuclear forces [14]. The development of such weapons significantly complicates the global strategic environment and decision-making process in crisis situations.
- *Deployment of nuclear and non-nuclear weapons on the same platforms*, which may result in the launch of ballistic or cruise missiles with conventional weapons

being mistakenly considered by the opponent as use of nuclear weapons.

- *Appearance of low-yield nuclear weapons*, the presence of which reduces the threshold for the use of nuclear weapons and, therefore, increases the likelihood of escalation of armed conflict into a nuclear war [15].
- *Development of the latest ICT-based anti-satellite arsenal* used to affect the operations of enemy satellites, including elements of the Ballistic Missile Early Warning System (BMEWS), and destroy them using anti-satellite systems located on the Earth. At the same time, the fundamental vulnerability of spacecraft for cyber attacks is primarily due to the need to use communication channels with the Earth in the process of satellite operations. At present, this seems to be one of the most serious threats to strategic stability. In addition, cyber assets can affect the efficiency of satellites within *Combat operations system in common information space*, being actively improved in military developed states. The technological basis of the concept of Combat operations in the common information space is the aggregation of all armed forces elements in the single computer network. Thus, each of the elements of this network can also be exposed to cyber attacks.
- *Militarization of outer space* associated with the expansion of military space projects in some nuclear-weapon states.

Thus, the main factors of the global impact of ICT on strategic stability are:

- Use of ICTs for destructive politico-military purposes;
- Temptation to win a large-scale war, associated with the explosive development of technologies that encourage to acquire strategic advantages;
- Tendency to blur the borders between peaceful state of countries and their transition to the state of war, along with blurring the line between defense and attack in military and nuclear planning;
- Changes in logic of global confrontation, with the integrated use of non-military methods based on malicious ICTs leading to the goals of war being achieved even without an armed conflict (Fig. 2, 3);

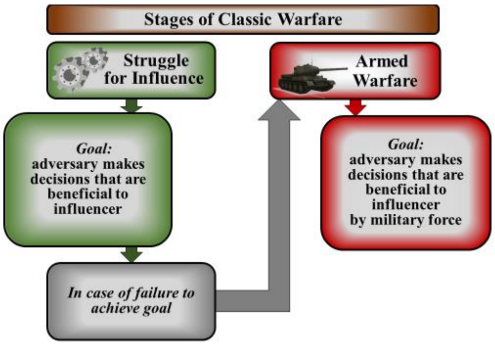

Stages of Classic Warfare
Struggle for Influence
Armed Warfare
Goal: adversary makes decisions that are beneficial to influencer
Goal: adversary makes decisions that are beneficial to influencer by military force
In case of failure to achieve goal

Fig. 2. Stages of classical warfare without the complex use of ICTs.

- *Reduction of "conflict escalation staircase", associated with an increased likelihood of ICT attacks on elements of the military nuclear missile infrastructure.*

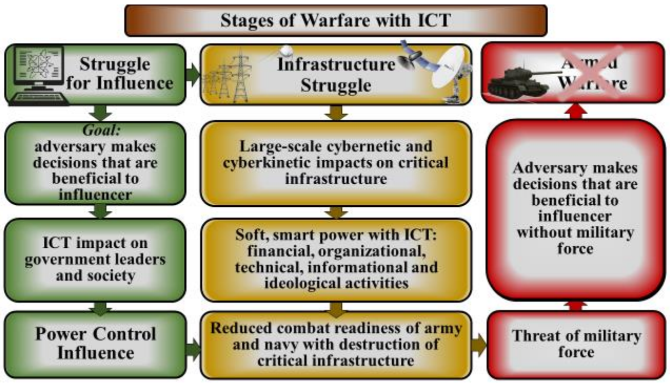

Stages of Warfare with ICT
Struggle for Influence
Infrastructure Struggle
Armed Warfare
Goal: adversary makes decisions that are beneficial to influencer
Large-scale cybernetic and cyberkinetic impacts on critical infrastructure
Adversary makes decisions that are beneficial to influencer without military force
ICT impact on government leaders and society
Soft, smart power with ICT: financial, organizational, technical, informational and ideological activities
Power Control Influence
Reduced combat readiness of army and navy with destruction of critical infrastructure
Threat of military force

Fig. 3. Stages of warfare with complex use of ICTs.

During the development of criteria for evaluation of the level of strategical stability and corresponding specific approaches to ensure it, one should take into account both general characteristics applicable to any historical period and features of the current state. The accelerated development of ICTs is currently one of such exceptional features. Analysis confirms that all factors, which destabilize the modern system of strategic stability, are nowadays associated with the development of ICTs. Therefore, it seems to be advantageous to emphasize the corresponding ICT threats as a separate destabilizing factor. Moreover, today many other factors are aggravated by the use of ICTs for destructive purposes, the militarization of peaceful information technologies, and the ease, suddenness and speed associated with both information technology and information-psychological weapons.

IV. Conclusions

1. The most dangerous ICT-threats to international security are: use of information and cyber weapons for military and political purposes to perform hostile actions and acts of aggression; destructive cyber impact on the elements of Critical National Infrastructure; interference in domestic affairs of sovereign state, violation of social stability, initiating interethnic and international conflict through ICTs. These dangers poses a threat to global security, and therefore requires the search for additional mechanisms of international governance.
2. Situation in the field of strategic stability can be assessed as a crisis. Given the gradual destruction of the regime of limitation and reduction of strategic weapons and the absence of negotiations on the limitation and reduction of nuclear weapons, the existing mechanisms of international governance in this area are not enough.
3. In the context of ensuring strategic stability, the security of missile and nuclear weapons requires

special attention. All nuclear states are upgrading nuclear systems, seeking to introduce new computer technologies. More and more components of the military nuclear infrastructure, from warheads and their delivery systems to control and guidance systems as well as command and control systems of strategic nuclear forces, depend on sophisticated software, which makes them potential targets for ICT attacks.

4. The particular attention is required for strategic weapons defense, ballistic missile early warning system, air defense and missile defense systems, and nuclear weapons command and control. At the same time, in addition to or instead of the principle of deterrence due to an imminent retaliatory strike, there is growing interest in deterrence by blocking the use of offensive means ("left of launch") using ICTs.

5. The most dangerous threat to strategic stability that is not hypothetical but already real is risk of ICT's effect on the decision to use nuclear weapons, i.e. the increasing probability of erroneous authorized launch of ballistic missile as a result of incorrect information or a lack of confidence in correct operations of the systems and perception of certain actions as an initial stage of the transition to mutual assured destruction. This reduces the level of strategic stability significantly.

6. Under these conditions, the following international actions with the participation of Russia in response to pressing global challenges to international security and strategic stability are advisable:

- Recovery of RF-US negotiations on the limitation and reduction of strategic nuclear missile weapons; involvement of other states with nuclear weapons to limit and reduce the strategic nuclear forces;
- Development and establishment of common (RF, USA, PRC) understanding of the strategic stability criteria;
- Development and establishment of common (RF, USA, PRC) understanding of the danger of ICT threats for international security and stability;
- Development of common approaches to assess likelihood of unintentional and intentional ICT attacks on strategic nuclear forces;
- Explicit establishment of likely response to the detection of ICT attacks on strategic nuclear forces, for ICT weapons deterrence.

These measures can become the basis for creating a deterrence policy in the ICT environment, as it has been done with nuclear weapons during the bipolarity. In parallel, work on the establishment of control over ICT weapons will be advantageous, which could include:

- Ban on ICT attacks on specific objects, primarily in the military sphere (statements, agreements, treaties);
- Limitations and/or abandonment of offensive ICT opportunities;
- Steps to control ICT weapons proliferation;
- International standards on means and methods to prevent and eliminate cyber conflict;
- Development of convention to prohibit the harmful use of ICT in the field of nuclear weapons.

References

[1] R. Molander, A. Riddile and P. Wilson, Strategic information warfare: a new face of war, Library of Congress Cataloging in Publication Data, RAND (Firm), 1996, 33 p.

[2] J.S. Nye., The Information Revolution and Soft Power, Current History 113(759), 2014, pp.19-22.

[3] M.C. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation, 2009, 238 p.

[4] J.S. Nye, Our infant information revolution, Australian Strategic Policy Institute, The Strategist, 19 Jun 2018.

[5] N.P. Romashkina, Global Military Political Problems in International Informational Security: Trends, Threats and Prospects, Voprosy kiberbezopasnosti [Cybersecurity issues], 2019, No 1 (29), pp. 2-9. DOI: 10.21681/2311-3456-2019-1-2-9.

[6] S.A. Joshi, G. Aravalli, A. K. Vidyashree, S. Ranade and S.S. Badami, Wireless controlled military combat robot system, 2017 2nd International Conference on Communication and Electronics Systems (ICCES), IEEE, March 2018.

[7] W. Knight, Military artificial intelligence can be easily and dangerously fooled, MIT Technology Review, Oct 21, 2019.

[8] Cyber Electromagnetic Activities, Field Manual No. 3-38, Headquarters Department of the Army, Washington, DC, 12 February 2014, 96 p.

[9] D. Trenin, Strategic Stability in the Changing World, Carnegie Endowment for International Peace, March 2019.

[10] A. Arbatov, A New Era of Arms Control: Myths, Realities and Options, Carnegie Endowment for International Peace, October 2019.

[11] Informational Security Problems in Modern International crises and conflicts of XXI century / A.V. Zagorski, N.P. Romashkina, eds. – Moscow, IMEMO RAN, 2016,183 p.

[12] A. Arbatov, Dreams and Realities of Arms Control. World Economy and International Relations, 2019, vol. 63, No 11, pp. 5-16.

[13] Missile Defense Systems at a Glance, Arms Control Association, August 2019. URL: https://www.armscontrol.org/factsheets/missiledefenseataglance.

[14] T. Anichkina, High-Precision Long-Range Conventional Weapons and Nuclear Arms Control, World Economy and International Relations, 2019, vol. 63, No 9, pp. 14-21.

[15] A Low-Yield, Submarine-Launched Nuclear Warhead: Overview of the Expert Debate, Congressional Research Service, March 21, 2019