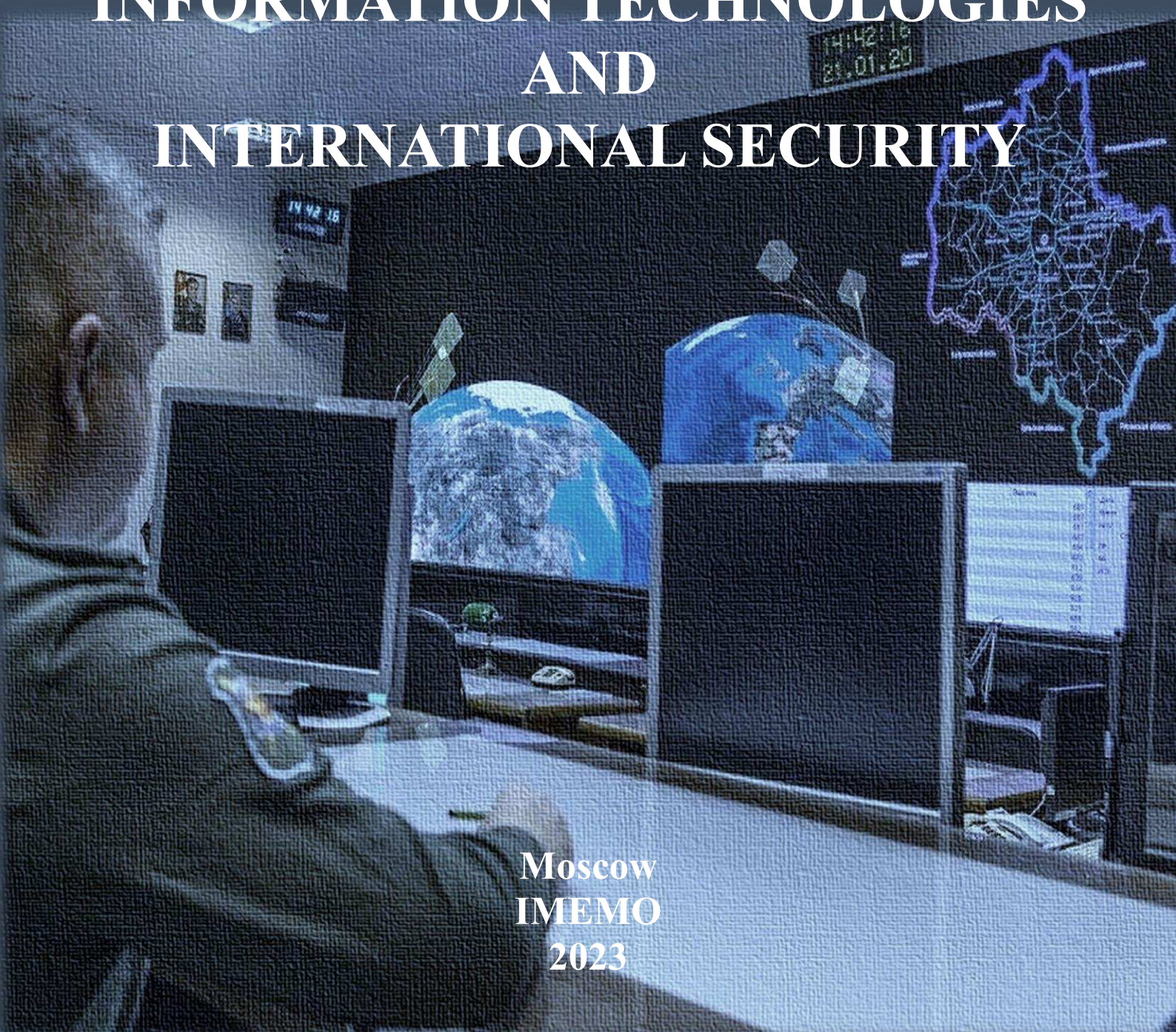




PRIMAKOV NATIONAL RESEARCH
INSTITUTE OF WORLD ECONOMY AND
INTERNATIONAL RELATIONS,
RUSSIAN ACADEMY OF SCIENCES

N.P. Romashkina
A.S. Markov
D.V. Stefanovich

INFORMATION TECHNOLOGIES AND INTERNATIONAL SECURITY



Moscow
IMEMO
2023

PRIMAKOV NATIONAL RESEARCH INSTITUTE
OF WORLD ECONOMY AND INTERNATIONAL RELATIONS,
RUSSIAN ACADEMY OF SCIENCES

N.P. Romashkina
A.S. Markov
D.V. Stefanovich

INFORMATION TECHNOLOGIES
AND
INTERNATIONAL SECURITY

Moscow
IMEMO
2023

УДК 327
ББК 66.4(0)
R75

Recommended by the IMEMO Academic
Council

Series “Library of the Primakov National Research Institute of
World Economy and International Relations”

Reviewers:

Doctor of Military Sciences, Candidate of Technical Sciences, Professor N.I. Turko,
Doctor of Technical Sciences, Professor S.A. Petrenko

Chapter 1 – Candidate of Political Science N.P. Romashkina,

Chapter 2 – Doctor of Technical Sciences A.S. Markov,

Chapter 3 – D.V. Stefanovich,

Chapter 4 – Candidate of Political Science N.P. Romashkina (Section 4.1), D.V.
Stefanovich (Section 4.2),

Doctor of Technical Sciences A.S. Markov (Section 4.3)

Cover with a photo by E.A. Kael

R75

Romashkina N.P., Markov A.S., Stefanovich D.V. Information Technologies
and International Security : [electronic resource]. – Moscow : IMEMO, 2023. –
111 p. – URL: [https://www.imemo.ru/publications/info/information-technologies-
and-international-security](https://www.imemo.ru/publications/info/information-technologies-and-international-security)

ISBN 978-5-9535-0613-7

DOI 10.20542/978-5-9535-0613-7

The monograph is devoted to topical issues of international security and strategic stability in the context of accelerated development of information and communication technologies. It justifies the importance of ensuring international information security. The monograph examines the possibility of establishing an IT-arms control regime under the UN auspices. Different aspects of regulation of software security systems and of the use of supercomputers in the context of the international information security are examined. The impact of information and communication technologies on strategic stability is analyzed. This monograph is addressed to specialists in the field of information and communication technologies and international security, university lecturers, students, and graduate students at universities, as well as a wide range of English speakers and English learners.

УДК 327
ББК 66.4(0)

IMEMO publications are available at <https://www.imemo.ru>

ISBN 978-5-9535-0613-7

© IMEMO, 2023

CONTENTS

FOREWORD	4
ABBREVIATIONS	6
INTRODUCTION	7
CHAPTER 1. Information and Communication Technology and International Security	12
1.1. International Information Security as Part of the Global Security Problem	12
1.2. Past, Present, and Future International Information Security on the UN Agenda	14
1.3. Political & Military Issues of International Information Security	26
1.4. Russia's Problems in the Field of Information Security	29
CHAPTER 2. Software Systems and International Information Security	34
2.1. Security Flaws of Software Systems	34
2.2. Ways to Increase Confidence in Program Security	42
CHAPTER 3. Supercomputers and Security Problems	56
3.1. Supercomputer Ratings	57
3.2. Supercomputers in the Nuclear Sphere	59
3.3. Using Supercomputers	61
3.4. "Supercomputer" Security	63
CHAPTER 4. Information and Communication Information and Strategic Stability	65
4.1. Strategic Stability in the Era of Information and Communication Technology	65
4.2. Information and Communication Technology and Nuclear Deterrence	76
4.3. The Problem of Attribution of Computer Attacks in the Process of Ensuring Strategic Stability	87
CONCLUSION	101
BIBLIOGRAPHY	103
ABOUT THE AUTHORS	110

FOREWORD

This book is devoted to topical issues of the influence of information and communication technologies (ICT) on international security and strategic stability. The book broadly examines the problems of information security in international political and legal relations, and its interaction with the internal development of states. From a special perspective, the security of software systems and the use of supercomputers is explored. Targeted attention is paid to the influence of the hostile impact of information technologies on the national defense of states and particularly on the strategic stability of relations between nuclear powers.

The book attempts to explain the need and possible measures to ensure international information security as part of global security, promotes the philosophy of creating a regime of control over aggressive ICT technologies under the auspices of the UN. Obviously, such issues are greatly influenced by the ideological and political interests of different states. Therefore, their initiatives are affected by propaganda goals that are also examined in the arguments presented in the book.

For several decades, attempts have been made within the framework of the UN and other international forums to introduce ICT into the legal framework and develop rules and methods to combat their hostile use. In this area, contradictions between states are not accidental. Russia, China, and the countries that have joined them see the main danger in the possible influence of ICT on their public opinion to destabilize the current political system, to disseminate alternative information and form opposition sentiments and movements (preparation of “color revolutions”). For their part, the United States and other Western countries emphasize freedom of information and insist on a narrower and more applied approach – measures to regulate the military-political use of ICT. At the same time, they are trying to divide these activities into illegal attack technologies and legitimate self-defense measures.

After lengthy disputes, on March 12, 2021, all 193 UN countries unanimously approved the report, which was called by the Russian representative a triumphant success of diplomacy in a difficult international situation. It contains a wide set of provisions of a general political nature, which is designed for voluntary implementation by States and is very far from their tacit practical activities. It is hardly realistic to count on specific interstate agreements to limit the use of ICT to influence the internal, foreign policy and security of states in the foreseeable future.

Also, the direct relationship between the mentioned threat and arms control is not currently visible, as well as the possibility of extending this control to cyber weapons. However, it is clear that while the possibility of control over the means of information warfare is now doubtful, the rejection of traditional control over nuclear and other weapons completely excludes any constructive interaction of responsible powers in this area in the future. This is especially true in the context of a sharp escalation of international tensions and the threat of nuclear war in 2022-2023 in connection with the Ukrainian conflict. Nevertheless, the dialogue on this issue should be continued at the diplomatic and expert levels.

The content of the presented monograph reflects exclusively the point of view of its authors, which is due to the novelty and early stage of scientific elaboration of the subject, and to the high degree of its politicization. At the same time, despite the complexity of the topic and the versatility of the analytical calculations, it provides experts with rich food for thought and further scientific research in this area. The monograph is addressed to specialists from various fields of ICT, teachers, students, and graduate students of military and civilian universities, as well as to a wide range of readers interested in security issues.

A.G. Arbatov
Academician of the Russian Academy of Sciences

ABBREVIATIONS

ACCS	– automated combat control system
ACS	– automated control systems
AD	– air defense
AI	– artificial intelligence
APCS	– Automated process control systems
BM	– ballistic missile
BRICS	– Interstate Association of Brazil, Russia, India, China, and South Africa
CPI	– critical public infrastructure
CNI	– critical national infrastructure
EWS	– Early warning system
ICT	– information and communication technology
IIS	– international information security
ISC RAS	– Interdepartmental Supercomputer Center of the Russian Academy of Sciences
MD	– missile defense
MEDIA	– media outlets
MF	– military forces
MFA	– Ministry of Foreign Affairs
MIC	– military-industrial complex
MOD	– Ministry of Defense
NATO	– North Atlantic Treaty Organization
NGO	– non-governmental organization
NW	– nuclear weapons
OEWG	– UN Open-ended Working Group on International Information Security
REW	– radio-electronic warfare
SCO	– Shanghai Cooperation Organization
SNF	– strategic nuclear forces
U.N.	– United Nations
UNGA	– United Nations General Assembly
UNIDIR	– UN Institute for Disarmament Research
WMD	– weapons of mass destruction

INTRODUCTION

This publication continues researching the issues covered by the monographs of the Information Security Problems Group of the Primakov Center for International Security of the IMEMO “Threats to Information Security in Crises and Conflicts of the 21st Century”, “Problems of Information Security in International Military and Political Relations” and others and is aimed at studying the most relevant and important issues of our time related to threats from malicious applications of information and communication technologies (ICT) and finding solutions to strengthen international relations. As in previous publications on this subject matter, the authors present readers with an extensive array of sources, following basic scientific principles: “I believe nothing without proof and leave nothing without proof” and “What is accepted without proof can be rejected without proof.”

Information and communication technologies, that is, all processes of interaction with information carried out through computing devices and various means of communication, are an invariable attribute of everyday life and have an unprecedented impact on economic and political processes, social structures, and international relations. In recent decades, ICTs have become a catalyst for progress in people's lives. The pandemic of SARS-CoV-2 coronavirus, when entire branches of economy, science and education went online, marked the comprehensive significance of new technologies in the modern world in the sharpest terms. All states recognize the significant benefits of ICTs, but the avalanche-like increase in threats in this area has led to a deep awareness that their malicious use can pose a serious threat to peace, international security, and strategic stability. This problem has become even more urgent during the current crisis. Thus, international information security (IIS) has become an integral part of global security. That is why various aspects of IIS have been on the agenda of the First Committee of the UN General Assembly for more than 20 years, which considers issues related to threats to peace and international security and discusses ways to strengthen them.

The first chapter of the monograph presents the results of the analysis of these activities, examines the possibility of creating an international system to ban information (including cyber) weapons, proves the relevance and increasing importance of the study of these processes by the scientific community. The chapter substantiates representation of the IIS issue as a part of a broader topic of international security against the background of global military and political challenges. It forecasts the prospects of discussing the issues of ensuring IIS within the UN. The expediency of developing an Information Security Strategy of the Russian Federation is raised.

Even the current crisis in US-Russian relations, did not see any changes in the activities of the UN platforms – the dialogue remained intact. The First Committee of

the UN General Assembly, as a negotiating platform for international information security, has proved its relevance, as well as the significance of Russia's global initiatives. At the same time, in the long term, expert, academic and business meetings will also be important, where it is possible to search for ways to develop multilateral relations in cyberspace.

One of the most important foundations of IIS is a set of thirteen international rules, norms, and principles of responsible behavior of states, recommended by UN General Assembly Resolution A/RES/73/27 “Achievements in the field of information and telecommunications in the context of international security”, adopted on December 11, 2018. Emphasizing the importance of these regulations, it should be noted that they focus on specific actions of the world community within the life cycle of international conflicts in the field of ICT, in the information as well as in the cyber space, namely in the latent and open phases of cyber conflict. The importance of these discussions, in particular, is confirmed using lethal weapons by Israel in 2019 against targeted hostile computer attacks prepared from the Gaza Strip.

At present, the objective reasons for possible cyber conflicts related to the legal and technical regulation of the security of computer systems have not been sufficiently investigated. First, this applies to software systems, which are a system-forming element of the ICT sphere, its product and at the same time one of the main sources of instability. Considering their lifecycle and role in the process of ensuring IIS, it is necessary to emphasize paragraphs 9 and 11 of the said set of rules, norms, and principles, viz:

- States must take reasonable measures to ensure the integrity of supply channels so that end users can have confidence in the security of ICT products.
- States should promote responsible reporting of ICT vulnerabilities and share relevant information on existing practices to address such vulnerabilities to limit and, where possible, eliminate possible threats to ICTs and ICT-dependent infrastructure.

The second chapter of the monograph is devoted to substantiating the expediency of clarifying the above points in terms of researching the objective factors of emergence and elimination of software vulnerabilities, as well as related threats and risks in the context of international security. At the same time, it is important to note that the issues of transparency of actions of the world community in the field of ICT, exclusive preference of preventive mechanisms of IIS, as well as increasing confidence in the security of software systems through legal and technical regulation are the most relevant and in-demand.

At present, the use of ICT is becoming one of the most important elements of the military and political potential of states, supplementing and sometimes replacing traditional political and diplomatic means and weapons. Amid the parallel processes of the destruction of the arms control regime and the growing contradictions in great

power relations, the importance of military power, military, and dual-use technologies as a key factor of competition and confrontation persists and is even increasing. One of the newest, most complex, and expensive examples of such technologies is supercomputers, the development and improvement of which is rapidly growing and becoming a significant indicator of the capabilities of state and non-state actors. The driver of progress in increase of the computing power of supercomputers in Russia, the USA and other countries is to a large extent the defense structures: the armed forces and the defense-industrial complex.

Supercomputers are actively being deployed to solve key security challenges:

- Maintenance and modernization of the nuclear arsenal in the absence of field tests,
- Optimization of development processes for advanced weapons and military equipment by reducing the number of tests, thanks to qualitatively new modeling capabilities,
- Meteorology on a global scale, in particular for naval forces, allowing the prediction of the state of various environments and the planning of operations, taking into account all necessary external factors,
- Planning of logistical support for the activities of the armed forces and defense industry in normal and extreme modes.

It appears that in all the above areas, threats to global security can be associated, in particular, with a possible lag of one or another country exercising strategic deterrence in this area. In this case, the threat can be realized both in the case of the lagging party realizing the negative prospects and trying to avoid such a scenario by initiating a conflict, and in the case of the leading party having information about the lack of such capabilities of the potential object of aggression and the desire to consolidate dominance by strikes “unreactive”. The problem of the influence of supercomputers on international and national security processes is investigated in the third chapter of this monograph.

The issues of the malicious use of ICTs in the politico-military sphere are the most complex in the process of international discussion. The first reference to IIS threats not only in the civilian sphere but also in the military sphere was made in UN General Assembly resolution 54/49 “Developments in the field of information and telecommunications in the context of international security” of December 1, 1999. Since then, no new international instruments normatively restricting such malicious activities have been adopted by the UN. Therefore, information operations, providing unique opportunities to create a disruptive effect in the politico-military sphere, are constantly being improved, new ICT weapons are being developed to fight against command-and-control systems, intelligence, and electronic warfare, to use ICT to interfere in the internal affairs of states, to affect critical public infrastructure (CNI) facilities, and in particular the facilities of the military industrial complex.

Thus, ICT can provoke the outbreak of interstate military conflict. First of all, because of the disproportionate use of methods of responding to threats and attacks, when the affected party may use real weapons in response. In addition, a conflict can arise by mistake, since there is currently no universal methodology for identifying perpetrators, no criteria for classifying cyber-attacks as an armed attack have been developed, and no universal principles for investigating incidents have been established. The issues of coordination of measures taken in response to information operations recognized as acts of force remain unresolved. As a result, information wars and the use of new technologies can become the detonator of interstate military conflict, even with the use of nuclear weapons (WMD).

ICT already has an impact on strategic stability. Therefore, ensuring global security and strategic stability requires the development and modernization of mechanisms of international governance in the digital space. However, it is not necessary to fundamentally change the underlying principles, as ICT aggravate, complicate, deepen, and modify pre-existing problems in this area. Thus, threats to strategic stability are further enhanced by the development of new anti-satellite systems, remotely controlled robotic strike vehicles, autonomous operation capabilities of various systems and subsystems, automated decision-making systems, etc., which may be subject to ICT-attacks, means of cyber-electromagnetic activities, which are actively being improved in developed countries, primarily in the USA. In addition to technological destabilizing factors, there is also a psychological one, which can be formulated as a loss of fear of nuclear war among society and political elites, which potentially significantly lowers the threshold for the use of weapons. Another dangerous factor is the belief that a local “small” nuclear war is acceptable and can be won. At the same time, damage assessment and development of countermeasures are significantly hampered by the intangibility of ICT, the difficulty of attributing the source of the attack, the possibility of operating under a “false flag”, the wide range of actors that apply malicious technologies: state and nonstate actors, and lone-wolf hackers. Indeed, the problems of developing measures of transparency, trust, and predictability, agreeing, and verifying regarding restrictions or abandoning cyber weapons, now may seem insoluble, but history knows many examples when a crisis has become an important motivation to achieve positive global results. All this increases the level of uncertainty and instability. An analysis of strategic stability in the ICT era is presented in the fourth chapter of this monograph.

A unique feature of today's IIS system that allows us to hope that international cooperation in ensuring global security will eventually prevail is the mutual high ICT vulnerability of many countries in the world. First, the most vulnerable are the states with the most developed ICT domain. Second, in the absence of any restrictions, there are incentives for the creation and mutual use of ICT for politico-military purposes for hostile actions and acts of aggression. Thirdly, the countries with the most developed and therefore vulnerable to cyber influences techno sphere, implement a set of measures aimed, on the one hand, at minimizing the opportunities of opponents for destructive, system-destructive impact on their critical

infrastructure, and on the other – for advance covert preparation of global systems of operational and technical positions (cyber networks) to control and if necessary implement similar impacts on key objects of critical infrastructure of other countries. However, in doing so, there is a serious risk for a country that is a leader in the ICT confrontation, associated with the risk of control, disinformation, and manipulation by a competent adversary. This is possible if the adversary identifies the leader nation's cyber networks, exploits them, and monitors their activities, with no meaningful effort other than to identify and monitor cyber activity.

For these reasons, ensuring international information security in today's digital era has become one of the most important tasks of the global community.

CHAPTER 1

International Security and Information and Communication Technology

1.1. International Information Security as Part of the Global Security Problem

The avalanche-like increase in threats from the malicious use of information and communication technologies (ICT) in the political, military, economic and social spheres have led to a deep awareness of the fact that emerging technologies can bring additional threats to international peace and security. Thus, an issue of international information security, i.e. the state of the global information space, which excludes the possibility of violating the rights of individuals, society and the state in the information sphere, as well as destructive and illegal impact on the elements of national critical information infrastructure¹, has become an integral part of international security as a system of international relations, based on compliance by all States with generally recognized principles and norms of international law and the principles of international security. Thus, the principles of international security, providing for the assertion of peaceful coexistence, ensuring equal security for all States, the establishment of effective guarantees in the military, political, economic, and humanitarian fields, prevention of nuclear and space arms race, respect for the sovereign rights of every people, a fair political settlement of international crises and regional conflicts, certainly include the creation of international information security. In this case, the IIS system, designed to counter threats to strategic stability and to ensure equal partnership in the global digital environment, is understood as a set of international and national norms and institutions, chief among which is the UN, to regulate the activities of various actors of the world information space².

There is every reason to discuss issues related to ICT development in the main areas of UN activity: peace and security, human rights, and sustainable development. Parallel to the work on advances in ICT in the context of international security, discussions in various UN bodies on other aspects include digital cooperation, Internet governance, sustainable development, and human rights (including commercial and personal data protection, freedom of opinion and information), as well as cybercrime and cyberterrorism.

¹ Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security for the Period up to 2020 // Security Council of the Russian Federation. URL: <http://www.scrf.gov.ru/security/information/document114/>.

² Inforum-2014: Results // XVI National Forum on Information Security. URL: <http://2014.infoforum.ru/infoforum-2014-itogi/>.

Since the effective functioning of the collective security mechanism enshrined in the UN Charter is an integral part of international security, the problem of ensuring IIS has become part of the agenda of one of the six main committees of the UN General Assembly (UNGA), which is known as the First Committee dealing with disarmament and related international security issues. It is here that states discuss threats to peace and seek ways to promote it. Therefore, the process of international information security at the UN plays a crucial role and requires in-depth analysis by the expert community. There are several reasons justifying the expediency and importance of discussing IIS issues in the First Committee of the UNGA. Let us name the main ones.

First, the analysis and forecasting of threats from the malicious use of ICT by both states and non-state actors proves the possible impact of new computer technologies on increasing the likelihood of armed conflicts, their escalation and, consequently, of large-scale war. The issue of information security is strategic, and the level of ICT security has a significant impact on the level of strategic stability. It is a threat to international peace, which means that it is necessary to search for additional mechanisms of international governance. Without agreement among states in this area, the growth and scope of such dangers will increase. The discussion of global international processes in the First Committee of the UNGA allows the development of confidence-building measures, principles, and norms of responsible behavior of states in the digital space, which can reduce the risk of armed conflicts and their escalation. Such activities also allow emphasis on other approaches that contribute to stability and security in the ICT space, such as coordination and support for IT security capacity building.

Second, analysis of precedents of ICT-attacks on critical state infrastructure proves that their number and scale are growing exponentially year after year. Cyber-attacks on systems and facilities so vital to a country that their disruption or destruction has an irreversible negative impact on national economic security, healthcare, law and order, governance systems, military facilities, etc., directly threaten the lives of many people and justify the need to discuss responsible government behavior in the information environment.

Third, despite the development of national and regional instruments for regulating and controlling ICT activities, as well as within the framework of international organizations, no state in the world today can consider itself fully protected from trans-border information threats and cannot solve the issues associated with these dangers alone. Therefore, discussion at the global level of the UN is of vital importance. The emphasis on coordination among states and the various stakeholders that are now included in many national and regional cyber and information security strategies is also reflected in the discussion of these issues within the UNGA First Committee. Results at the global level, in turn, influence national and regional norms and principles, which can also contribute to promoting peace and stability in the ICT space.

1.2. Past, Present, and Future International Information Security on the UN Agenda

The issue of international information security was put on the UN agenda at the initiative of the Russian Federation more than 20 years ago. It was first raised in 1998 in a proposal by Russia to sign a statement at the level of the presidents of the Russian Federation and the United States to create *an international legal regime banning the development, production, and use of information weapons*. The document called for coordination, at the UN level, of international community's approaches to the use of ICT for military purposes, definition of terms “information weapons” and “information warfare”, analysis of capabilities of new technologies to modernize existing weapons and create new types of weapons, international cooperation to monitor threats in the information space and development of an international treaty to combat terrorism and crime in the digital sphere. Russia's proposal was not fully accepted, but the issue was outlined in the “Joint Statement on Common Security Challenges at the Turn of the 21st Century”, signed by the presidents of Russia and the United States following the Moscow Summit (September 2, 1998), which acknowledged “the importance of promoting the positive aspects and mitigating the negative aspects of the information technology revolution now taking place”.³

On September 23, 1998, Russia delivered a special message on the issue of IIS to the UN Secretary-General. Attached to the letter was a draft resolution entitled “Developments in the Field of Information and Telecommunications in the Context of International Security” for consideration by the First UNGA Committee on Disarmament and International Security. The draft included a proposal for all UN member states to inform the Secretary General of their views on the problems of IIS, as well as on the advisability of creating an international legal regime to prohibit the development of dangerous types of information weapons. However, Resolution A/RES/53/70⁴, adopted in December 1998, unlike the proposed draft, contained no reference to the threat of the use of information technologies for politico-military purposes, definitions of the terms “information weapons” and “information warfare” (instead, it was proposed that the concepts of “unauthorized interference” and “misuse of information and telecommunications systems and information resources” be defined), provisions on the need to establish a regime prohibiting such weapons, and on the comparability of the impact of the weapons. The latter provision could become the basis for using international experience in the creation of WMD control regimes to develop a corresponding regime for ICT weapons. According to Russian

³ Joint Statement on Common Security Challenges at the Turn of the 21st Century. September 2, 1998 // Consortium Codex. Electronic Fund of Legal and Normative-Technical Documentation. URL: docs.cntd.ru/document/901764255.

⁴ Resolution Adopted by the General Assembly [on the Report of the First Committee (A/53/576)] 53/70. Developments in Information and Telecommunications in the Context of International Security. January 4, 1999 // United Nations. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70&referer=/english/&Lang=R.

participants in the discussion, despite criticism of the original draft resolution by USA and British representatives, the statement by the US delegation noted “the flexibility shown by the main sponsor of the resolution in advancing this initiative”. Since then, the Secretary General has submitted a report to the UN General Assembly on an ongoing basis, reflecting the positions of states on the issue.

Thus, resolution A/RES/53/70 initiated by Russia played a fundamental role in the process of achieving the global goal: discussing and creating a new international regime, i.e., a set of rules, norms, and measures to ensure security of information, ICT, and methods of their use. Since 1998, Russia has been annually submitting to the UN General Assembly resolutions under the general title “Developments in the field of information and telecommunications in the context of international security”. More and more states have been co-sponsoring the resolutions, which have become global in nature and already cover about 100 countries worldwide. For many years, the resolutions were approved by consensus. However, in 2005 – 2008 the voting was held due to significant discrepancies between the Russian Federation and the USA on several issues those connected with the conceptual framework and recognition of the possibility of using ICT for military-political purposes. The USA was the only country to vote against these resolutions during the second term of President Bush Jr. In 2016, the only country that insisted on voting was Ukraine, which ended up “abstaining” rather than “against”. The votes in 2018 – 2019 were the result of the beginning of a new, one might say, post-crisis phase of the IIS process at the UN (Table 1.1).

The tasks set by Russia in 1998 have not yet been resolved but are becoming more and more urgent with each passing year. The search for answers led to the creation of *the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)*, which became the most important mechanism of the First UNGA Committee in the process of addressing information security issues. The first GGE, consisting of representatives of 15 states, began its work in 2004 in accordance with UNGA resolution A/58/457⁵ and was aimed at enhancing the efforts of the international community to study existing and potential threats to information security, possible restrictive measures and to study national and international strategies for global ICT security⁶.

⁵ Resolution Adopted by the General Assembly on 8 December 2003 [on the Report of the First Committee (A/58/457)] 58/32. Developments in Information and Telecommunications in the Context of International Security // United Nations. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/454/85/PDF/N0345485.pdf?OpenElement>.

⁶ Resolution Adopted by the General Assembly on 7 January 2002 [on the Report of the First Committee (A/56/533)] 56/19. Developments in Information and Telecommunications in the Context of International Security // United Nations. URL: <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/476/30/PDF/N0147630.pdf?OpenElement>.

Table 1.1. UN General Assembly resolutions “Achievements in the field of information and telecommunications in the context of international security”, introduced by Russia in 1998 – 2019

Document	Date	Voting results
A/RES/53/70	04.12.1998	Adopted without a vote
A/RES/54/49	01.12.1999	
A/RES/55/28	20.11.2000	
A/RES/56/19	29.11.2001	
A/RES/57/53	22.11.2002	
A/RES/58/32	08.12.2003	
A/RES/59/61	03.12.2004	
A/RES/60/45	08.12.2005	For – 177, against – 1 (USA), abstentions – 0
A/RES/61/54	06.12.2006	For – 176, against – 1 (USA), abstentions – 0
A/RES/62/17	05.12.2007	For – 179, against – 1 (USA), abstentions – 0
A/RES/63/37	02.12.2008	For – 177, against – 1 (USA), abstentions – 0
A/RES/64/25	02.12.2009	Adopted without a vote
A/RES/65/41	08.12.2010	
A/RES/66/24	02.12.2011	
A/RES/67/27	03.12.2012	
A/RES/68/243	27.12.2013	
A/RES/69/28	02.12.2014	
A/RES/70/237	23.12.2015	
A/RES/71/28	05.12.2016	For – 181, against – 0, abstained – 0
A/RES/73/27	05.12.2018	For – 119, against – 45 (Albania, Andorra, Australia, Austria, Belgium, Bulgaria, Macedonia, Canada, Cyprus, Denmark, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Spain, Monaco, Montenegro, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, San Marino, Slovakia, Slovenia, Sweden, Ukraine, United Kingdom, United States, Estonia, France abstained – 14
A/RES/74/29	12.12.2019	For – 129, against – 6 (Georgia, Israel, Canada, UK, USA, Ukraine), abstentions – 45

Source: 53rd to 74th sessions of the UNGA. Resolutions. First Committee. Disarmament and international security issues // United Nations. URL: http://www.un.org/ru/ga/first/53/first_res.shtml...
http://www.un.org/ru/ga/first/70/first_res.shtml...https://www.un.org/ru/ga/first/74/first_res.shtml.

“Questions related to the work of the group of governmental experts on the problem of information security” sent to the UN Secretariat on April 28, 2003⁷, contained specific proposals of the Russian Federation in the context of the activities of the first GGE. The analysis shows that Russia thus laid the foundation for the development of an international, mutually acceptable document aimed at strengthening the IIS. According to these proposals the states should be responsible for any activity in the information space conducted by them or from the territories under their jurisdiction. The basis of the future IIS regime could be the obligation of the member-states to refrain from actions on damaging critical infrastructure of another state, on undermining the political, economic, and social systems, on psychological impact on the population to destabilize the state and society. The draft report, prepared after three meetings of the first GGE in 2004, was not adopted because of serious disagreements, primarily between Russia and the United States.

In 2005, “given the complex nature of the issues under discussion, no consensus was reached on the preparation of the final report”.⁸ Only the procedural report A/60/202 was adopted. The main contradictions were on the following two principal issues. The first concerned the threats from the use of ICTs for politico-military purposes and the negative effect of malicious information technologies on national and international security. The necessity of considering these threats, and, hence, the importance of elaborating a corresponding international document within the framework of the UN First Committee, was pointed out by Russia, Belarus, Brazil, China, Malaysia, South Africa, and South Korea. The United States, the United Kingdom, Germany, and France considered only the criminal and terrorist components of information security to be the subject of discussion at the UN. The second question was the need to study issues related to the content of information flows. Russia and its supporters believed that threats related to information content should be investigated in the GGE, while the USA argued that only technical issues of information infrastructure security, that is, cybersecurity in US terminology, were sufficient. A compromise on these two issues has not been reached so far.

However, the Group of Governmental Experts of the 2nd Convocation, convened in 2009 at the initiative and under the Russian chairmanship⁹, continued to discuss these issues. Limited consensus was achieved. The work of the Group during this period was influenced by the change of the US President, which led to the recognition by the United States of the need to develop a common terminology as

⁷ Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary-General. A/58/373. September 17, 2003 // United Nations. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/523/42/PDF/N0352342.pdf?OpenElement>.

⁸ Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report of the Secretary-General. A/60/202. 5 August 2005. // United Nations. URL: <https://digitallibrary.un.org/record/555369?ln=ru>.

⁹ Resolution Adopted by the General Assembly on 6 January 2006 [on the Report of the First Committee (A/60/533)] 60/45. Developments in Information and Telecommunications in the Context of International Security // 15 July 2011. <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/490/32/PDF/N0549032.pdf?OpenElement>.

well as international norms and mechanisms for controlling the ICT sphere. In 2010, after four sessions, the GGE issued a Report¹⁰ that subsequently made it possible to start a substantive discussion on IIS. The Russian proposals were supported by Australia, Canada, Israel, Japan, and South Korea, despite the criticism of the American delegation. For the first time, these proposals highlighted the threat of states deliberately creating “ICTs as instruments of warfare and intelligence, for political purposes”, the uncertainty in identifying the source of the impact, and the risk of instability and misperception of state responses. This was an important recognition of the problem of information technology for politico-military purposes at the UN level. Further evidence of this was the UN Secretary-General's report of 15 July 2011, A/66/152¹¹, which included responses he received from some governments, including the United States. The US response noted the problem of “the transference of traditional forms of state conflict into cyberspace” and included the states themselves among the threat actors. It also pointed out that “in some circumstances, disruptive activities in cyberspace can constitute an armed attack”. However, the issue of cross-border information flow content has not yet been addressed by the United States in terms of international information security. According to the Russian participants, the activities of the second GGE on IIS were a breakthrough for Russia, which managed to fix the most important aspects for the Russian Federation in the UN agenda. Today we can consider the results of the 2009 – 2010 Group as the first steps to create an international regime of control over information weapons.

Established by UNGA Resolution A/RES/66/24 of 2 December 2011 and comprising representatives of 15 countries, the mandate of the third GGE, which included a study of existing and potential threats in the ICT domain and possible strategies to minimize them. The Group's report, adopted by consensus of all participants in 2013¹², contained recommendations to address existing and potential ICT threats from states, actors on their behalf, and non-state actors. With the leading role of the state, as stated in the document, civil society and business can enhance the effectiveness of this process. Thus, it is a matter of recognizing the principle of state responsibility for malicious activities in the digital space carried out from their territory, which was proposed by Russia in a document sent to the UN Secretariat back in 2003. In addition, the Report recommended that countries adopt voluntary transparency and confidence-building measures and expand international cooperation on information security not only with developed countries, but also with developing

¹⁰ Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Note by the Secretary-General. A/65/201. July 30, 2010. // http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201&referer=/english/&Lang=R.

¹¹ Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the Secretary-General. A/66/152. 15 July 2011. // United Nations. C. 17–25. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/416/93/PDF/N1141693.pdf?OpenElement>.

¹² Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security UN General Assembly. A/68/98. 24 June 2013 // United Nations. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/sgreports/68/&Lang=R.

countries. However, the recommendations contained in the 2013 Report were only concerned with linking the security of the information environment to the existing norms of international law. It was not possible to reach a compromise on the question posed by Russia about the need to adopt additional legal norms in relation to the ICT environment at that time.

The 4th GGE began its work in accordance with UNGA Resolution A/RES/68/243 of January 9, 2014¹³ and included representatives from 20 countries. In addition to its regular tasks, the Group was to further develop rules for responsible behavior of states in the digital space, determine the conditions for applying existing international norms to the ICT environment, and identify instances where additional norms were needed to address the unique characteristics of ICTs. In early 2015, a Letter to the UN Secretary General was sent by the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the UN, with an annex containing improved “Rules of Conduct for States in the Information Space”¹⁴ (the original “Rules of Conduct” were sent by SCO member states to the UN Secretary General during the 66th UNGA session in 2011¹⁵). The new edition included a new Rule 3: “Do not use information and communication technologies and information and communication networks to interfere in the internal affairs of other states and to undermine their political, economic and social stability”. Rule 7 was expanded and clarified, calling for “recognition that the rights one has offline should also be protected online”, possibly with some limitations under Article 19 of the International Covenant on Civil and Political Rights. Additionally, Rule 10 was developed: “Develop confidence-building measures to increase predictability and reduce the likelihood of misunderstandings as well as the risk of conflict. These measures include, among other things, the voluntary exchange of information on national strategies and organizational structures to ensure the information security of the country, the publication of ‘white papers’, and the exchange of best practices wherever practicable and appropriate. The document enshrines the obligation of states not to use ICT to violate international security and to interfere in the internal affairs of other countries, to destabilize their political, economic, and social systems”. The Rules of Conduct call on states to refrain from the use of force or the threat of force in resolving international disputes in the digital space.

¹³ Resolution Adopted by the General Assembly on 27 December 2013 [on the report of the First Committee (A/68/406)] 68/243. Developments in Information and Telecommunications in the Context of International Security // United Nations. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/454/05/PDF/N1345405.pdf?OpenElement>.

¹⁴ Letter Dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General. A/69/723 // United Nations. URL: <https://undocs.org/ru/A/69/723>.

¹⁵ Letter Dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. A/66/359. // United Nations. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/58/PDF/N1149658.pdf?OpenElement>.

The final report A/70/174¹⁶ of the 4th GGE was the most substantive and groundbreaking. In addition to the threats presented in previous GGE reports on IIS, Section II, “Existing and Emerging Threats”, notes for the first time that not only are some states increasing their ICT capabilities for military applications, but also that “the use of ICT in future conflicts between states is becoming more likely”. This is an important diplomatic and political outcome that Russia has long sought to achieve. In addition, for the first time the Report refers to real, rather than hypothetical, cases of ICT-attacks on critical state infrastructure, which are among the “most damaging attacks using ICT”. It is logical to assume that this wording emerged as a result of the analysis of complex multi-targeted cyber-attacks on Iranian nuclear facilities in 2010 – 2012, behind which state structures were very likely. The issue of terrorist use of ICTs, not only for recruitment, financing and so on, but also for attacks on ICT information facilities and related infrastructure, is of great importance in the document. The crucial point about the need not to legalize and regulate conflicts in the ICT space, as suggested by the United States and its partners, but to prevent such conflicts, was supported in the Report by 20 countries that supported the applicability of international law to the digital space.

The main outcome of the work of the 4th GGE was paragraph 12 of the final Report on the adoption of the “Rules of Conduct on International Information Security”.

The 5th GGE on IIS, which began its activity in 2016 in accordance with Resolution A/RES/70/237¹⁷, included representatives of 25 countries. Thus, since the convening of the first GGE, the number of GGE member states has increased from 15 to 25. And the number of States wishing to participate in the GGE has grown exponentially. An important task of the GGE, according to Russian representatives, was the inclusion of the “Rules of Conduct” in the next UN General Assembly resolution “Developments in the field of information and telecommunications in the context of international security”, which would make the “Rules” part of international “soft” law and initiate the formation of a system of international standards in this area, ensuring a more stable world order. The hope for the possibility of discussing IIS issues at the meeting of the presidents of Russia and the United States in 2017 and for the approval of the “Rules of Conduct” appeared after the accession to power of the USA President Donald Trump. Even the possibility of signing a bilateral agreement on the prevention of incidents in information space, like the documents that deal with incidents at sea and in airspace, was considered. However, in particular, due to accusations of Russian cyber interference in the USA

¹⁶ Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174/. 22 July 2015 // United Nations. URL: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=R

¹⁷ Resolution Adopted by the General Assembly on 23 December 2015 [on the Report of the First Committee (A/70/455)] 70/237. Developments in Information and Telecommunications in the Context of International Security // United Nations. URL: <https://undocs.org/ru/A/RES/70/237>.

presidential election, the meeting did not take place, and hopes for the inclusion of the “Rules of Conduct” in the next resolution were not fulfilled.

2017 was a crisis year for the Group of Governmental Experts on IIS at the UN. The 5th GGE concluded its work on June 23, 2017, in New York. The final meeting of the GGE was supposed to adopt a final report, as it had done previously in 2010, 2013, and 2015. However, consensus could not be reached; for the first time since 2004, the final document was not adopted. The draft report submitted by the German chairman for consideration by the GGE was not supported by representatives of Russia, the BRICS and CIS countries, and several developing countries. One of the principals, if not the main reason for the failure, was significant contradictions between Russia and the United States on the issue of the right of self-defense in response to cyber-attacks.

For example, NATO decided to apply Article 5 of the Washington Treaty, that is, to respond with all available means, including military, in response to a cyber-attack against a member of the Alliance¹⁸. And in May 2019, USA partner Israel launched an airstrike against a building in the Gaza Strip, where the Israeli armed forces claimed that a cyber-attack was being prepared to damage the quality of life of its citizens¹⁹. Thus, it is no longer a hypothetical, but a real use of military force, not even in response, but to prevent cyber-attacks. Russia believes that the sources of cyber threats should not be identified by states without evidence. Some states, particularly Cuba, believe that a cyber-attack does not amount to an armed attack, and therefore the right of self-defense should not be used in such cases. An additional “grey area” is also the right of self-defense against attacks by non-state actors.

At the end of 2018, the UN First Committee established two parallel deliberative processes: the UN Open-ended Working Group (OEWG) on IIS²⁰, and the UN Group of Governmental Experts on Developments in Information and Telecommunications in the Context of International Security (GGE).²¹

Regarding equitable geographic distribution, regional diversity, and participation in previous GGEs, the 6th GGE was formed at the suggestion of the

¹⁸ The North Atlantic Treaty. Washington D.C. April 4, 1949. URL: https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

¹⁹ Doffman Z. Israel Responds to Cyber-Attack with Air Strike on Cyber Attackers in World First // Forbes. 2019. May 6. URL: <https://www.forbes.com/sites/zakdoffman/2019/05/06/israeli-military-strikes-and-destroys-hamas-cyber-hq-in-world-first/#34426905afb5>.

²⁰ Resolution Adopted by the General Assembly on 5 December 2018 [on the Report of the First Committee (A/73/505)] 73/27. Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27.

²¹ Resolution Adopted by the General Assembly on 22 December 2018 [on the Report of the First Committee (A/73/505)] 73/266. Advancing Responsible State Behavior in Cyberspace in the Context of International Security // United Nations. URL: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/266.

USA and was composed of 25 countries²². The GGE meetings was closed and do not include any other governmental or nongovernmental observers. However, the GGE resolution required consultations with several regional organizations²³. GGE decisions was to be made by consensus, the results of the meetings are generally not published, but a final report was submitted to the 76th UNGA at the end of 2021.

The resolution on the OEWG, which began work at the initiative of Russia and to which any country could become a member, provides for the possibility of amending the existing “Rules of Conduct” and adding new items to them, organizing regular discussions with experts from various fields, as well as issues of malicious content.²⁴ With a mandate to produce a consensus report at the end of 2020 at the 75th UNGA based on the results of four sessions and two inter-session consultations, the OEWG is uniquely positioned to find common ground. The March 2020 “Preliminary Draft Report of the OEWG on Developments in Information and Telecommunications in the Context of International Security”²⁵ notes that the problem of IIS spans many fields and disciplines, and therefore it is appropriate to use the results of exchanges with representatives of intergovernmental and regional organizations, NGOs, business, and science. Based on the analysis of ICT threats to international security and stability, the OEWG confirmed the growing trends toward the use of ICTs for malicious purposes, which can hinder the benefits of such technologies. Moreover, in the process, the group recognizes the individual and shared digital responsibilities of states, the unequal access of countries to ICTs and, therefore, the need to reduce such inequalities, and emphasizes the importance of reducing the “gender digital divide” in IIS decision-making processes.

Both groups, recognizing the importance of the involvement of business and academia and nongovernmental organizations (NGOs), plan to discuss a code of conduct for states, international mechanisms to combat ICT threats and the application of international law to the digital environment. However, the new format of the IIS discussion was more complex than before. The main contradictions between Russia and the United States at this stage related to a key issue: Russia called for the development and adoption of legally binding rules of conduct for states, thus incorporating them into international law, while the United States viewed existing law as an effective and sufficient instrument for regulating ICT activities. On the other hand, the new format provided a more effective complementary discussion

²² Kenya, Mauritius, Morocco, South Africa; Jordan, India, Indonesia, Kazakhstan, China, Singapore, Japan; Romania, Russia, Estonia; Brazil, Mexico, Uruguay; Australia, Great Britain, Germany, Netherlands, Norway, USA, France, Switzerland.

²³ The GGE Requires Consultation with Several Regional Organizations, Including the African Union (AU), the European Union (EU), the Organization of American States (OAS), the Organization for Security and Cooperation in Europe (OSCE), and the Association of Southeast Asian Nations (ASEAN).

²⁴ Methodological Issues of Application of Norms, Rules and Principles of Responsible Behavior of States to Promote an Open, Secure, Stable, Accessible and Peaceful ICT Environment. Edited by A. Streltsov, E. Thicke, 2020. URL: http://namib.online/wp-content/uploads/2020/07/Brochure_IKT_rus_view.pdf.

²⁵ Initial “Pre-draft” of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf>.

process. Moreover, even the presence of some competition between the GGE and the OEWG motivated each group to reach more effective agreements and solutions.

The results of the GGE and OEWG had a significant impact on information security trends and policies on a global scale. Therefore, scientific analysis of these processes was as relevant as possible.

In 2021, important positive changes have taken place at the international level. The UN adopted the final reports of the OEWG and the 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, significantly different from traditional spaces.²⁶

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. It was assumed that this would contribute to improving the effectiveness of countering existing and potential threats to international security in the information and communication environment.

On December 6, 2021, the UN General Assembly by consensus adopted the Russian-US 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.²⁷

Even the current crisis in Russian-US relations, which began in 2022, did not stop the UN's activities in providing IIS – the dialogue has been preserved. The OEWG, as a negotiating platform for international information security, has proved its relevance, as well as the significance of Russia's global initiatives.

One of the main issues is still the lack of a unified international legal regime regulating the ICT space, since today only some generally accepted norms of

²⁶ 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. URL: <https://front.un-arm.org/wpcontent/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>.

²⁷ 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. URL: <https://documents-ddsny.un.org/doc/UNDOC/GEN/N21/336/94/PDF/N2133694.pdf?OpenElement>.

international law and various domestic legislation are applied. At the same time, it should be noted that there are contradictions in these documents, which can be used by various actors in their own interests, including malicious ones. In this regard, three areas of work on IIS remain the main focus of both groups: the applicability and sufficiency of international law; the currently non-binding norms of behavior of countries, the so-called Rules of Conduct or Code of Conduct in the World Digital Space; and confidence-building measures between states in the ICT environment. A new important trend is likely to be the initiative to create and analyze common repositories of data with the positions of states on the application of international law to the use of ICTs in the context of international security, as well as on the practice of such application. This information is proposed to be submitted on a voluntary basis to *the UN Institute for Disarmament Research (UNIDIR) Cyber Policy Portal*. It is logical to assume that such an approach should not cause serious controversy, as it aims to reach a common understanding of the applicability of already agreed norms and assess the need to develop new ones, as well as to motivate countries to participate in this process. However, its success will depend on the quantity and quality of the information gathered and on the professionalism of the analysts. It is advisable to expect useful results if modern, as objective as possible quantitative methods for analyzing the necessary and sufficient data are used.

In this context, another ICT challenge arises, related to the lack of efficiency of methods for analyzing textual information as compared to the processing of structured numerical information. The type and structure of the data provided to *the UNIDIR Cyber Policy Portal* must be unified and deeply thought-out. And the data itself should exclude politicization of the process as much as possible. However, this is unlikely to be fully achievable. Therefore, a new level of high-performance analytics, including unstructured textual information in the analysis, is needed to obtain objective results. The ability to extract useful insights from the unstructured textual information provided will be a key challenge in this new UN process.

An additional tool of textual analysis could be an academic analysis to compare the data provided to UNIDIR with the information on precedents for the application of legal norms to the ICT space that are discussed at international and domestic conferences and at events of institutions and organizations. This will make it possible to identify real concerns and pressing issues that may not be voiced in the information officially provided to the UN. Then the so-called feedback from states will make it possible to draw useful conclusions, which should subsequently become part of the agenda of the UN groups in the relevant area.

Currently, methods to solve such problems are actively developing based on machine learning and artificial intelligence (AI). These are technologies for obtaining information from unstructured source text by converting them into a set of structured data in a computer-friendly format. As a rule, such methods include syntactic and linguistic analysis, categorization, clustering, extraction of concepts (entities), modeling relationships between entities, thematic indexing, content analysis, studying

frequency distributions of words, annotation, etc. Interpretation of the results also takes place using data mining techniques. Such ICT today is already widely used in business, science, public administration, security, and intelligence systems. Thus, if modern cyber technologies are applied directly to international information security at the UN, this will be the best evidence of support for modern peaceful ICT as opposed to countering their malicious use.

Disagreement over the advisability of developing special international legal norms applicable to the use of ICT for military purposes continues to have a negative impact on the compromise between states and UN groups. Considering the problem as irrelevant at this stage, the US believes that sufficient practical experience in incident management must first be accumulated. Russia, on the other hand, remains convinced that the main goal should be to prevent the use of ICTs for military and political purposes.

Serious diplomatic efforts in the work of both groups will require the following issues:

- the applicability of international law to ICT-attacks in peacetime,
- control of the proliferation of information weapons,
- control of dual-use ICTs,
- the applicability of the UN Charter to cyberspace, in particular the right of self-defense,
- preventive measures to prevent ICT-attacks, in particular the issue of notification before applying countermeasures,
- ICT-attack attribution,
- the use of ICTs to violate sovereignty and interfere in the internal affairs of states,
- the obligation of states not to allow their territory to be used for ICT-attacks by state or non-state actors against other states,
- tools for coordinating responsible behavior of states in the ICT space,
- the principle of the binding nature of the “Rules of Conduct” and the possibility of their expansion,
- the role of the UN in developing confidence-building measures,
- basic human rights in the process of applying new norms and rules of behavior in the ICT space,
- building information security capacity,
- developing a unified conceptual framework for IIS,
- an assessment of the equal applicability of the Rules of Conduct in wartime and peacetime,
- functions and coordination of the work of the GGE and WGOS.

When analyzing and forecasting the prospects of IIS, it is necessary to take into account the most important political characteristics of the current stage, which do not contribute to the efficiency of the process. They are related to the lack of cooperation of the “great powers” in this field, to the lack of transparency in relations between

states, which makes it difficult to assess the commitment of countries to the norms and principles of behavior in the digital space. The lack of clear incentives to comply with norms and the absence of concrete benefits from it significantly hinder the development of an international regime for the management and control of harmful ICTs. Thus, expanding research to evaluate existing rules applicable to the information space, as well as to identify additional norms, is now as relevant as possible. At the same time, it would be advisable to work on the classification of threats in this field at the international level, as well as on the monitoring of dangerous ICT incidents. Interdisciplinary and multidisciplinary analysis of existing threats to IIS, scientific forecasting and planning of future dangers by the scientific and expert community thus becomes even more important.

1.3. Political & Military Issues of International Information Security

One of the most important current trends is related to the fact that for most countries of the world the strategic importance of the security of ICT systems, which have become crucial factor in ensuring the sovereignty, defense capabilities and security of the state. At the same time, today we are talking about the threat of the accelerated development (race) of information armaments. According to some estimates, more than 30 states already possess offensive cyber weapons.²⁸ ICT can provoke the outbreak of interstate military conflict, primarily because of the possibility of disproportionate use of methods to respond to threats and attacks: the affected party may use real weapons in response. In addition, the conflict may arise by mistake because there is currently no universal methodology for identifying perpetrators, no criteria for classifying cyber-attacks as an armed attack have been developed, and no universal principles for investigating incidents have been formed.

Another global issue is information security of military facilities as part of critical infrastructure (CI), which includes systems and facilities that are so vital to the country that their disruption or destruction would have an irreversible negative impact on national and economic security, health care, law, and order, etc. The *security of CI* in this context is understood as the *protection against threats, implemented using special information technologies for the destruction or for inadmissible use of these objects*. Even if these objects are not directly connected to the Internet, automated process control system (APCS) devices used for remote control over secure communication lines can be hacked because of an attack on other objects, on which the APCS is functioning. Isolation of the network from external systems, which was considered an immutable requirement 10 – 15 years ago, is no longer seen as an effective protective measure, as it has become uneconomical and difficult to implement in practice. Therefore, the threat of a large-scale complex attack on CI is more than real and rapidly growing. At the same time, it is necessary

²⁸ Romashkina N.P. Strategic Stability: New Challenges of the Infosphere // Russian International Affairs Council. 2017. November 23. URL: <http://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery/>.

to take into account the close interconnection of civilian support systems of the CI with the military infrastructure.

Today dozens of countries already have software to attack CI facilities. At the same time, the threat indicator for the APCS is currently assessed by experts as critical or high. In 2019, monthly cyber-attacks on one in four computers at industrial enterprises in Russia were recorded. Malware is currently being developed in many countries, but 83% of all sites used to spread “malware” are in just 10 states. The leader of this ranking is the USA, where a quarter of all infection sources are located.

Such “malware” can target government agencies, banks, satellite, oil and gas, transportation systems, power and nuclear plants, communications systems, ports, airports, and military facilities, with dire consequences at both the national and global levels. Thus, such malware is a promising strategic weapon, and the increasing complexity of critical infrastructure hardware and software leads to an increased likelihood of errors and vulnerabilities that can be exploited by adversaries.

Global trends that increase threats to such facilities include the use of personal mobile devices at CI facilities; the transition to digital production and process control systems; the connection of office and industrial corporate networks to the Internet; and the complexity of transcontinental supply chains for production and process control software systems. These trends apply to all CI facilities. But of greatest concern are threats to the automated combat control system (ACCS) of nuclear weapons (NW) – communications, command, and control (C3) in Western terminology. Threats that create the problem of ensuring the ICT security of military-industrial complex facilities, signs of the presence and possibility of implementation of these threats are presented in Table 1.2.

Table 1.2. The problem of ensuring information security of military facilities as part of the critical infrastructure of the state

Threat	Signs of a threat	Possibilities of delivering on the threat
Development of ICT tools for malicious effects on military-industrial complex facilities	The presence of ICT threats to various elements of the military organization and infrastructure. The most important: strategic weapons, EWS, nuclear weapons command and control system, missile defense, AD.	<ul style="list-style-type: none"> • Cyber-attacks on military or related civilian infrastructure, • physical damage to the software, element base, communication lines and networks of the military facility,
	Increased use of remotely controlled robotic strike vehicles, AI for military purposes, automated	

	<p>decision-making systems, etc., that can be subjected to cyber-attacks.</p>	<ul style="list-style-type: none"> • remote “logical” harm through malware, “logic bombs,” etc., • Intentional or unintentional remote harm through computer networks (including the Internet) or through contact with a computer, • cyber espionage and the creation of cyber networks, • cyber-sabotage, • creating uncertainty among commanders and personnel about the smooth and efficient operation of systems.
	<p>The conversion of strategic forces in various countries to digital information transfer technologies, making them more vulnerable to technical errors and deliberate cyber-attacks.</p>	
<p>Reducing the level of strategic stability</p>	<p>The impact of ICT development on the growth of probability:</p>	
	<ul style="list-style-type: none"> • of an erroneously authorized ballistic missile (BM) launch, 	
	<ul style="list-style-type: none"> • the use of the Internet to provide false information from the Ballistic Missile EWS about enemy ballistic missile launches due to the growing sophistication of cyber-attacks, 	
	<ul style="list-style-type: none"> • damage or destruction of communication channels, interference in the control system of armed, including nuclear forces, 	
	<ul style="list-style-type: none"> • reducing the confidence of military decision makers in the operability of the command, control, and command systems of the Armed Forces. 	
	<p>The impact of the increased likelihood of disabling or destroying nuclear weapons through ICTs on the future of nuclear disarmament and nonproliferation processes.</p>	
	<p>Influence of ICT factors on the level of strategic stability.</p>	

Source: Romashkina N.P., Markov A.S., Stefanovich D.V. International Security, Strategic Stability and Information Technologies – Moscow, IMEMO, 2020. – 98 p. (in Russian). URL: <https://www.imemo.ru/files/File/ru/publ/2020/2020-017.pdf>.

1.4. Russia's Problems in the Field of Information Security

The analysis of global ICT threats to international peace and security leads to the conclusion that it is advisable to create a system of deterrence of the use of information weapons, and, consequently, global information warfare. Proceeding from the fact that methods using modern ICT are becoming an important element of the military potential of states, supplementing conventional military means, and new technologies can become a detonator of unleashing an interstate military conflict, one of the most important tasks of the state in the process of building a system based on the concept of deterrence, is to improve the legislative and technological support of national information security.

One of the most important tasks in this area today is to improve the necessary legal framework. Its solution may include:

- 1) collection and analysis of information about the state and issues of Russian legislation regulating the security, development, and use of digital technology,
- 2) monitoring of the legislation of Russia and foreign countries regulating information security issues, which should be conducted on an ongoing basis by experts proactively and at the request of parliament,
- 3) improvement of legislation regulating the development and use of digital technologies, information-psychological and information-technological security, which will lead to the continuous improvement of state policy in this area.

As part of the scientific approach to the issue of legislative provision of information security, the following signs of the issue can be identified.

1. Inconsistency between modern ICT (big data, cloud technologies, supercomputers, AI, etc.) and Russian legislation regulating information security, development, and use of digital technologies. For example, despite the avalanche growth of opportunities for the collection of citizens' personal data on the Internet (personal data is part of it) and the use of their arrays (the so-called “big data”), this area is still not regulated and not introduced into the legal framework. Arrays can be used for malicious purposes, including politico-military ones. In addition, this data is accumulated and can be used against a person many years later. Thus, the legislative regulation of such processes is part of the information security of the state.

2. The high cost and complexity of technical protection of personal data information systems.

3. Ambiguity of some provisions of the laws, which are interpreted differently by state regulators and operators and require specification, clarification, and explanation. In addition, there is an issue of terminology. The UN uses an accommodating term “information and communication technologies”, ICT, at the initiative of Russia. Official documents of the Russian Federation also lack the term

“cyber”, “cybernetic”, “cybersecurity”, etc. But the term “cyber” is actively used in technical regulations and GOSTs.

4. *Dependence of information security of the Russian Federation on foreign suppliers* of software and hardware components and equipment. Thus, Internet technologies (browsers, search engines, social networks, operating systems, etc.) are outside Russian control. This creates additional security threats. Therefore, the state should have a complete technological chain, from the processor to the final software.

5. *Vulnerability of information security elements due to the lack of qualified specialists, software, and insufficient coordination with law enforcement agencies.*

6. *Being ahead of the development of attacking ICT technologies compared to security technologies of ICT industry leaders* (in particular, with respect to information containing state or commercial secrets, as well as servers of government agencies and other critical state infrastructure), which requires constant monitoring of the legislation of the Russian Federation and foreign countries regulating information security issues.

7. *Risks of damage to the reputation of the state due to the malicious use of ICTs in the context of political competition*, which can be expressed not only in reputational but also in financial losses.

8. *The need to adapt Russian legislation to global threats to information security* (in particular, it may be the development and adoption of the Information Security Strategy of the Russian Federation).

9. *The need to improve the legislation of the Russian Federation*, contributing to the creation of an international regulatory framework to combat ICT threats.

10. *The expediency of harmonization and unification of legislations of states - allies and partners of the Russian Federation* in the field of information security amidst formation of the global information space and the accelerated growth of global threats to information security.

At the present stage, one of the main strategic priorities of state policy has become an increase in the importance of information security as a systemic element of governance, as well as the improvement of regulatory and legal support in the ICT sphere. At present the legislation of the Russian Federation in the field of ICT is going through a growth stage. Thus, ***the goal*** is to create a mechanism to align the process of developing laws with current realities and the progress of ICT to ensure information security of the state.

The main *challenges* to achieving this goal are related to the quality of public administration and the level of information security, which are generally determined by the ability of the state:

- 1) ensure the functioning of information resources and flows necessary and sufficient for sustainable livelihoods and development to withstand technical and psychological threats,
- 2) fully protect state and trade secrets from unlawful encroachments,
- 3) maintain the efficiency of work, the possibility of “self-development” and adequate responses of the system to increasing challenges,
- 4) to ensure the sustainability and security of the state against ICT threats in the politico-military sphere.

In this case, the primary tasks of the expert community are:

- 1) preparation of proposals and recommendations incorporating the results of research using traditional and modern interdisciplinary methods to identify intra-and inter-systemic contradictions, socio-legal and political problems in the field of ICT,
- 2) development of *a methodology* for identifying legal problems in the ICT sphere, as well as general socio-political conditions for the preparation and adoption of legislative acts for continuous improvement of legislation in the field of information technology.

Thus, the activity of experts from various fields should result in the creation of a permanent mechanism that will allow the process of drafting laws to be coordinated with existing realities and the progress of ICT to ensure information security of the state. In the foreseeable future, it is advisable to adjust this mechanism to *a comprehensive approach*:

- 1) amending existing legislation based on the analysis of application practices and new conditions related to the accelerated development of ICTs,
- 2) simultaneous work on the preparation of the Information Security Strategy of the Russian Federation,
- 3) preparation of new normative legal acts after the release of the Information Security Strategy of the Russian Federation.

The expediency of creating a system of deterrence of malicious ICT at this stage is confirmed by the constant improvement of the regulatory framework in the states with the most developed ICT, which is the basis of their policy in the information space. Thus, in March 2023 in the United States, a new National Cybersecurity Strategy was approved²⁹, in which Russia is still indicated as one of the main opponents of the United States. The previous cyber strategy was adopted in the USA in September 2018.³⁰

²⁹ National Cybersecurity Strategy. March 2023. The White House, Washington. URL: <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

³⁰ National Cyber Strategy of the United States of America. September. 2018. URL: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

In addition to the National Cyber Strategy, the USA has *the US Department of Defense Cyber Strategy* and *the US Joint Cyber Command Strategy* (a functional structure comprising more than 6,000 specialists from various military departments and commands) called “Conquering and Holding Dominance in Cyberspace”³¹. Also important in this context is NATO’s decision to invoke Article 5 of the Washington Treaty, which provides for collective self-defense, in the event of a cyber-attack, although it is emphasized that not every cyber-attack will invoke Article 5³². Consequently, the US. has a comprehensive strategic program to ensure and maintain information superiority by enhancing its capabilities and comprehensively reducing the capabilities of other actors. Thus, today we are no longer talking about the preconditions for the emergence of a new sphere of competition in the information space, but about the fact that a new era of strategic confrontation – ICT confrontation – with the indication of the leader in the face of the United States, opponents, among them named Russia, a detailed step by step system plan of action, as well as specific measures of counteraction and “punishment” of opponents – has already occurred.

Under such conditions, ensuring a secure ICT environment as part of the global international security system requires Russia to take special measures. In particular, it is advisable to raise the question of the develop a Russian Information Security Strategy. It is also justified by the fact that strategic documents that legally determine the directions and prospects of state development (and ICT is one of the most important characteristics of development) play a special role at the present stage and create a legal basis for innovative development, defining the foundations of state policy.

The most important characteristics of a strategy, unlike all other types of documents, in particular, are:

- 1) targeted approach to development, based on the definition of the most important goal and objectives for its achievement, the priority of which determines the content and essence of the results of action for the development of the relevant area,
- 2) a systematic approach to implementation, providing for the solution of these tasks and, accordingly, the maximum coverage of all the main areas to be involved in the implementation of the strategic directions of public policy in the relevant area,
- 3) a set of specific coordinated and interrelated activities, tools, and resources to achieve the results of these tasks in each of the priority areas,
- 4) actions according to a single stage-by-stage plan with clearly defined targets and indicators at each stage, as well as a developed system of financing of the main activities,

³¹ Department of Defense Cyber Strategy 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_

³² NATO is Ready for Collective Defense in Cyber Attacks, But Not in All Cases. // RIA Novosti. 2016. June 14. URL: <http://ria.ru/world/20160614/1447513284.html#ixzz4Be5c0CYs>.

- 5) monitoring the implementation of the strategy and the application of a system of legal control measures for the achievement of final and intermediate results.

Thus, the strategy is usually developed within the framework of *defining the goal and setting tasks, forecasting, planning, and programming* at the federal level, at the level of subjects of the state and at the level of municipalities. Obviously, ***the Strategy*** as a system of formally defined provisions that enshrine the strategic goal, tasks, and directions of activities of public authorities to achieve it, means and resources that can be spent on it, is significantly different from ***the Doctrine***, which is essentially a philosophical, political, or legal theory, concept, teaching, system of beliefs, guiding theoretical or political principle.

The Information Security Strategy of Russia can become the foundation for the development of the information sphere in the country, providing organizational, legislative, and economic conditions and guarantees of a safe evolutionary process. The document is intended to formulate the goal and objectives of development, as well as protection against threats and risks in the information space. The strategy may describe a comprehensive systematic approach to the implementation of these goals and objectives, coordinated and interrelated actions and activities that would be based on target indicators and indicators at each stage of implementation. An important part of the strategy is also a clearly defined system of monitoring and measures of legal control over the achievement of final and intermediate results. Such a document can play an important role in shaping the ICT arms control regime.

CHAPTER 2

Software Systems and International Information Security

2.1. Security Flaws of Software Systems

One of the most important topics of international information security is a set of thirteen international rules, norms, and principles of responsible behavior of states, recommended by the UN General Assembly Resolution A/RES/73/27 “Achievements in the field of information and telecommunications in the context of international security”³³. Emphasizing the significance of these rules, it should be noted that they focus on specific actions of the world community within the life cycle of international ICT conflicts (including in information and cyberspace³⁴), namely in the latent and open phases of cyberconflict. The importance of such discussions, in particular, is confirmed using lethal weapons by Israel in the Gaza Strip in response to the hostile, targeted computer attacks by Hamas³⁵.

However, the objective causes of cyber conflict associated with legal and special (technical) regulation of the security of computer systems are currently very poorly researched. First, this applies to software systems, which are a system-forming element of the ICT sphere, its product and one of the main sources of instability. Considering the life cycle of software systems and their role in the process of ensuring IIS, it is necessary to specifically emphasize paragraphs 9 and 11 of the aforementioned set of rules, norms, and principles, namely:

- states must take reasonable measures to ensure the integrity of supply channels so that end users can have confidence in the security of ICT products,
- states should promote responsible reporting of ICT vulnerabilities and share relevant information on existing practices to address such vulnerabilities to limit and, where possible, eliminate potential threats to ICTs and ICT-dependent infrastructure.

This chapter is devoted to substantiating the feasibility of clarifying and modifying these points in terms of researching the objective factors for the

³³ Resolution Adopted by the General Assembly on 5 December 2018 [on the Report of the First Committee (A/73/505)] 73/27. Developments in Information and Telecommunications in the Context of International Security // United Nations. URL: <https://undocs.org/ru/A/RES/73/27>.

³⁴ In addition to the ict terminology base, the chapter uses established definitions in the field of cybersecurity adopted by the international communities in which Russia participates, such as ISO, IEC and ITU, to ensure the completeness of the study.

³⁵ Israel Defense Forces. Official IDF Twitter. URL: <https://twitter.com/idf/status/1125066395010699264>.

emergence, exploitation, and elimination of program vulnerabilities, as well as the threats and risks associated with them in the context of international security.

It should be added that the issues of transparency of the global community's actions in the field of ICT, the exceptional preference for preventive mechanisms of IIS³⁶, as well as increasing confidence (through legal and technical regulation) in the security of software systems in the context of international security are the most relevant and in-demand.

2.1.1. Terminological apparatus of program security

In general terms, *international information security* is understood as the state (property) of protection of the global information space from threats in the information sphere. Unfortunately, for political reasons, threats in the information sphere are interpreted differently by different countries, which precludes a precise definition.

With respect to the distinction between information assets and corresponding threats of a technical nature, it is possible to distinguish the concept of *information security of computer systems* (as a state of protection of assets from threats of integrity, availability, and confidentiality) and further its sub-property – *the security of software systems*.

Cybersecurity is understood as *the property of cyberspace assets security*, but at present there are also different interpretations of the degree of virtuality (i.e., boundary) of cyberspace and the class of threats (targeted, military or any other nature) considered. For example, different interpretations of cyberspace are presented in many documents of national and international organizations and communities, such as the US Department of Defense, ITU, ISO and others.

When studying the security of software systems, first, the concept of *secure software* is distinguished, which is understood as *software that is created using security measures aimed at eliminating vulnerabilities during the development and implementation, as well as their timely elimination in case of detection during the life cycle of systems*. Based on the theory of information security, software security factors should be identified at the stages of its life cycle, namely: defect, vulnerability, threat, and risk (Figure 2.1).

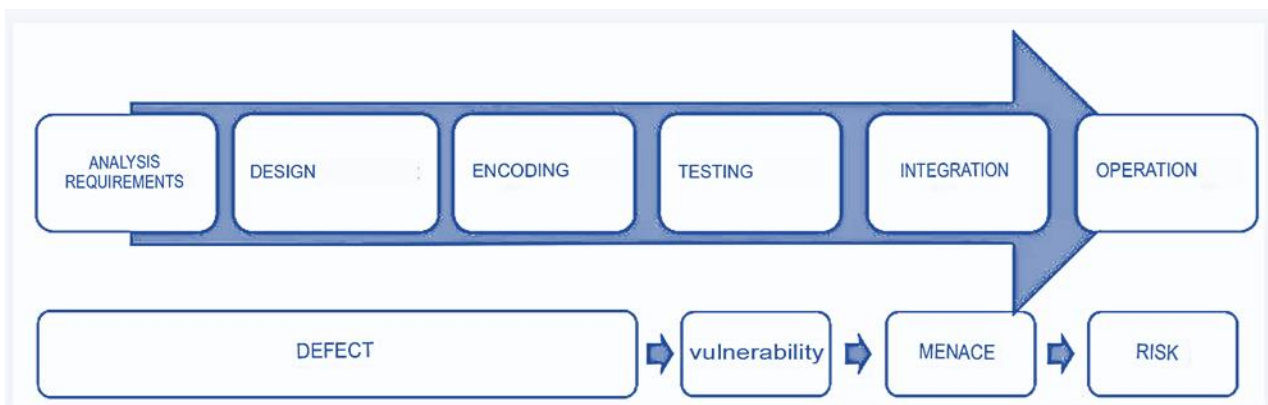
A defect (flaw, incorrectness, weakness) is *any error made during the design or implementation of a program which, if not corrected, could cause a program vulnerability (i.e., potentially affect the level of information security of the system)*.

³⁶ Sherstyuk V.P. Confidence-Building Measures Should be Expanded, Increased. Only Then Will It Be Possible to Achieve Something // International Life. 2019. April 25. URL: <https://interaffairs.ru/news/show/22336>.

A vulnerability is a *flaw in a program that can be used to implement information security threats*. The presence of a vulnerability can constitute **a threat to an information resource (or asset)** if it can be implemented to reduce the level of information security of the system.

The combination (as a rule, multiplication) of the magnitude of the possible damage and the probability of the threat realization constitutes the risk of information security systems.

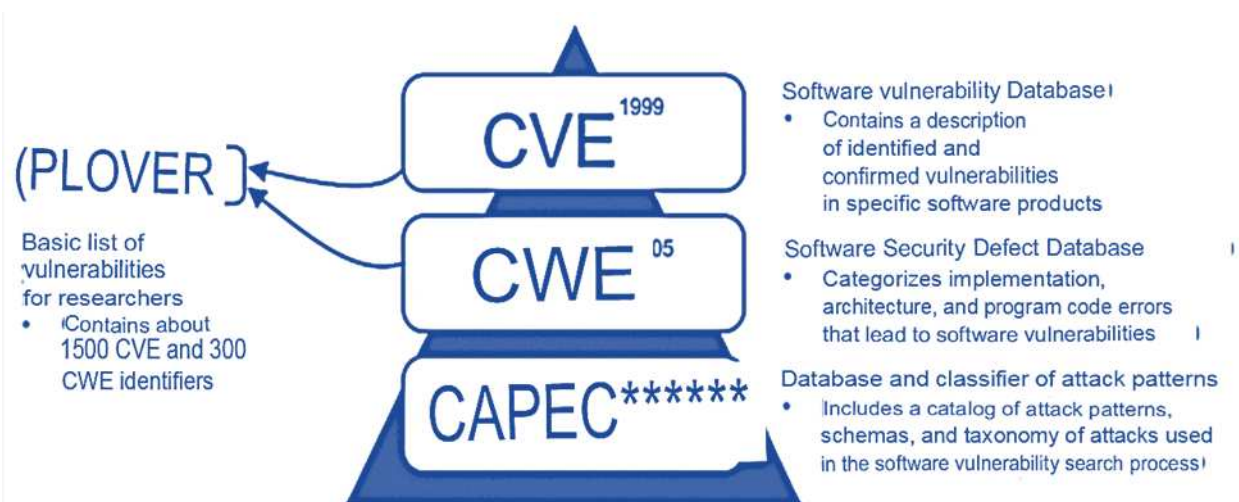
Figure 2.1. Software security factors



Source: Picture built by the author.

It can be argued that, at present, the conceptual base of software security has developed and is at the appropriate level of iterative development of the modern information security paradigm. This is evidenced by modern systematics of defects, vulnerabilities, and attacks (e.g., Figure 2.2).

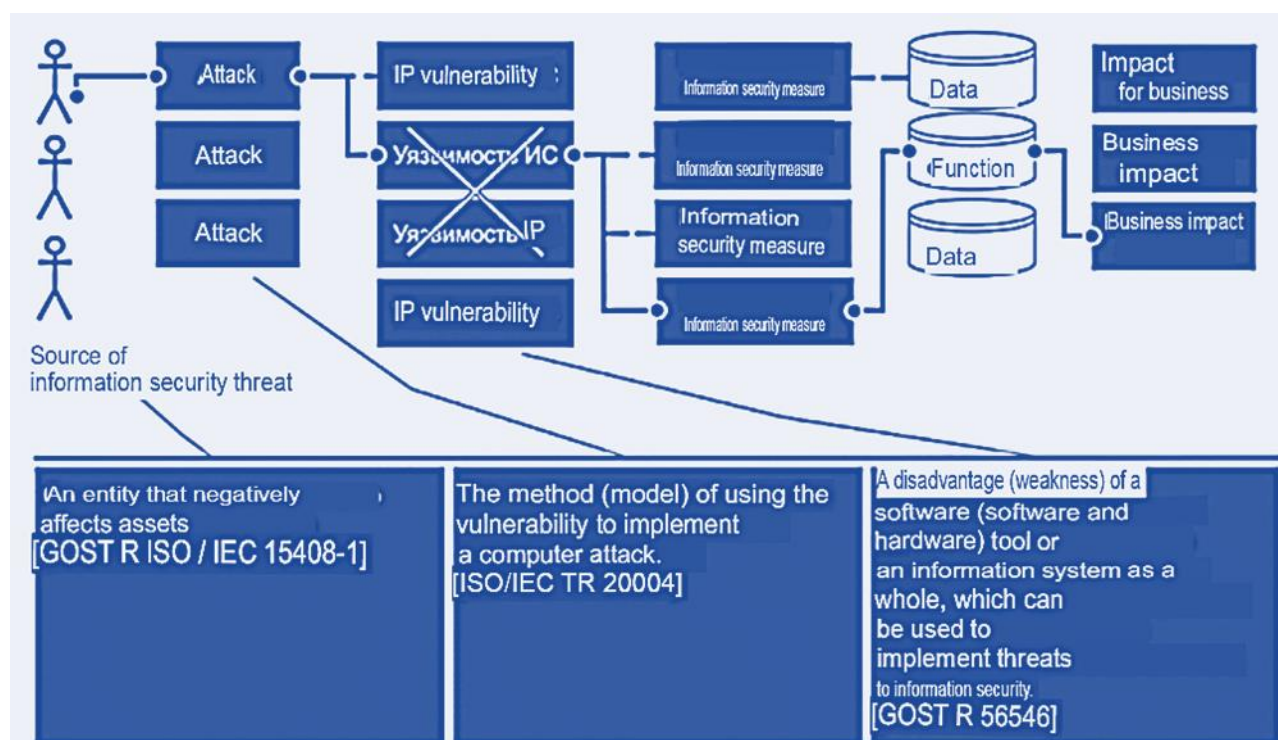
Figure 2.2. Fragment of the MITRE ontology with examples for researchers



Source: MITRE. URL: <https://cve.mitre.org/>.

Identification and correction of vulnerabilities eliminates corresponding threats and incidents (computer attacks). Thus, methods of enhancing systems security focused on vulnerabilities and software defects are in fact a priori in nature, and therefore have several advantages over “reactive” methods focused on a security event or incident that has already occurred (Figure 2.3).

Figure 2.3. Conceptual model of a computer attack that implements a vulnerability



Source: OWASP Top Ten. URL: <https://owasp.org/www-project-top-ten/>.

2.1.2. Problems of software vulnerability

Due to the development of the informatization of international society, there has been a shift in the sphere of national, including military, assets, and communications into the area of ICT space. Currently, several states have adopted the concept of cyberspace as the fifth theater of military operations and indicated the creation of a type of cyber warfare, with “about 120 countries in the world have practiced the skill of cyber warfare”³⁷. Accordingly, in the field of international security, it becomes very relevant to study the problems of predicting, preventing, and deterring international conflicts in cyberspace.

³⁷ Andrey Krutskikh: More Than 120 Countries Have Practiced Cyber Warfare. International Life. URL: <https://interaffairs.ru/news/show/22362>.

The development of a cyber conflict goes through several open and latent phases. As far as the security of software environments and systems is concerned, three phases can be distinguished:

- identifying vulnerabilities and working out the possibility of their implementation for the purpose of cyber-attacks of various purposes,
- detecting and responding to incidents, usually related to ongoing cyber-attacks,
- eliminating the consequences of successful cyber-attacks.

The latter two phases deal primarily with situational and crisis management issues and have been the focus of recent international negotiations and initiatives on international cyberspace security. At the same time, the initial phase of the cyber conflict directly related to program security has been little studied in the field of international law and given mainly to technical regulation, which has national or fragmented interstate traits in different countries. Moreover, in the field of international technical regulation, several contradictions have accumulated due to the lack of confidence in the safety of software products, parts of which were developed or tested by companies in other countries. In other words, the resolution of this problematic situation is important in the field of international security; it has a strictly precautionary character and meets the target of increasing confidence in the security of software systems within the context of international ICT security.

2.1.3. Program security in the context of IIS

It is necessary to point out two factors of IIS specifically related to the security of software systems:

- 1) the critical structural complexity of programs causes an increase in man-made risk,
- 2) the use of ICT has expanded the range of intentional threats, namely in terms of remote (including covert and unprovable) computer attacks, as well as threats to compromise ultra-large-scale data.

The main reason for man-made risk is the extremely high structural complexity of programs compared to, for example, hardware or organizational and technical systems. For example, the length of the operating system source code with high-level language applications can reach 5 – 20 Gb, which means that the number of logical operators (program graph nodes) can be about tens of millions, which is quite far beyond the cognitive abilities of a human programmer or tester. Experience shows that many specialists in the sphere of software system security psychologically abstract away and unconsciously do not understand the scale of “the curse of dimensionality” of a program structure. To illustrate the above, we present the exhaustive testing capabilities of a trivial program procedure-function (Table 2.1).

The second IIS factor is the cause of the fifth theater of war in cyberspace. Most today's computer attacks are vulnerability-based, with the attacker only needing to find one vulnerability in software to implement its corresponding threats.

Table 2.1. Example 1

Given:	Procedure-function for multiplying two 32-bit numbers
Hypothesis:	The examiner spends 1 second to check the correctness of the result
To find:	Time required to perform full-featured testing on all combinations of input data
Solution:	$N = 2^{32+32}$ $T=N \times 1 \text{ s.} = 18446744073709551616 \text{ c.} \approx 584, 9 \text{ trillion years}$

Source: Table constructed by the author.

2.1.4. The significance of software vulnerabilities

Noting the vulnerability of software systems, it is worth highlighting that despite the efforts of developers, the number of errors and vulnerabilities is not decreasing (Figure 2.4), the space of threats and challenges in ICT is in constant flux, and individual errors or vulnerabilities lead to major accidents and disasters (Table 2.2). It is also important to add that the volume of the open international MITRE CVE vulnerability database exceeds 110,000 vulnerabilities, and the volume of the Russian FSTEC domestic market-oriented database of CVE is 20,000 vulnerabilities.

Table 2.2. An example of the price of a software error

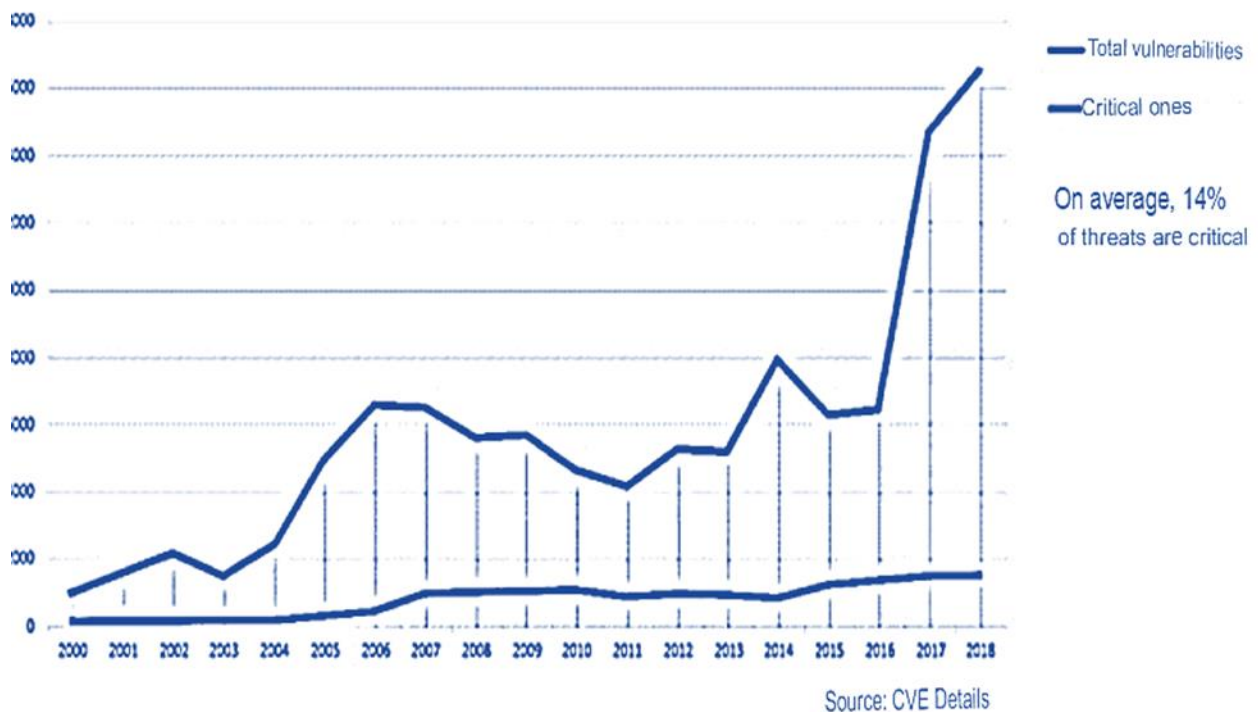
Event	Short Description	Direct damage
Error in NASA's <i>Mars Climate Orbiter</i> program	Loss of space satellite due to erroneous unit conversion	Over \$125 million
Failure to open Heathrow Airport Terminal 5 in London	Functional error when returning luggage	More than 500 flights canceled, 42,000 pieces of luggage lost in 10 days
Error in the program <i>The Mariner 1 Spacecraft</i>	Loss of spaceship due to code error – programmer missed a hyphen	Over \$18 million.

Source: https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html.

Considering the objective presence of vulnerabilities in software and the complexity of their detection, many major players in the software market (Facebook, Google, Yandex, Microsoft, the US Department of Defense, and others) try to take maximum advantage of crowdsourcing by holding open competitions to identify vulnerabilities (the so-called bug bounty). For example, Google has spent \$12 million to pay for bugs and vulnerabilities found, and the US Department of Defense has already held five Hack the Pentagon contests, in which ethical hackers submitted about a hundred reports on vulnerabilities in software resources of US military automated control systems (ACS) in 2018 alone. Not surprisingly, software vulnerability issues have affected both black market and spy scandals. The most high-profile incident of 2017 was the “leak” of a Windows vulnerability from the NSA database, which was used by the malicious program *WannaCry* (*Wanna Decryptor*), which, incidentally, was acknowledged by *Microsoft* officials.

As we know, the *WannaCry* malware illegally encrypted the resources of 500,000 computers worldwide in just two weeks. The victims included the Russian Foreign Ministry, Russian Railways, the cell phone operator Megafon, and others.³⁸ *Microsoft* actually found out about the vulnerability from well-wishers who chose to remain anonymous. Microsoft Bulletin MS17-010 also does not contain any information with acknowledgements for reporting the vulnerability used by the *WannaCry* malware.

Figure 2.4. Growth of vulnerabilities in the MITRE CVE database



³⁸ WannaCry Epidemic: What Happened and How to Protect Yourself // Kaspersky Lab. 2017u May 13. URL: <https://www.kaspersky.ru/blog/wannacry-ransomware/16147/>.

2.1.5. Program security in the context of strategic stability

It is worth noting the connection of software security not only with international information security, but also with strategic stability. As resonant examples we can cite related incidents last year, namely, the access of pro-Chinese hackers to US satellite resources, which, according to *Symantec*, introduced a software tab in the system software of the SU, which allowed, allegedly, to change satellite orbits and intercept sensitive data³⁹.

Chronologies of cyber operations related to nuclear incidents have been described in various sources.

2.1.6. Foreign studies in program security

The problematic of software products and systems security is in high demand, as evidenced by both current trends in international certification of secure software products⁴⁰, and relevant research conducted by DARPA (Table 2.3).

Table 2.3. DAPRA research on software vulnerabilities

Exploratory research	Purpose
Vetting Commodity IT Software and Firmware (VET)	Control of undeclared features and bookmarks in the software of peripheral devices (faxes, printers, phones, etc.)
Automated Program Analysis for Cybersecurity (APAC)	Creating tools to automate the detection of undeclared features and bookmarks in software for mobile platforms (Android)
Cyber Grand Challenge (CGC)	Academic vulnerability detection competitions
Clean-slate design of Resilient, Adaptive, Secure Hosts	Creating methods and tools (development environment, verification environment, runtime environment) for developing computer systems that are resistant to computer attacks
Mining and Understanding Software Enclaves	Improving software reliability, including the creation of techniques and tools for verification and static analysis of the source code of programs.

Source: Defense Advanced Research Projects Agency. URL: www.darpa.mil.

³⁹ Menn J. China-Based Campaign Breached Satellite, Defense Companies: Symantec // Reuters. 2018. 19 June. URL: <https://www.reuters.com/article/us-china-usa-cyber/china-based-campaign-breached-satellite-defense-companies-symantec-idUSKBN1JF2X0>.

⁴⁰ Barabanov A., Markov A. Modern Trends in the Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria // Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015. P. 30-33. DOI: 10.1145/2799979.2799980.

2.1.7. Prohibitive measures in the field of program security regulation

The relevance of cyber threats and related challenges to international information security and strategic stability implies intensified initiation and compliance with international treaty processes in the field of ICT. However, in the global community, instead of consolidation in the field of increasing confidence in security of programs, “prohibitive” measures still dominate, for example,

- in Europe, there is a contradiction between the requirements for collaborative certification (based on collaborative protection profiles) and those of the European Union or individual nation states,
- the USA has imposed restrictions on the use of software products that have been certified in China and Russia. In turn, China and Russia are implementing asymmetric measures,
- several countries pursue import substitution policies, blacklist suppliers of foreign products or impose restrictions on the use of imported products,
etc.

As far as Russia is concerned, this is most clearly demonstrated by the last two events of the past year:

- a ban on the use of Kaspersky Lab products in government institutions in several Western countries,
- a five-year ban on the use of US software that was certified with the provision of software source codes in Russia, etc., within US government agencies.

Even though such a policy is justified in certain geopolitical conditions, it is not constructive in terms of increasing international integration and security on several problematic issues – for example, it contradicts the consolidation of countries to counter the illegitimate activities of third parties, especially the criminal hacker community.

2.2. Ways to increase confidence in program security

Increasing confidence in the security of software systems creates an objective trusted platform for reducing threats, risks and, ultimately, incidents in cyberspace. The following ways to improve the security of software systems in the context of international information security can be proposed:

- legal regulation of software security, including vulnerability awareness,
- technical regulation of software security, including international conformity assessment (certification) of software products and control systems (management) of software production.

Legal regulation (as general regulation) must establish ICT security relations, and technical regulation (as special regulation) must establish relations in the technical sphere on ICT security issues. The goals of legal regulation are partly contained in Russian initiatives of a global character, including the previously mentioned set of 13 international rules, norms, and principles of responsible conduct of states, recommended by UN General Assembly Resolution A/RES/73/27, and supported by 139 countries. As for technical regulation, the international and interstate systems of standardization and certification, harmonized with the Russian regulations, have developed in world practice. At the same time, it is obvious that both legal and technical regulation of international information security in the field of ICT is at the initial stage of formation, certain issues of which are discussed in this chapter, namely:

- 1) increasing the maturity of international software enterprises,
- 2) increasing the level of reliability of certification results of software information protection with the provision of access to the source code at the stage of testing.

2.2.1. Regulation of safe program development

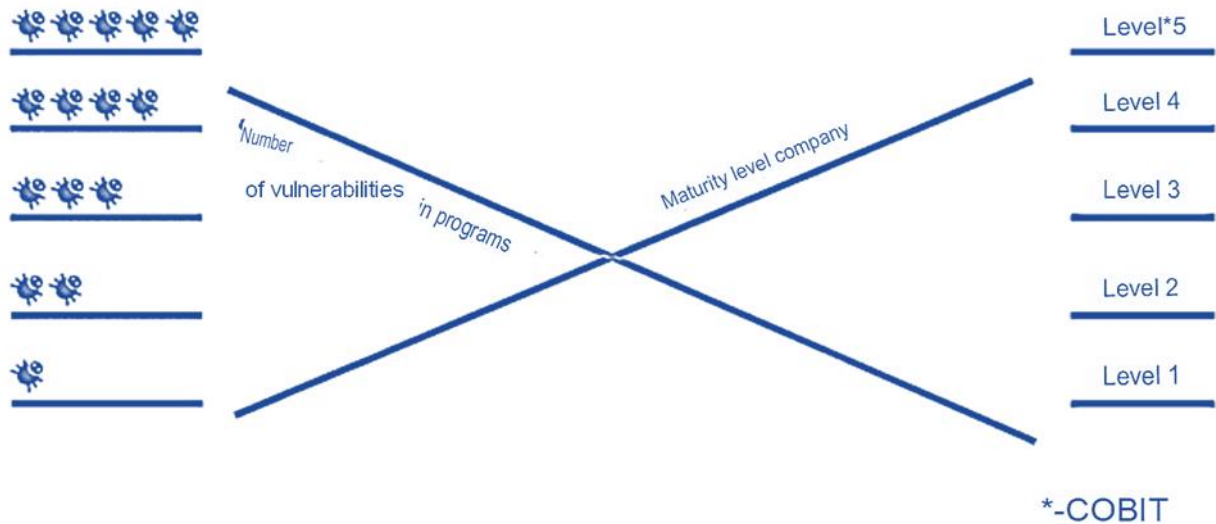
Statistics from testing laboratories have shown that the main cause of software vulnerabilities is the low maturity of software companies that ignore security measures related to the design, development, production, implementation, delivery, and maintenance of software products. Thus, the authors have obtained statistics showing that the level of management (or maturity⁴¹) of a company significantly influences the security level of the developed, produced or supplied software, namely the degree to which vulnerabilities are present and possibility of their quick correction in case of detection. Research by testing laboratories have shown a strict inverse correlation between the total number of vulnerabilities and the maturity levels of the software company (Figure 2.5). According to *Microsoft*, the number of vulnerabilities in software fell by more than 80% with the introduction of an appropriate management subsystem (*Microsoft Secure Software Development Life Cycle*).

Often threats to software security involve not only the developer, but also the manufacturer and suppliers. In other words, a computer attack on an organization's software resources can be conducted at various stages of the software lifecycle. Nowadays, the most popular attacks are computer attacks on the supply chain (supply chain attack). Their purpose is to compromise the least protected objects in the supply chain. Software resources of not only the end customer, but also of all the participants in the supply chain can be compromised. The attack is implemented through the introduction of malicious software or a hardware-software implant into the solutions used by the organization (Figure 2.6).

⁴¹ Effective IT Governance at Your Fingertips // Information Systems Audit and Control Association (ISACA). URL: <https://COBITonline.isaca.org/>.

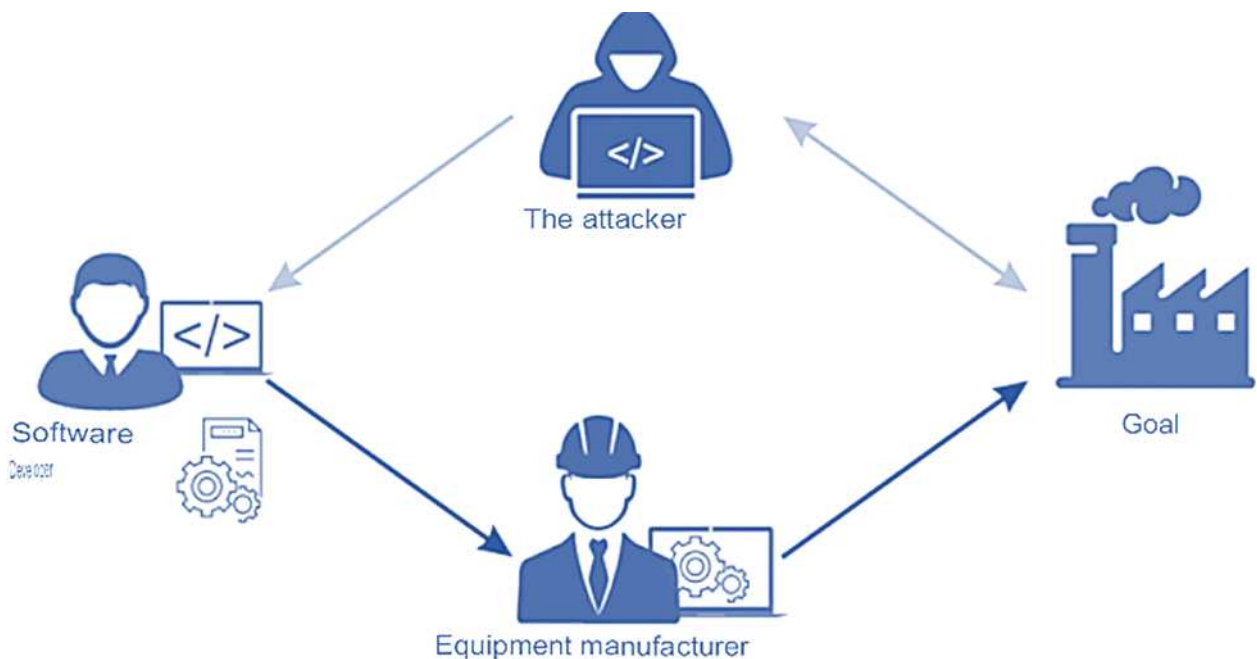
To illustrate the size of the disaster at the initial stage of program creation, Figure 2.7 shows statistics on the distribution of program developers depending on the involvement of third parties in development.

Figure 2.5. The “5 by 5” law of inverse proportionality of company maturity and the number of vulnerabilities in software products



Source: Picture built by the author.

Figure 2.6. Conceptual model of an attack on the supply chain



Source: The MITRE Corporation. URL: mitre.org.

Known examples of these attacks include compromising software development tools, stealing certificates or signing malicious software with a developer's certificate, compromising embedded microcode, installing malware on devices (cameras, USB devices, phones), etc.

One recent high-profile case involving targeted attacks on the supply chain is the *Shadow Hammer* cyber operation. The cyber operation implanted malware into a legitimate ASUS Live Update utility. The attack was targeted at a select group of users, strictly defined by the MAC addresses of personal network adapters. More than 600 unique MAC addresses were extracted from more than 200 malicious samples involved in this attack. The largest percentage of the address data related to Russia.

At the management systems level, the main measures to minimize the risks of exposure to supply chain attacks taken by the developer and suppliers are:

- implementation of safe development processes,
- implementation of an information security management system (e.g., in accordance with ISO/IEC 27001).

At the level of individual processes, the main security measures include penetration testing, code security auditing, control of third-party components used, etc.

Figure 2.7. Statistics of outsourcing in programming



Source: State of software development in 2018 // Coding Sans LTD. URL: <https://codingsans.com/state-of-software-development-2018>.

Several guidelines (“good practices”) and standards from international and national organizations related to secure software development are now known, e.g., Microsoft SDL, Cisco SDL, BSIMM, US Department of Defense recommendations, ISO/IEC 27034, ISO/IEC TR 24772, etc. Threats to the supply chain are well developed in the literature, while unintentional threats, as well as threats to other sub-stages of the software lifecycle, are often poorly described. The available international standards do not provide complete regulation of all software development processes and procedures, taking into account the current range of threats to information security.

Tables 2.4 and 2.5 show fragments of the analysis of regulatory documents in the field of creating secure programs, which demonstrates the lack of completeness of foreign studies.

To ensure the completeness of the processes of software development, security measures and relevant threats to information security (in the development and delivery of programs), the technical committee on standardization of Russia TC-362 “Information Security” developed and enacted a national standard for the creation of secure software – GOST R 56939-2016 “Information Security. Development of secure software. General requirements”, as well as initiated the development of a line of related standards. The idea of the national standard and aspects of its harmonization, as well as the scheme of harmonization of this standard with international standards are presented in Figures 2.8 and 2.9, respectively.

Table 2.4. Threat directories related to the software lifecycle

Catalog of threats related to the software life cycle	Consideration of threats specific to the development environment	Accounting for unintentional threats
MITRE&DSE	+	-
NIST SP 800-30 rev.1	-	-
NIST IR 8144	+	-
MITRE CAPEC	+	-
BDU FSTEC of Russia	-	+

Source: Table constructed by the author.

Table 2.5. Regulatory documents on the development of safe programs

Characteristics, availability of safe software development measures	Standard/Guideline					
	ISO/IEC 15408	Microsoft SDL	Open SAMM	OWASP CLASP	ISO/IEC TR 24772	ISO/IEC 27034-1
Employee training	-	+	+	-	-	-
Ensuring infrastructure security	+	-	-	-	-	-
Configuration management of programs under development	+	-	-	-	-	-
Modeling threats to the security of information, the source of which are programs	+	+	+	+	-	-
Defining requirements for the development of safe programs	+	+	+	+	-	-
Using the source code design standard	-	+	+	+	+	-
Conducting a static analysis of the source code	-	+	+	+	-	-
Performing dynamic code analysis	-	+	+	+	-	-
Conducting examination of the source code of programs in manual mode	-	+	+	+	-	-
Conducting a vulnerability analysis	- ⁴⁰	+	+	+	-	-
Ensuring security of supply	+	+	+	-	-	-
Remediation of exploitable vulnerabilities	+	+	+	+	-	-
Ability to use documents in certification	+	-	-	-	-	-
Availability of a methodology for selecting a subset of development measures	+	+	+	-	-	+
Consistency with program lifecycle processes (according to ISO/IEC 12207)	-	-	-	-	-	+

Source: Table constructed by the author.

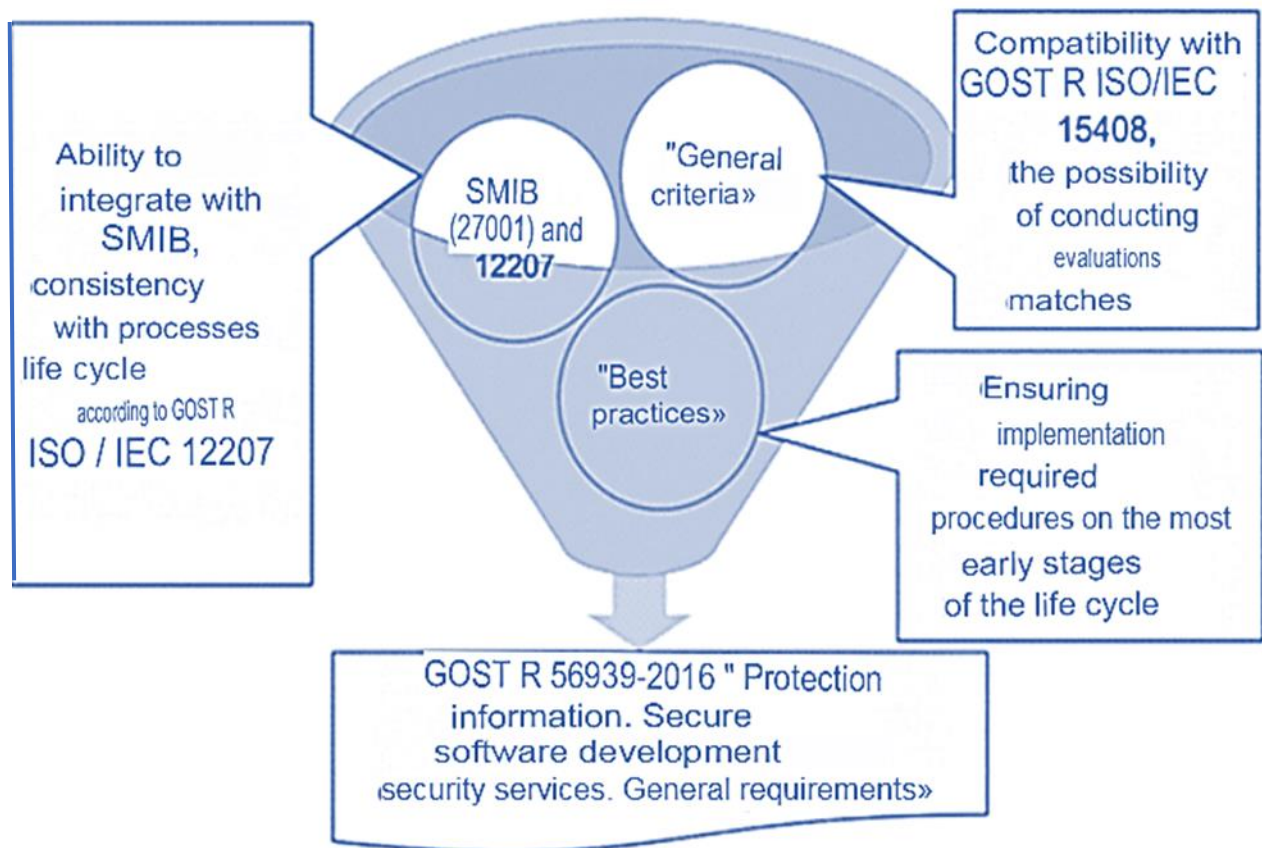
⁴² The ISO/IEC 20004 standard defines an approach to vulnerability detection in IT product compliance assessment with reference to ISO/IEC 15408.

The goal of creating a line of standards for secure software development is to prevent the emergence of software vulnerabilities and to eliminate them. In this case, there is a connection between the design processes (which is regulated by GOST R ISO/IEC 12207) and the measures for secure development, which are selected considering a risk-based approach, i.e., considering the actual threats. Security measures in the standard are divided into three groups (program implementation, program support, organizational support) and include nine main processes:

- requirements analysis,
- architecture design,
- construction,
- qualification testing,
- documentation and configuration management,
- solving problems during operation,
- acceptance support,
- management of the development environment infrastructure,
- personnel management.

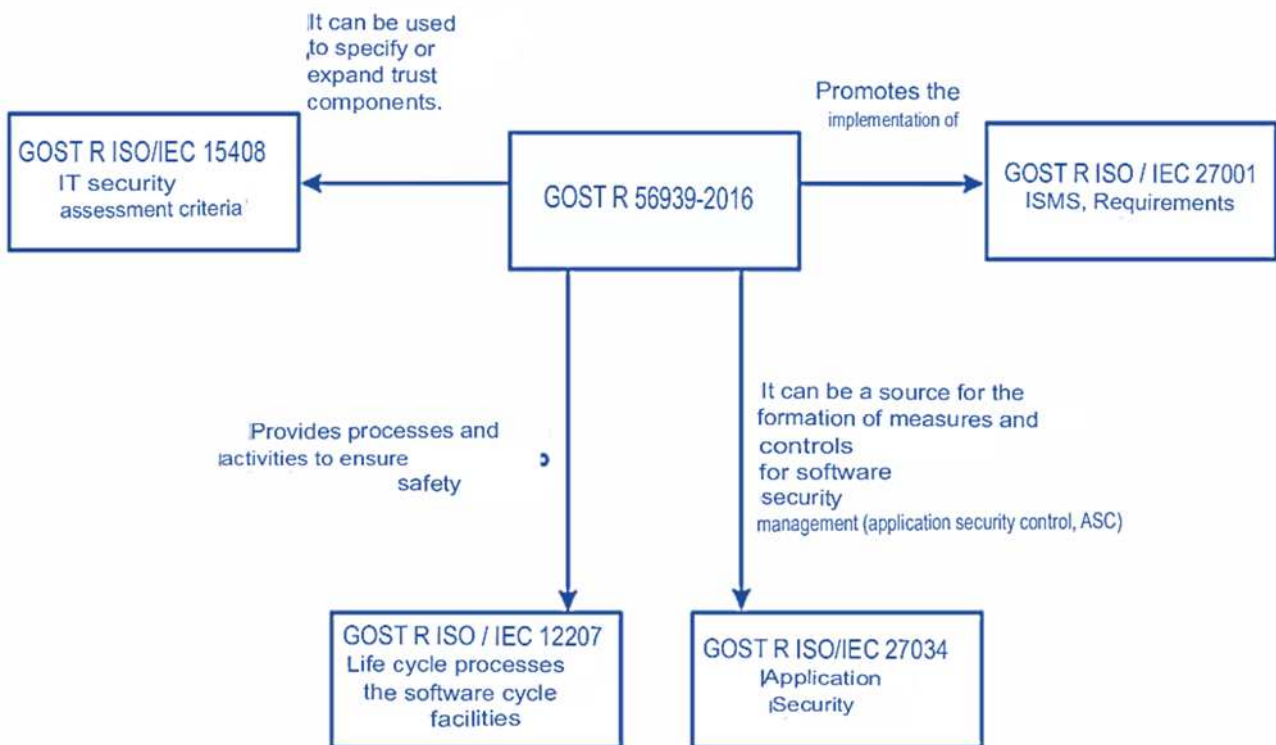
The relationship of processes and basic safety measures is shown in Figures 2.10 and 2.11.

Figure 2.8. Conceptual model of the formation of the standard for the development of safe programs



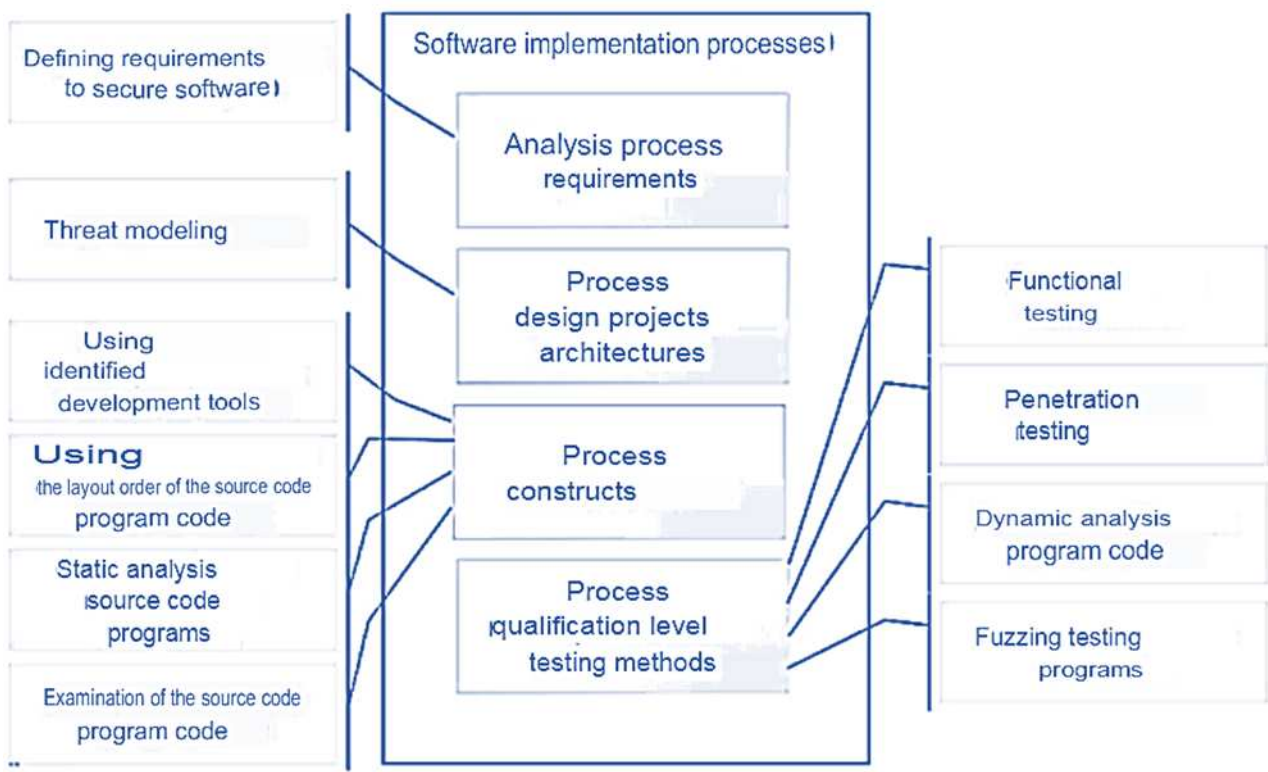
Source: Based on the experience of the NGO “Echelon”.

Figure 2.9. Harmonization of the safe design standard



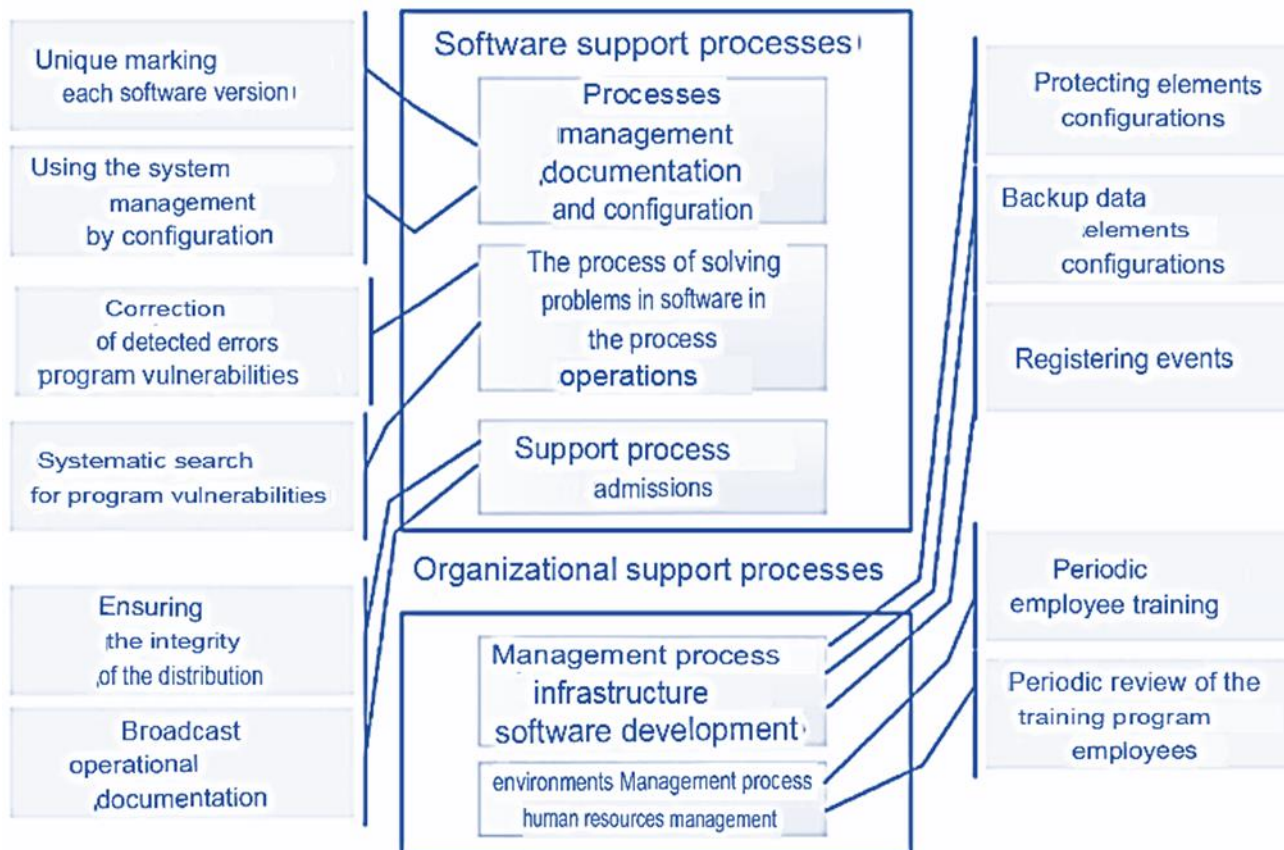
Source: Based on the experience of the NGO “Echelon”.

Figure 2.10. Measures to implement safe programs



Source: Based on the experience of the NGO “Echelon”.

Figure 2.11. Measures to support and secure programs



Source: Based on the experience of the NGO “Echelon”.

2.2.2. Regulation of assessment of program compliance with information security requirements

Conformity assessment in the field of information security usually takes the form of obligatory certification of information security tools according to information security requirements, the goal of which is ultimately to minimize the risk of exploitation of vulnerabilities in software. To explain the effectiveness, efficiency, and limitations of certification testing methods and techniques, let us give a classification of testing approaches and the defects and vulnerabilities sought. In the most general terms, testing methods are classified as follows:

- by lifecycle: verification, code analysis and program testing,
- on startup: static analysis and testing (dynamic analysis),
- by availability of source code: black box method (e.g., functional testing) and white box method (structural testing).

The choice of method and technique depends on the purpose of testing, i.e., on the class of defects and vulnerabilities detected. The classes to be detected can generally be divided into:

- unintentional and intentional,

- non-functional and functional,
- the known, the similarly known and the unknown.

At the same time, intentional vulnerabilities, particularly software bookmarks, are associated with combinations of rarely used input data, when stochastic methods have insignificant effect. In the following case of classification, it is easy to show that functional vulnerabilities (especially of the combined type) are syntactically correct, i.e., they cannot in principle be found by methods of subroutine code correctness checking (not to mention deductive verification of several lines of code) without correct functional specifications. There is a striking difference between labor-intensiveness of detecting known vulnerabilities and unknown vulnerabilities. Obviously, checks for known vulnerabilities via trivial scanning or for known computer viruses via antivirus protection should not be attributed to certification tests (i.e., not to the implementation stage), but to the management of support for program operation and maintenance, since they are valid only in relation to a time point of operation. It is easy to see that the choice of a class of defects determines the approaches to software testing, some of which belong to the domain of reliability theory (when the main factor is a failure or a manifest error), and some – to information security theory. Mistakes in such classification lead to a substitution of concepts with ensuing negative consequences in the field of certification and information security. Regarding information security testing, the most well-known program verification techniques in the literature are:

- applied (algorithmic) verification,
- code inspection,
- static decomposition analysis (identifying undeclared opportunities by collecting and analyzing routes),
- static signature-heuristic analysis,
- dynamic structural analysis and debugging,
- functional testing (“black box”, deterministic approach),
- phasing (“black box”, stochastic approach),
- penetration testing (vulnerability detection and exploitation), etc.

With the various advantages and disadvantages of these approaches, it can be stated that there is no universal method today. For example,

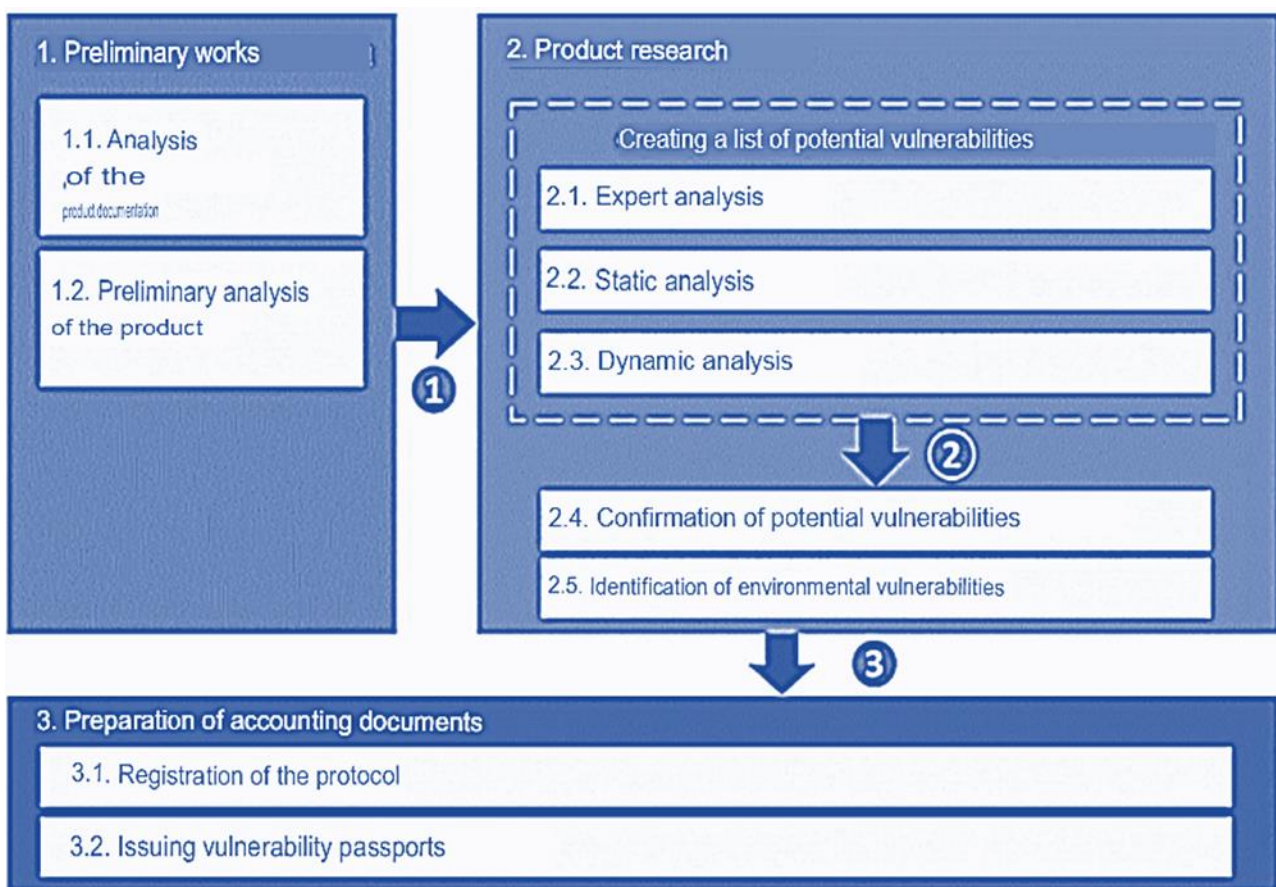
- the password bookmark is easy to find by the presence of constants in the authentication operation loop, while the logical bomb is easily detectable by the counter,
- failure and denial of service can be fixed during phasing or stress testing,
- coding errors are usually detected at the stage of compilation parsing.

At present, open-source approaches to detecting vulnerabilities of known types are based on the conceptual approach of ISO/IEC TR 20004. Among other things, guidelines focused on application testing (e.g., NIST SP 800-163, OWASP MSP, etc.), penetration testing and auditing (PTES, OWASP ASVSP, etc.) are known

in global practice. A comprehensive approach to program security testing is now being tested in Russia. Despite the use of many different methods and techniques of software verification, it is impossible to get an acceptable level of trust in software resources without providing access to the source codes. This can be most clearly shown by the example of “floating” errors and program bookmarks, the initiation of which is associated with rare combinations of input data, i.e., they cannot be found by black box testing methods, such as phasing testing. In other words, only access to program source code gives some probability of detecting any vulnerability through expert knowledge. Figures 2.12 and 2.13 show statistics on the performance of basic software security analysis methods, which confirm the leading role of the expert and the preference for source code and specifications, as well as the performance of various vulnerability detection methods, respectively. Thus, two conclusions can be made:

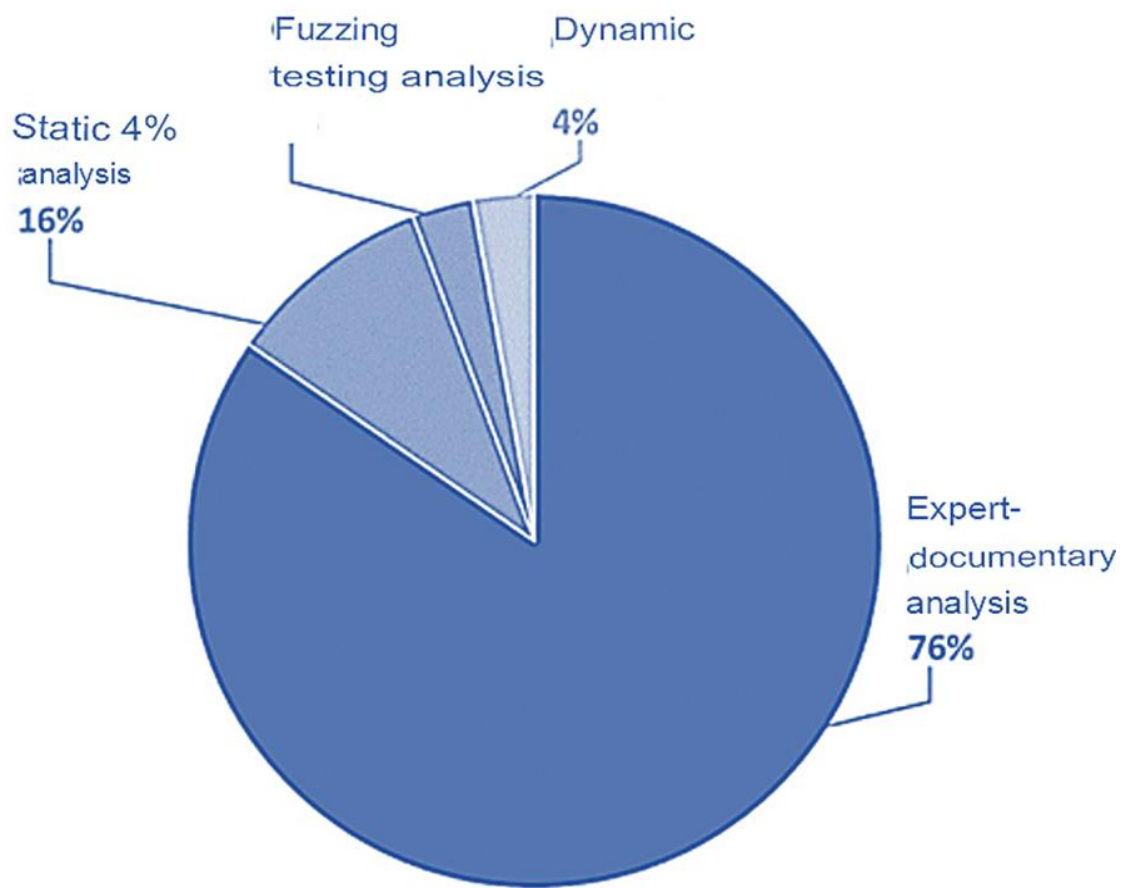
- the effectiveness of software security checks depends to a large extent on the qualifications of the experts who make the decision when assessing the level of the defect, vulnerability, and threat,
- it is impossible to provide an acceptable level of confidence in the security of programs without providing access to the source code of the programs.

Figure 2.12. Conceptual model of vulnerability detection during software certification tests



Source: Based on the experience of the NGO “Echelon”.

Figure 2.13. Effectiveness of different vulnerability detection methods



Source: Based on the experience of the NGO “Echelon”.

2.2.3. International aspects of organizing access to program source code

Unfortunately, access to the source code of software systems is a highly debated.

Political criticism eventually leads to the previously mentioned prohibitive measures in international society integration to ensure the necessary level of international information security. The most prominent prohibitive policy act is the US Defense Authorization Act of 2019 #115-232, which does not allow the use of US IT products in defense if they have been certified within the last 5 years with the provision of source code in foreign countries.

At the political level, there is an obvious substitution of the concepts of “opening the code” and “organizing access to the code for the period of testing”. Let us take a closer look at this point. The opening of the code as such, of course, carries the threat of disclosure of information on vulnerabilities and compromise of intellectual property. However, hiding code vulnerabilities at the interstate level to ensure offensive information confrontation immediately discredits any trust in computer systems and products between specific countries and nullifies any international agreements.

At the industrial or commercial level, the main threats seen by development companies are the threat of intellectual property theft and the threat of illegitimate disclosure of vulnerability information to other third parties. At the same time, the experience of test labs shows that there has long been a known solution to ensure the strict fulfillment of code security requirements, namely, the creation of a stand-alone secure bench in a secured room or “clean room”. In such a room, the access to the source code of the programs is established on the territory of the client (under the control of the client's security service) only *for the period of testing*. Within the scope of this access, in a closed secure environment, the program is built, its integrity is recorded (checksums) and the necessary agreed upon checks are performed. Of course, without the consent of the client’s security service it is not allowed to take out any data carrier, initiate a communication session outside, etc. All documentary evidence of the checks and conclusions are discussed and approved by the client. As a result, if a vulnerability is detected, the following happens: the client fixes the vulnerability and approves the report materials, or the customer blocks the report materials (in this case they do not get a certificate). In this case, the public actions of the testing laboratory are limited by the non-disclosure agreement (with penalties), that is, the possible risks of the customer are taken into account. This approach is characterized by a number of following advantages and guarantees:

- it allows you to improve the security of programs by consolidating the activities of developers and client-approved specialists of the testing laboratory,
- identified vulnerabilities are corrected as part of the certification on a mandatory basis, and information about this is not revealed to third parties,
- checks are absolutely transparent, all actions (organization of access, control and monitoring of work, discussion of results, preparation of reporting documents, etc.) are technically and normatively ensured by the client's security service,
- there is an element of trust in the software because there is always a chance to detect potentially dangerous code (or to demonstrate its absence), which in the end is in the interest of both sides of the certification.

At the same time, the issues of opening access to the source code for testing are understood by many large software companies. For example, Microsoft has opened access to the source code of its software products in more than 30 countries⁴³, including Russia. Kaspersky Lab division located in Moscow offered to open access to the source code of its software products to authorized certification authorities in the United States⁴⁴.

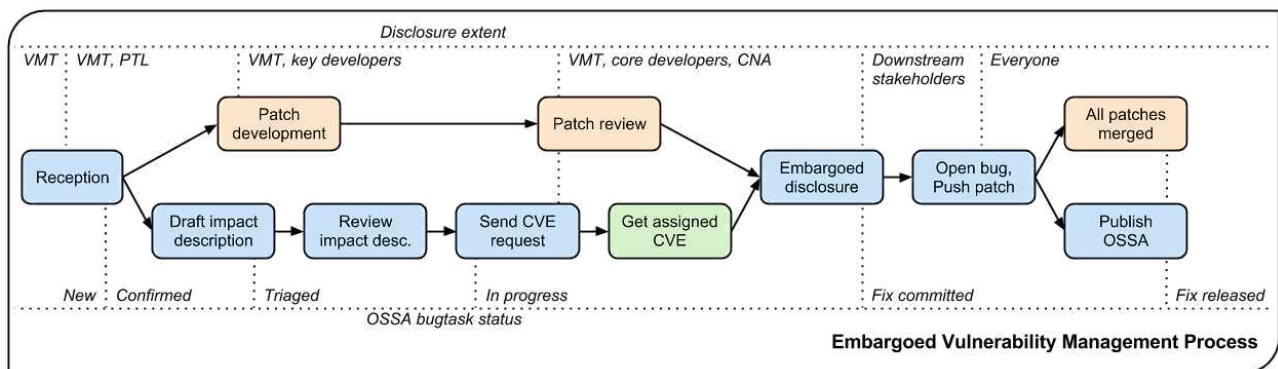
⁴³ The Microsoft Transparency Center in Brussels // Microsoft URL: <https://blogs.microsoft.com/eupolicy/transparency-center/>.

⁴⁴ Finkle J., Auchard E. Kaspersky Lab to Open Software to Review Says Nothing to Hide // Reuters. 2017. 23 October. URL: <https://www.reuters.com/article/us-usa-security-kaspersky-russia/kaspersky-lab-to-open-software-to-review-says-nothing-to-hide-idUSKBN1CS0Y1>.

However, even the requirement to verify source code has become the subject of political controversy between the US., whose approach involves a shift toward simplified *collaborative security* profiles, and the EU, which is strengthening software verification under the recent EU Cybersecurity Act.

Finally, a direct link between vulnerability detection and company maturity should be pointed out. If a developer has mature development and manufacturing processes, they also publish information about vulnerabilities discovered (Figure 2.14).

Figure 2.14. Software vulnerability detection and description scheme



Source: Openstack. URL: openstack.org.

* * *

The presented material allows us to conclude about the vital role of software security in the sphere of international information security. The two most promising directions for improving the security of international information security software are seen as the most promising:

- research on the convergence of best practices in legal and technical regulation, considering the provision of access to source codes during the testing phase,
- research in the field of information and cybersecurity management of organizations-developers and suppliers of software systems.

Considering the scientific assertions received and the dynamics of the ICT sphere, the following interpretation of paragraphs 9 and 11 is proposed as part of the development of the previously mentioned set of international rules, norms, and principles of responsible behavior of states:

- states must take reasonable measures to ensure the integrity of supply channels so that end users and suppliers can have confidence in the security of ICT products and services,
- states should promote responsible reporting of ICT vulnerabilities, share relevant information on existing practices to address such vulnerabilities, and take measures to eliminate and address relevant threats to ICTs and ICT-dependent infrastructure in a timely manner.

CHAPTER 3

Supercomputers and Security Issues

A single tight and accepted definition of “supercomputer” or “super machine” does not yet exist. *Hewlett Packard Enterprise* suggests the following formulation: “The term 'supercomputers' means systems for performing highly complex tasks or tasks that involve large amounts of data, by concentrating the computing resources of many computers working in parallel (forming a 'supercomputer'). Supercomputers operate at maximum efficiency and performance, usually measured in petaflops. They are often used in meteorology, energy, health care, manufacturing, and other fields”.⁴⁵

In a piece about the Fischer supercomputer created for the Joint Institute for High Temperatures of the Russian Academy of Sciences, Rostec defines a modern supercomputer as “a huge device consisting of memory modules, processors, boards, combined into computing nodes connected by a network. A control system distributes tasks, controls workload, and monitors task performance. Cooling and uninterruptible power supply system's ensure uninterrupted operation of the supercomputer. The entire complex can take up considerable space and consume huge amounts of energy”.⁴⁶

Russian programmers define a supercomputer as “a very powerful computer with thousands of processors that many times speeds up complex calculations and processes petabytes of data. In a supercomputer, individual machines are connected by a high-speed network (interconnect)”.⁴⁷

The architecture of a supercomputer can be illustrated by the example of the Lomonosov supercomputer from Moscow State University (Figure 3.1).

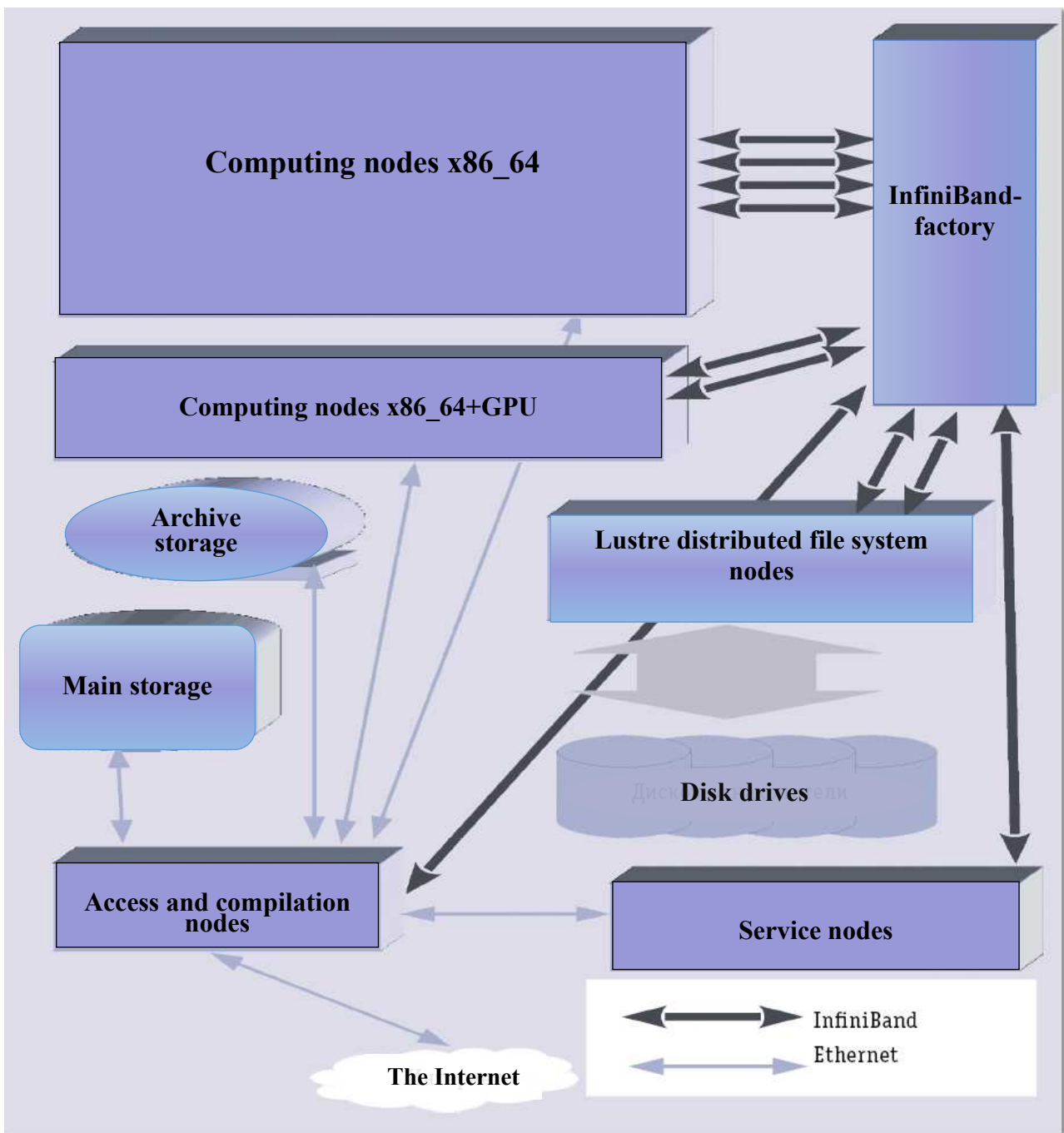
Due to the exceptional amount of information processed and the speed of processing, supercomputers are also actively used in the field of security, ranging from logistics tasks to simulation of the flow of processes in nuclear warheads. Their role will only increase in the future, therefore, their place in the process of ensuring national and international security requires an in-depth expert analysis.

⁴⁵ Definition of Supercomputers // Official Hewlett Packard Enterprise Website URL: <https://www.hpe.com/en/ru/what-is/supercomputing.html>.

⁴⁶ Supercomputers: Titans of Computation // Official Website of Rostec. 2019. October 4. URL: <https://rostec.ru/news/superkompyutery-titany-vychisleniy//>.

⁴⁷ Abramov S. Supercomputers: Reverse Records // Science and Life. 2019. №1. URL: <https://www.nkj.ru/archive/articles/35326//>.

Figure 3.1. The architecture of the Lomonosov supercomputer



Source: V. Voyevodin, S. Zhumatiy, S. Sobolev, A. Antonov, P. Bryzgalov, D. Nikitenko, K. Stefanov, V. Voyevodin. The practice of the supercomputer “Lomonosov”, Open Systems. SUBD, 2012, NO. 07.

3.1. Supercomputer Ratings

The most common characteristic of supercomputer performance is “petaflops”, equal to 10^{15} flops, where “flops” is an off-system unit indicating the number of floating-point operations per second for a given computing system. The 1 petaflops

milestone was reached in 2008 with the *Roadrunner* supercomputer, built by IBM for Los Alamos National Laboratory in New Mexico, USA⁴⁸. In the coming years, supercomputers with performance measured in exaflops, equal to 10^{18} flops, are expected to appear.

The best modern supercomputers usually participate in the global *Linpack Top-500* ranking, which can be considered quite representative. As of June 2020,⁴⁹ the largest number of supercomputers in the ranking (226 units), as well as the maximum total computing power is in China. In second place is the United States (113 units). The conditional “five” also include Japan, France, and Germany. Thus, in June 2020, Japan's *Fugaku* (415.5 petaflops) outpaced *Summit* (Oak Ridge National Laboratory) with a capacity of 148.6 petaflops⁵⁰ and took first place. And the closest Chinese competitor was *Sunway TaihuLight* (National Supercomputer Center, Wuxi), which took 4th place.

Fugaku's leadership is especially important due to its use of ARM rather than x86 architecture, as the overwhelming majority of the ranking participants have.

Russia ranks 19th (out of 28) and is represented by two supercomputers, the best of which is *Christofari*, created by a Sberbank subsidiary called SberCloud in cooperation with NVIDIA. The performance of this supercomputer is about 6.7 petaflops, which corresponds to the conventional 29th place in the world. There are no domestic military supercomputers in the rating. At the same time, there is no doubt that the domestic nuclear weapons complex faces tasks like those that are solved by their American counterparts in national laboratories. Note that it is FGUP “RFYC-VNIIEF” (Sarov city), which is part of Rosatom State Corporation, that positions itself as a leader “in the field of supercomputing technologies”⁵¹.

Within the CIS there is also an “internal” rating of the “Top 50” most powerful computers, which shows that in our country supercomputer technology is used both in science and in business, although research tasks dominate. Moreover, all supercomputers in the rating use *Intel*⁵² processors.

⁴⁸ Fact Sheet & Background: Roadrunner Smashes the Petaflop Barrier // IBM Official Website. URL: <https://www-03.ibm.com/press/us/en/pressrelease/24405.wss>.

⁴⁹ LIST STATISTICS // Linpack Top-500 website. URL: <https://www.top500.org/statistics/list/>

⁵⁰ Japan Captures TOP500 Crown with Arm-Powered Supercomputer // Linpack Top-500 website. URL: <https://www.top500.org/news/japan-captures-top500-crown-arm-powered-supercomputer/>

⁵¹ Kostyukov V.E. Proposals for Development of Russian Supercomputer and Information Technologies. Projects of FGUP “RFYC-VNIIEF” (State Corporation “Rosatom”). Presentation at the Meeting Chaired by D.A. Medvedev, 19.02.2016. URL: <http://static.government.ru/media/files/p5s9xN7FOBTZFoMahAzjAGjSh0aiXBAJ.pdf>.

⁵² The Lomonosov Moscow State University Research Computing Center and the Interdepartmental Supercomputer Center of the Russian Academy of Sciences Announce the Release of the Thirty Second Edition of the Tor50 List of the Most Powerful Computers in the CIS // Lomonosov Moscow State University Research Computing Center. 2020. March 31. URL: http://top50.supercomputers.ru/newsfeed_local/11.

In September 2020, the Siberian National Center for High Performance Computing, Data Processing and Storage signed an agreement to create a network of supercomputer centers, whose goal is to become one of the top 50 supercomputers in the world⁵³.

3.2. Supercomputers in the Nuclear Sphere

The main projects in the nuclear sphere have been implemented at RFYC-VNIIEF since 2009, with 2020 declared as the deadline for achieving the target indicators. The characteristics and specifics of the supercomputer application in the city of Sarov are not regularly published in the open press. In February 2012 it was stated that the RFYC-VNIIEF supercomputer with a performance of more than 1 petaflops is among the ten most powerful in the world. Plans were also indicated to bring the capacity up to 5 – 10 petaflops “in the near future”, and by today (2019 – 2020) the goal of reaching the exaflops level was to be achieved. Obviously, there are problems worldwide with reaching such characteristics. At the same time, data on the actual performance of the Sarov supercomputers were not revealed in a thematic interview at the end of 2019⁵⁴. At the same time, in 2017, several RFYC-VNIIEF employees were implicated in a cryptocurrency mining⁵⁵. Note that back in the early 2010s, RFYC-VNIIEF developed a line of universal and specialized compact supercomputers with performance ranges from 1 to 8 teraflops⁵⁶. These machines are used at enterprises in the aerospace and nuclear industries. As of 2013, it was reported that more than 60 such computers had been delivered to various organizations⁵⁷. Striking evidence of at least positioning RFYC-VNIIEF as a leader in the supercomputing area in Russia is Rosatom's proposal to identify this organization as the sole supplier of supercomputer modeling systems for departments and state-owned companies from 2020 to 2024, namely the Logos automated design system⁵⁸. On the example of RFYC-VNIIEF results, namely one of the patents registered in 2018, one can assess the complexity of ensuring the operation of supercomputers as such, primarily in terms of cooling of computing system⁵⁹.

⁵³ A Network of Supercomputer Centers Will Be Created in Tomsk and Novosibirsk // TASS. 2020. September 16. URL: <https://tass.ru/sibir-news/9468063>.

⁵⁴ Russian Supercomputers Are Losing Their Positions in the Top-500. Is it important? // “Country-Rosatom”. 2019.24 September. URL: <http://strana-rosatom.ru/2019/09/24/%D0%BF%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D0%BA%D0%B0-%D1%81%D0%BA%D0%BE%D1%80%D0%BE%D1%81%D1%82%D0%B8/>.

⁵⁵ Bitcoins Tripled Mining in Sarov // Kommersant. 2019.26 October. URL: <https://www.kommersant.ru/doc/4140085>

⁵⁶ Compact Supercomputers // VNIIEF website. URL: http://vniief.ru/unvisible_aria/products/it/razr/7e6f3b8049bdd12cbafefe3d902053fb

⁵⁷ The Federal Nuclear Center in Sarov Has Produced More Than 60 Supercomputers // TASS. 2013. July 30. URL: <https://tass.ru/ekonomika/554776>.

⁵⁸ Rosatom is Loading into Supercomputers // Kommersant. 2020. 31 August. C. 5.

⁵⁹ Korzakov Y. N. et al. Cooling System for Massively Parallel Computing Systems. 10.05.2018, Patent of the Russian Federation 2653499.

In 2019, nuclear specialists from RFYC-VNIIEF, in cooperation with the Roselektronika holding company (the Research Center for Electronic Computing of the Vega Concern), created a computing complex for the information and telecommunications center of the Military Innovation Technopolis ERA in Anapa⁶⁰. The characteristics of this supercomputer have not been published, but a report in a departmental publication mentions another Roselektronika invention, a “compact mobile supercomputer”⁶¹. As stated in late 2018, it is capable of peak performance of 2.2 petaflops⁶². Note that the US Navy Supercomputer Center (Navy DSRC) currently has about the same capacity⁶³. But by the end of 2020 – beginning of 2021 the US Navy is planning to put a new supercomputer with 12.8 petaflops performance into operation, which will be the most powerful in the whole US military department⁶⁴. Technopolis “ERA” assumes that the supercomputer commissioned in the spring of 2019 is only the first stage, and in the future, an increase in computing power is planned. At the same time, according to the media, in May of the same year the head of this organization was replaced, which could relate to the dispute around the purchase of supercomputers.⁶⁵ Within the framework of “Army-2020” International Military Tech Forum (IMTF) it was tentatively agreed to use supercomputers of Technopolis ERA on deep learning neural networks⁶⁶.

Another development by Rostech is the first supercomputer based on Russian processors. In 2019, Research Institute for Control Computers named after I.S. Brooke used Russian 8-core Elbrus-8S microprocessors to create a supercomputer with a relatively modest capacity of 75 teraflops. However, at present it is difficult to say how widespread such import substitution will be.

“Compact Supercomputer” labeled as “APK-1MZ” is used since 2018 in the 12th Central Research Institute of the Russian Ministry of Defense, whose tasks include “justification of directions of development and maintenance of high combat readiness and efficiency of nuclear weapons of all types of the armed forces and arms of the Russian Federation”⁶⁷. APK-1MZ has a seemingly unimpressive peak

⁶⁰ Rostec Created a Computing Complex for Technopolis Era // Rostec State Corporation. 2019. March 25. URL: <https://rostec.ru/news/rostekh-sozdal-vychislitelnyy-kompleks-dlya-tekhnopolisa-era/>.

⁶¹ New “ERA”: Supercomputer, Electronic Superbrain // Zvezda Weekly. 2019. March 29. URL: <https://zvezdaweekly.ru/news/t/20193281328-FqxE6.html>.

⁶² Rostec Has Created a Mobile Supercomputer // Official Website of Rostec State Corporation. 2018. November 23. URL: <https://rostec.ru/media/pressrelease/rostekh-sozdal-mobilnyy-superkompyuter/>.

⁶³ Navy DSRC // Linpack Top-500 website. URL: <https://www.top500.org/site/50425>.

⁶⁴ DoD to Install Cray-AMD System at Navy DSRC in Mississippi // HPCWire website. 2020. February 17. URL: <https://www.hpewire.com/off-the-wire/dod-to-install-cray-amd-system-at-navy-dsrc-in-mississippi/>.

⁶⁵ The Head of the Military Technopolis “Era” Moved to the Presidential Administration // RBC. 2019. May 27. URL: <https://www.rbc.ru/society/27/05/2019/5ce674799a794703564069ec>.

⁶⁶ The Supercomputer of Military Innovation Technopolis “ERA” Will Test the Best Processors for Deep Learning Neural Networks // Official website of the Ministry of Defense of Russia. URL: <http://mil.ru/era/news/more.htm?id=12310458@egNews>.

⁶⁷ Twelfth Central Research Institute of the Ministry of Defense of the Russian Federation Named after V.A. Bolyatko (12th Central Research Institute of the Defense Ministry) // Official Website of the Ministry of

performance of 1.2 teraflops and is used for “numerical and simulation modeling of the implementation of parallel algorithms for processing large amounts of information during scientific research, followed by visualization of the calculated data”⁶⁸.

3.3. Using Supercomputers

Among the specific tasks to be solved using the supercomputer developed by the 12th Central Research Institute of the Russian Ministry of Defense is the modeling of several phenomena, including:

- the effects of an airborne shock wave on various weapons and military equipment (including mobile missile launchers),
- “Fall of the product on the concrete surface”, which, based on the illustrations, is understood as an assessment of the penetration capability of cruise missiles on the one hand and the resistance of protective structures to defeat by high-precision weapons on the other hand,
- the impact of electromagnetic radiation on the instrument compartment, which is an important element in assessing the resistance of certain products to the effects of a nuclear explosion – primarily the heads of missile systems of various types.

Other supercomputers (e.g., Lomonosov at Moscow State University, once the most powerful in Russia) are used to solve a wide range of tasks in the field of aerospace technology, drug development, seismology, etc.⁶⁹ One example of direct use of supercomputers for purposes directly related to Russia's defense capability is performing calculations for hypersonic vehicle development. Thus, based on the infrastructure of the Interdepartmental Supercomputer Center of the Russian Academy of Sciences (ISC RAS), simulation of high-speed turbulent flows at an air intake device⁷⁰ was performed. Such tasks are one of the key elements of designing cruise missiles with scramjet engines.

In the field of space technology, the use of supercomputers allows, for example, high-precision simulation of abnormal situations during the landing of descent spacecrafts, considering all possible scenarios and conditions of various environments. Thus, it is possible to reduce the development time and the cost of

Defense of Russia. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=12994@morfDictionary.

⁶⁸ According to information obtained by the author at the booth of the 12th Central Research Institute within the framework of the ISTF “Army-2020”.

⁶⁹ Supercomputer “Lomonosov” // Official Website of Moscow State University. URL: <https://www.msu.ru/lomonosov/science/computer.html>.

⁷⁰ Bendersky L.A., Lyubimov D.A., Rybakov A.A. Analysis of Scaling Efficiency in Calculations of High-Speed Turbulent Flows on the Supercomputer RANS/ILES by High Resolution Method // Proceedings of the Research Institute for System Research of the Russian Academy of Sciences. – 2017. – T. 7. – №. 4. – C. 32-40.

experimental testing of specific solutions. Modeling with the use of supercomputers also makes it possible to obtain a more accurate picture of turbulence processes, which is extremely important for the development of engines and high-speed systems⁷¹, among others.

In November 2019, the Central Research Institute for Precision Machine Building launched the “Center” software and technological complex with a performance of 50 teraflops for simulating tests of small arms and ammunition (evaluation of shooting accuracy by varying geometric parameters and initial bullet velocity, conditions of its flight from the barrel's channel)⁷². “Minin” supercomputer with a peak performance of 57.6 teraflops has also been operating since 2012 in JSC “Central Research Institute Burevestnik”, one of the leading domestic developers of artillery weapons. Interestingly, this company provides supercomputer computing resources for external users⁷³ as well.

US *Navy DSRC* capabilities are used to model climate, weather, and global oceans for the US Navy's meteorological units, allowing for consistently improved weather forecasts and, as a result, increased force effectiveness with a more accurate picture than that available to the enemy.

Supercomputers are also used in the fight against the SARS-CoV-2⁷⁴ pandemic. In the USA, military supercomputers are used to solve problems of increasing the safety of transporting infected people by air and reducing the risks of infection for crews by simulating air and moisture flows inside aircraft. In addition, supercomputer computing power is used to pre-evaluate the effectiveness of potential vaccines. An Oak Ridge National Laboratory *Summit* supercomputer has been used for genetic studies of patients with the new coronavirus, revealing the specific processes of the actual disease caused by SARS-CoV-2 and, potentially, improving the effectiveness of treatment and the development of new drugs⁷⁵.

The next stage of development, as already mentioned, will be the transition to the exam scale, i.e., to an exaflops-level super-computer. As stated, in the very near future two supercomputers with a capacity of more than one and a half exaflops each

⁷¹ Supercomputer Technologies in Science, Education, and Industry / Edited by V.A. Sadovnichy, G.I. Savin, V.V. Voyevodin. – Ser. 7 Supercomputer Education – Moscow: M.F. Lomonosov Moscow State Technical University, 2017.

⁷² Rostec Has Put the Center Supercomputer into Operation // Official website of Rostec State Corporation. 2019. November 8. URL: <https://rostec.ru/news/rostekh-vvel-v-stroy-superkompyuter-tsentr-/>.

⁷³ High Performance Computing Center at JSC “Central Research Institute “Burevestnik”. URL: https://www.burevestnik.com/products/yslugi_c.html

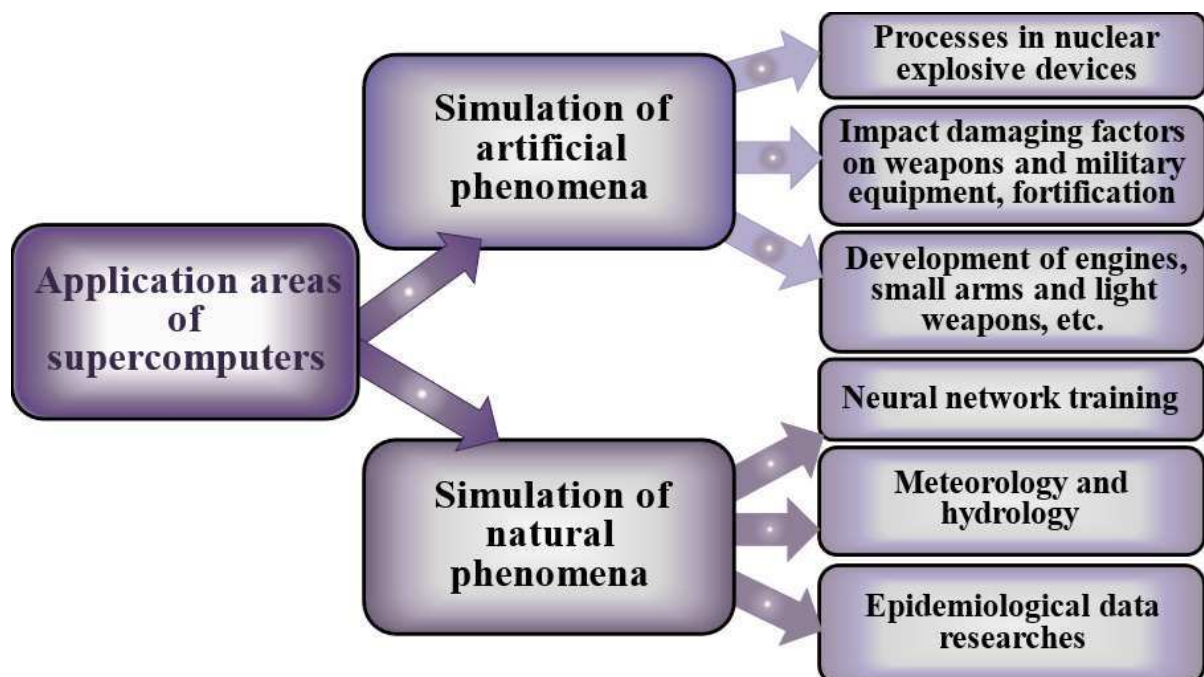
⁷⁴ Pentagon Supercomputers Puzzle Out How to Safely Airlift Coronavirus Patients // Defense One. 2020. April 13. URL: <https://www.defenseone.com/technology/2020/04/pentagon-supercomputers-puzzle-out-how-safely-airlift-coronavirus-patients/164553/>.

⁷⁵ Anderson M. Has the Summit Supercomputer Cracked COVID's Code? // IEEE Spectrum. 2020. August 2, URL: <https://spectrum.ieee.org/the-human-os/computing/hardware/has-the-summit-supercomputer-cracked-the-covid-code>.

will be launched in the USA.⁷⁶ The cost of their five-year development was \$1.8 billion. At the present time, more than two dozen teams of scientists are completing the preparation of the tasks, whose solution will require such power. The most promising areas include the energy industry, and almost all its directions – from miniaturization of internal combustion engines to increasing the efficiency of wind energy. New impetus can also be given to work in the field of thermonuclear energy.

All issues solved with the use of supercomputers can be conventionally referred to high-precision modeling of artificial and natural processes (Figure 3.2).

Figure 3.2. Applications of supercomputers



Source: Picture built by the author.

3.4. “Supercomputer security”

It seems reasonable to introduce the term “*supercomputer security*”, which is proposed to understand *the use of supercomputer technology to solve problems related to national defense in the broadest sense. Security in this case is defined as the state of protection of vital interests of the state from internal and external threats emanating from the possible decisive advantage of other countries, as well as non-state actors in the field of supercomputing.*

⁷⁶ Cleaner-Burning Gasoline Engines, Cities Powered by Wind, Nuclear Reactors That Fit on a Tabletop-Soon They Could All Be Within Reach // Exascale Computing Project. 2020. May 18. URL: <https://www.exascaleproject.org/cleaner-burning-gasoline-engines-cities-powered-by-wind-nuclear-reactors-that-fit-on-a-tabletop-soon-they-could-be-within-reach/>.

In general, in this field, supercomputers are used in the following key areas:

- maintenance and modernization of the nuclear arsenal in the absence of field experiments,
- optimization of development processes for advanced weapons and military equipment by reducing the number of tests, thanks to qualitatively new modeling capabilities,
- meteorological tasks on a global scale for the armed forces to predict the state of various environments and plan operations considering all necessary external factors.

In the context of increasing competition on the world stage, rivalry between “great powers”, and given that a number of tasks that require supercomputing capacity are among the most sensitive sectors of science and industry, directly affecting defense capabilities, it is difficult to hope to create conditions for expanding international scientific and technological cooperation in this area.

At present Russia is inferior to the leaders of the “supercomputer race” both qualitatively and quantitatively. At the same time, one cannot say that our country is still. It is also important to unite efforts of different participants of the domestic “supercomputer market” possessing relevant competences. In this regard, it seems that the only way to preserve and increase Russian Federation's potential in this field is to continue creating its own supercomputers based both on imported and domestic element bases. The recognition of the importance of this direction was seen at the thematic round table “The use of supercomputer technologies in the Russian Federation Ministry of Defense” within the framework of “Army-2020” IMTF⁷⁷, full information about which, as well as the presented assessments and proposals has not yet appeared in open sources.

Participation of domestic defense supercomputers in internal ratings could be a significant help to improve the accuracy of estimates in this area. Such an approach, apart from obvious benefits for the expert community and research organizations, would improve Russia's image as one of the flagship countries of the global digital transformation. In addition, it is possible that as part of the processes of diversification of the defense industrial complex, greater openness of information about the computing capacities of various enterprises and access to these capacities by commercial users could contribute to the growth of the share of “civilian” revenues of defense industry enterprises.

⁷⁷ The Use of Supercomputer Technology in the Ministry of Defense of the Russian Federation // Official Website of MVTF “Army”. URL: https://www.rusarmyexpo.ru/business_program/4107/33388.html.

CHAPTER 4

Strategic Stability and Information and Communication Innovations

4.1. Strategic Stability in the Era of Information and Communication Technology

The term “*stability*” in any field refers to constancy or the ability of a system to function, keeping its structure unchanged and returning to a state of equilibrium even after the impact of destabilizing forces (factors). In the politico-military sphere it is commonly believed that the higher the level of strategic stability, the less likely a large-scale and, above all, nuclear war will occur. For many years the concept of “*strategic stability*” in relations between the nuclear powers has been defined as *the state of their relations in which the incentives to launch a nuclear first strike is removed*. This was based on the realization that all the countries of the world had an interest in ensuring a necessary and sufficient level of strategic stability, but that the two largest nuclear weapon states bore the greatest responsibility. Since nuclear weapons still exist and their destructive capabilities are constantly being improved, this understanding of strategic stability is as relevant today as it was when it was formed during the Cold War.

However, over the past three decades the situation has changed significantly, the ideas about the ways and mechanisms of preventing nuclear war, developed in the period of bipolarity, no longer fully correspond to today's geopolitical realities and the level of technological development. These significant changes in international politico-military relations require taking into account not only the nuclear component, but also other indicators, while maintaining the traditional essence. In addition, today we are no longer talking about two global poles of confrontation, as during bipolarity, but about an increase in the number of factors influencing the level of strategic stability. Consequently, today it is necessary to talk not about poles, but about the system, and thus to assess the capabilities and characteristics *of the modern politico-military system*.

Considering *the strategic stability of military and political system as a state of peace (absence of large-scale war) within this system, which is maintained even under constant perturbations (destabilizing factors) for a certain (given) period of time*⁷⁸, at present we can state the existence of several global problems associated with the lack of common understanding between the world powers who are the main participants of the process of strategic stability, the characteristics of the military-

⁷⁸ Romashkina N.P. Strategic Stability in the Modern System of International Relations. – Moscow: Nauka, 2008. URL: <http://www.avnrf.ru/index.php/drugie-publikatsii/590-strategicheskaya-stabilnost-v-sovremennoj-sisteme-mezhdunarodnykh-otnoshenij>.

political system that should be maintained during the planned time, and most importantly, destabilizing factors.

Consequently, at the professional level it is necessary to talk not just about “maintaining” strategic stability, “preserving” it, “strengthening” it, etc. But rather about the need *to ensure* strategic stability and to work out new common qualitative and, most importantly, quantitative approaches to assessing its level based on available experience. And for this purpose, it is necessary to agree on common evaluation criteria.

The process of discussing such criteria has been halted at the Russian-US bilateral level since the mid-1990s because the United States did not consider it necessary. Today this has led to a global problem, because reducing the level of strategic stability below the necessary and sufficient level is extremely dangerous for all states without exception. Consequently, all countries of the world are interested in ensuring the necessary and sufficient level, as before, and it is still the nuclear-weapon states, whose number and role have changed, that bear the greatest responsibility.

What are the characteristics of a system in which it is vital to ensure a necessary and sufficient level of stability? What new destabilizing factors have emerged in recent decades?

1. *The changing indicators of the system of international relations after the periods of bipolarity and monopoly, led by the United States, with the complication of military-strategic relations between Russia and the United States, and with the emergence of a new global center of power – China, which is not involved in the process of nuclear disarmament.*

2. *The gradual erosion of the strategic arms limitation and reduction regime following the USA withdrawal from the Anti-Ballistic Missile (ABM) Treaty and the Intermediate-Range Nuclear Forces (INF) Treaty, the unsustainable existence of inter-state conventional arms agreements, and the absence of formal negotiations on nuclear arms limitation and reduction at the end of the START-3.*

3. *Nuclear missile multipolarity, which is expressed in the increase in the number of states with missiles and nuclear weapons, as well as in the growing probability of their further proliferation (states possessing ballistic missiles are in the Table 4.1).*

Table 4.1. States possessing ballistic missiles

№	State	№	State	№	State
1	Azerbaijan	14	Greece	27	UAE
2	Algeria	15	Denmark	28	Pakistan
3	Angola	16	Israel	29	Republic of Korea
4	Argentina	17	India	30	RF
5	Armenia	18	Iraq	31	Serbia and Montenegro
6	Afghanistan	19	IRI	32	Syria
7	Bahrain	20	Yemen	33	USA
8	Belarus	21	Kazakhstan	34	Taiwan
9	Brazil	22	DPRK	35	Turkmenistan
10	UK	23	PRC	36	Turkey
11	Vietnam	24	Cuba	37	Ukraine
12	Egypt	25	CSA	38	France
13	Germany	26	Libya	39	Japan

Source: Romashkina N.P., Markov A.S., Stefanovich D.V. International Security, Strategic Stability and Information Technologies – Moscow, IMEMO, 2020. – 98 p. (in Russian). URL: <https://www.imemo.ru/files/File/ru/publ/2020/2020-017.pdf>.

4. *Doctrinal changes in nuclear-weapon states* that are formally designed to strengthen deterrence but actually lower the threshold for the use of nuclear weapons.

5. *The evolution of military doctrines and strategies of NATO members, allies, and partners in ICT* that allow for defensive responses to an ICT-attack in both wartime and peacetime. NATO's decision to invoke Article 5 of the Alliance Charter in response to cyber-attacks is fundamental.

6. *Creation of a large-scale US missile defense system* (Figure 4.1).

Figure 4.1. US allies and partners in the creation of a large-scale missile defense system



Source: Romashkina N.P., Markov A.S., Stefanovich D.V. International Security, Strategic Stability and Information Technologies – Moscow, IMEMO, 2020. – 98 p. (in Russian). URL: <https://www.imemo.ru/files/File/ru/publ/2020/2020-017.pdf>.

7. *The increasing role and power of non-nuclear (high-precision and high-intelligence) weapons in strategic planning.*

8. *The basing of nuclear and non-nuclear weapons on the same platforms, because of which the launch of ballistic or cruise missiles with conventional weapons can be considered by the opponent as the use of nuclear weapons.*

9. *The emergence of low-yield nuclear weapons, the presence of which lowers the threshold for the use of nuclear weapons and increases the likelihood of an armed conflict escalating into a nuclear war.*

10. *Development of the latest ICT-based anti-satellite tools that allow the destruction of satellites by means of anti-satellite systems placed on the ground, as well as to influence the work not only of artificial Earth satellites of peaceful, but also dual and military purposes, including elements of EWS⁷⁹. Such means can affect*

⁷⁹ According to the latest data, there are more than two thousand active satellites in space: more than 900 belong to the United States, about 150 to Russia, about 300 to China and the rest to other states.

the effectiveness of satellites as part of the systems of warfare in the common information space, which is actively being improved in the states, developed in military respect. This is one of the most serious threats to strategic stability at the present stage. Recall that in June 2018 for the first-time cyber interference was detected in the functioning of a US military satellite, when, according to the company *Symantec*, the introduction of a “bookmark” in the software of the SU allowed to change the orbit of the satellite and intercept sensitive data⁸⁰.

11. *The possibility of militarization of outer space, including the use of the latest ICT.*

12. In addition to the technological characteristics that affect the level of strategic stability, more and more experts from different countries are paying attention to another feature of the modern world - the psychological one. It can be formulated as a *loss of fear of nuclear war among society and political elites*⁸¹. This situation can significantly lower the threshold for the use of weapons, including nuclear weapons.

In developing criteria for assessing the level of strategic stability and specific plans to ensure it based on the criteria, it is advisable to take into account both the characteristics common to any historical period and the specifics of the modern stage. The accelerated development of information and communication technologies is currently one of such exceptional features. At the same time, all destabilizing factors are now aggravated by the possibility of using ICT for destructive purposes. The lack of global governance mechanisms in this area (see chapter 1 of the monograph) also leads to a lower level of strategic stability than in the period of bipolarity. Cyber threats aggravate, complicate, deepen, amplify, and modify the problems that have always existed in ensuring nuclear weapons security (Figure 4.2).

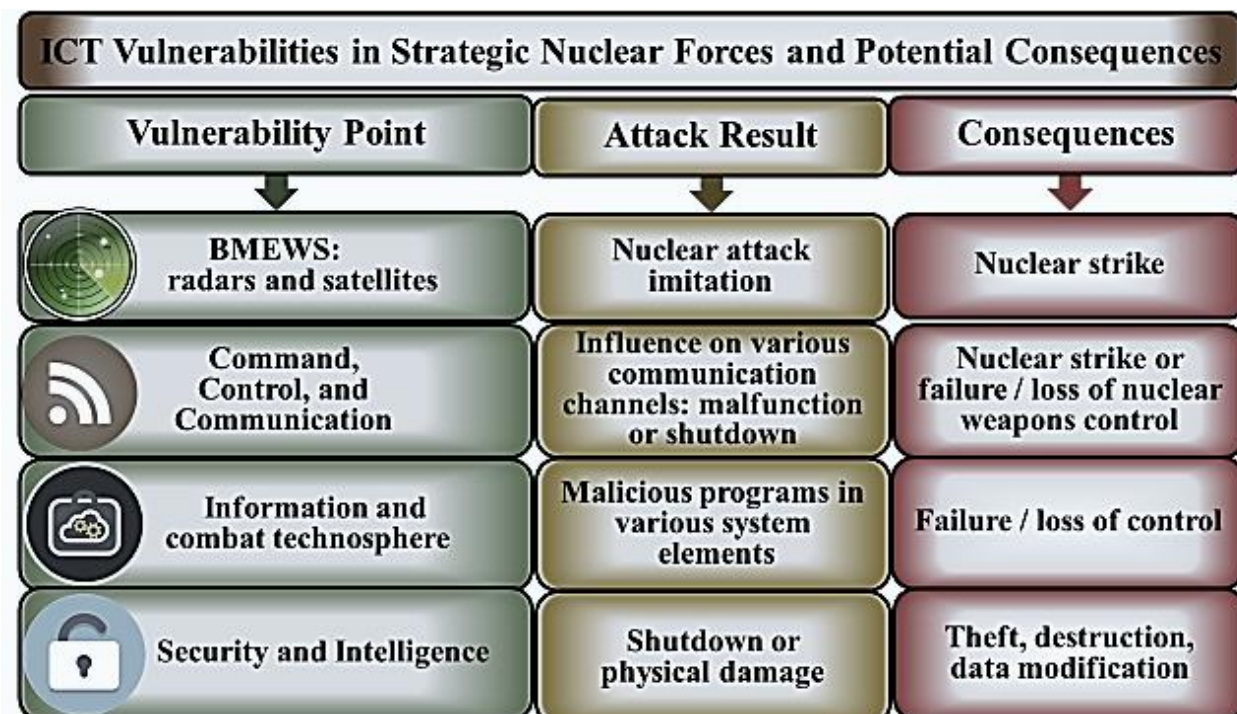
Not so long ago, skeptics suggested that it was inexpedient to discuss the issues of linking nuclear and cyber problems in the military field, that no agreements in this area were possible, and so on. However, the natural process of development of scientific and technological progress, primarily in the field of 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, the problem of ICT influence on the level of strategic stability recognized at the highest level in the great powers. The transition of the problem of the impact of ICT on the level of strategic stability to a new format takes place

⁸⁰ Symantec Recorded a Cyber Attack on Satellite Operators in the US and Asia // TASS. 2018. June 20. URL: <https://tass.ru/mezhdunarodnaya-panorama/5306217>.

⁸¹ Trenin D. V. Strategic Stability in a Changing World Order // RIAC. 2019. March 20. URL: <https://russiancouncil.ru/analytics-and-comments/comments/strategicheskaya-stabilnost-v-usloviyakh-smeny-miroporiyadka/>.

against the background of important events in the development of the international information security system and Russia's participation in this process.

Figure 4.2. Strategic nuclear weapons: selected ICT vulnerabilities and potential impacts



Note: The information-impact techno sphere is a set of technical information, control, impact, support and maintenance devices and systems together with the area of human military-technical activity.

Source: Romashkina N.P. Global military-political problems of international information security: trends, threats, prospects // *Voprosy kibbezopasnosti*. – 2019. № 1. URL: https://cyberrus.com/wp-content/uploads/2019/03/02-09-129-19_1.-Romashkina.pdf.

September 25, 2020 Russian President Vladimir Putin proposed a comprehensive program of measures for restoring Russia-US cooperation in the field of international information security, and in 2020 – 2021 he repeatedly stated the need to sign bilateral documents between the 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 space.⁸²

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 new edition of one of the fundamental

⁸² “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). URL: <http://en.kremlin.ru/events/president/transcripts/statements/64086>.

documents in this area, “Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security”.⁸³

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 US Department of State.⁸⁴ 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 situation in outer space, where the danger of an arms race is growing, as well as the problems of cybersecurity, are of paramount importance.⁸⁵

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 USA.⁸⁶

However, in 2022, the US unilaterally withdrew from cyber agreements reached in 2021 under the pretext of Russia’s special military operation (SSO) in Ukraine, embarking upon the path of aggressive action. Thus, in the short term, the United States is not willing to engage in dialogue with Russia as an equal partner, while Moscow will not accept any interactions imposed on it from a position of power. As was noted by Andrey Krutskikh, Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information

⁸³ “Fundamentals of the State Policy of the Russian Federation in the Field of International Information Security” (in Russian), April 12, 2021. URL: <http://www.kremlin.ru/acts/bank/46614>.

⁸⁴ Joint statement on the meeting in the framework of the Russian-US dialogue on strategic stability in Geneva, (in Russian), September 30, 2021, Joint statement on the meeting in the framework of the Russian-US dialogue on strategic stability in Geneva, September 30, 2021. URL: https://www.mid.ru/ru/foreign_policy/news/1777978/?lang=en.

⁸⁵ “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. URL: <https://tass.ru/politika/11535921>.

⁸⁶ Meeting with US President Joseph Biden, December 7, 2021, President of Russia (website). URL: <http://en.kremlin.ru/events/president/news/67315>.

Security, “We must agree on equal terms and on constructive solutions to global problems, those that exist in these areas in our bilateral relations”.⁸⁷

It is logical to assume that awareness of the globality and danger of threats, as well as awareness of mutual vulnerability, should lead the great powers to understand the need to draw “red lines” in cyberspace at both the factual and legal levels.

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 conferences on international security of the Russian Ministry of Defense in 2021 and 2022. In his report at the opening of the Conference in June 2021, 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”.⁸⁸

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.”⁸⁹

Several global problems of strategic stability emanating from the information space can be distinguished.

Problem 1: The growing probability of disabling or destroying nuclear weapons through the harmful effects of ICT, which already affects the prospects for nuclear disarmament and nonproliferation. On the one hand, the emergence of such

⁸⁷ Russia called for the intensification of international efforts in the field of cybersecurity. TASS. URL: <https://tass.ru/politika/16980085>.

⁸⁸ “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. Russia called for the intensification of international efforts in the field of cybersecurity. URL: <https://mil.ru/mcis/news/more.htm?id=12368274@egNews>.<https://mil.ru/mcis/news/more.htm?id=12368274@egNews>.

⁸⁹ “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. URL: https://function.mil.ru/news_page/country/more.htm?id=12331668@egNews.

a possibility may provide the states possessing nuclear weapons with a pretext to accelerate reduction of their arms. On the other hand, and more probably, it may become a serious reason for large-scale modernization of nuclear weapons, creation of more sophisticated and protected systems, which may result in qualitative and/or quantitative nuclear arms race and, consequently, a lowering of the level of strategic stability. Besides, information security issues already affect not only the prospects of nuclear disarmament and non-proliferation, but also the existing restrictive regimes.

Problem 2: The most serious, though still unlikely, threat is *the impact of false information from ICT on the likelihood of erroneously authorized launches of BM, as well as on the decision to use nuclear weapons*. The task of ballistic missile defense against erroneous launches has arisen since the first missiles were created. Every time it is solved anew during creation of new BMs, by putting them on duty, and by preparing and conducting tests, combat-training and combat-check launches. Although both the United States and Russia (the USSR) have always paid great attention to this issue, over the decades of nuclear weapons existence both countries have had cases of technical failures and human errors that could provoke a nuclear launch. Reducing the probability of an erroneous launch, which is never zero, will become more critical as the strategic forces move to digital information transfer technologies. For example, according to the Russian Ministry of Defense, our Strategic Rocket Forces (SRF) are expected to be fully digital by 2020⁹⁰.

This problem is related to the following possibilities of ICT:

- receiving false information from early warning systems (EWS) about enemy ballistic missile launches with nuclear weapons,
- implementation in the control of communication systems in the command posts of the SRF to create a situation of erroneous authorized launch,
- direct implementation into electronic systems of communication, command, and control over nuclear weapons (Automated Battle Management Systems – AMBS – in Russian terminology, Nuclear Command, Control, and Communications – NC3 – in Western terminology).

Hacking attacks can damage or disrupt communications channels, interfere with the command-and-control systems of armed forces, including nuclear forces, and reduce the confidence of military decision makers in the operability and effectiveness of command-and-control systems. For example, attackers can use DDoS attacks to disrupt communications, command, and control, and targeting systems. In a crisis, ICT attacks can negatively affect the decision to respond (Figures 4.3, 4.4). The threat of ICT-mediated disabling of military systems can

⁹⁰ By 2020 the Strategic Rocket Forces Will Completely Switch to Digital Information Transmission Technologies // Website of the Ministry of Defense of the Russian Federation URL: https://structure.mil.ru/structure/forces/strategic_rocket/news/more.htm?id=12142122%40egNews.

reduce the search for alternatives to military action and create significant challenges to successful signaling. As a result, the “escalation ladder” of conflict will be reduced, which, in turn, may cause the temptation to win the war without receiving a retaliatory strike.

In addition, this problem is related to the possibility of using the so-called “false flag” in cyber interference, when operations are conducted in such a way as to give the impression that they have been carried out by another actor. This also does not exclude the possibility of perceiving some actions as the initial stage of transition to the conditions of guaranteed mutual destruction. All this increases the probability of mistakenly launching BMs, and consequently reduces the level of strategic stability.

Threats are further amplified by the development of remotely controlled robotic strike capabilities⁹¹, AI for military purposes, machine learning, autonomous operation capabilities of various systems and subsystems, etc. that can be subjected to ICT- attacks, cyber-electromagnetic activities that are actively developed in the United States and which include cyber operations, electronic warfare, peacetime electronic attacks, and electromagnetic spectrum management operations.

One of today's opportunities to reduce ICT threats in the military sphere is the development of quantum cryptographic systems for information protection, including those of a defense nature. According to the Russian Ministry of Defense, Russia has the potential to produce such systems, including for military purposes⁹². Note that quantum cryptography is a method of protecting communications based on the principles of quantum physics, in contrast to traditional cryptography based on mathematical methods. The process of sending and receiving information in quantum cryptography is performed by physical means, for example, using electrons in electric current or photons in fiber-optic communication lines. Thus, constant, and automatic change of keys during transmission of each message in a one-time “encryption book” mode is provided. Technology relies on fundamental uncertainty of quantum system behavior – it is impossible to measure one photon parameter without distorting another. Therefore, it is possible to create such a communication system, which will always detect tampering: an attempt to measure parameters in a quantum system introduces disturbances into it, destroying or distorting original signals, which means that by noise level in a channel legitimate users can recognize that an interceptor is being used. To date, this is the only type of encryption with strictly proven cryptographic strength.

⁹¹ Balybin V.A., Vystorobsky S.G., Eltsov O.N., Syrbu I.A. Robotized Complexes of Electronic Warfare: Prospects for Creation and Use. Radio-Electronic Warfare in the Armed Forces of the Russian Federation, 2018. Materials from the radio-electronic warfare troops of the Armed Forces of the Russian Federation. 2018. URL: <https://reb.informost.ru/2018/pdf/1-5.pdf>.

⁹² Inforum 2018. The Defense Ministry Is Considering the Idea of Developing Quantum Cryptomachines // National Forum on Information Security “Inforum” Website. URL: <https://infoforum.ru/news/infoforum-2018-minoborony-rf-obdumyvaut-ideu-razrabotki-kvantovyyh-kriptomashin>.

Figure 4.3. Stages of classical warfare without the complex use of ICTs

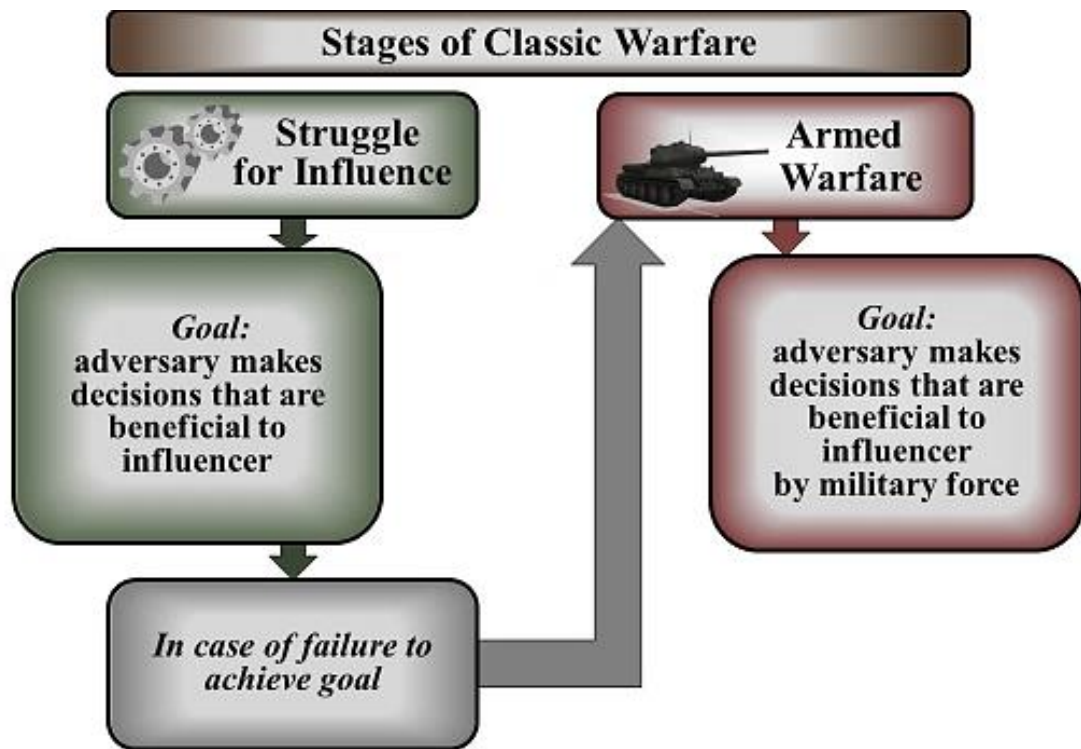
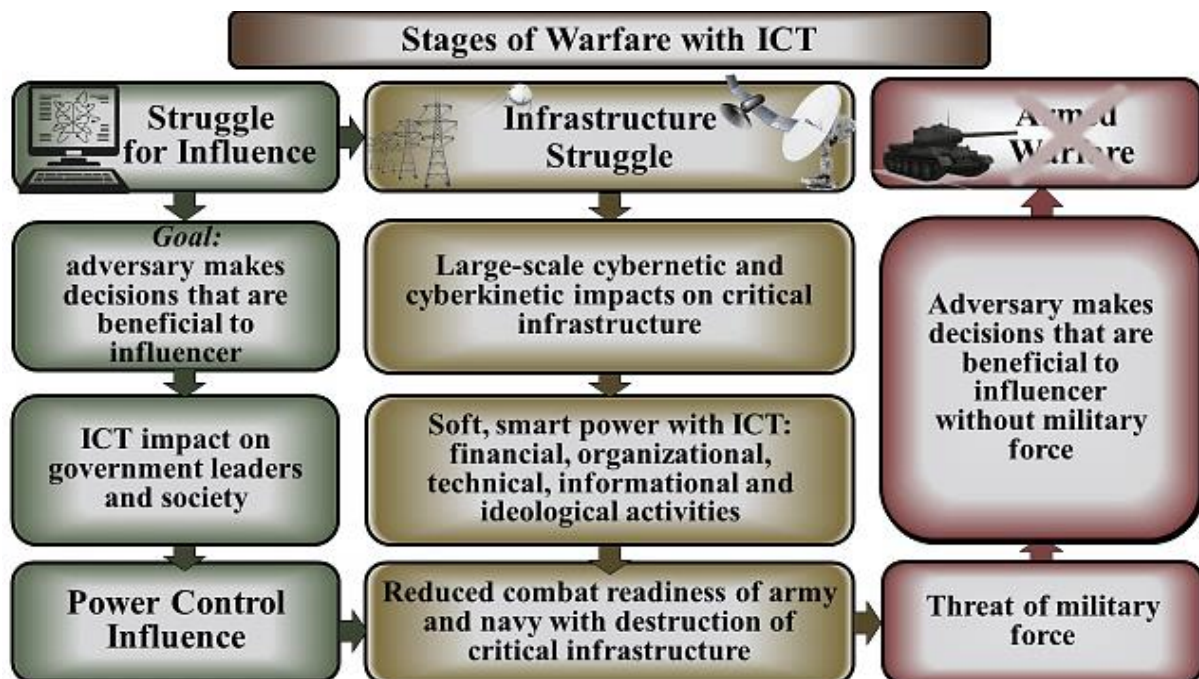


Figure 4.4. Stages of warfare with complex use of ICTs.



Source: Romashkina N.P. New Technologies: Challenges to International Security and Stability. BIT-2020: XX International Scientific and Technical Conference on Secure Information Technologies. URL: <https://ceur-ws.org/Vol-2603/short14.pdf>.

Problem 3: *The role of nuclear weapons in preventing information attacks on the military and other critical infrastructure of states.* So far, this problem looks purely theoretical. But given the rapid growth of threats in the information space, one must be aware that the nuclear and information spheres will probably be even more intertwined in the future, and this issue may become more acute.

4.2. Information and Communication Technology and Nuclear Deterrence

In the context of strategic stability, specific ICT threats to various elements of the systems of operation and use of nuclear weapons, the nuclear weapons themselves, as well as the supporting control and communications circuits, are crucial and yet insufficiently investigated, so they require additional expert analysis.

4.2.1. Directions and means of influence

For the purposes of this analysis, it is suggested that **ICT threats** be understood as *the potential for interference with the normal (planned) functioning of various systems and subsystems of controlling nuclear weapons and their carriers (including onboard ones) using cyber and other information technologies (“cyber interference”)*⁹³. In general, the directions and purposes of such interference are shown in Figure 4.5.

Let us distinguish several types of attacks in the area under consideration based on the means and technologies used:

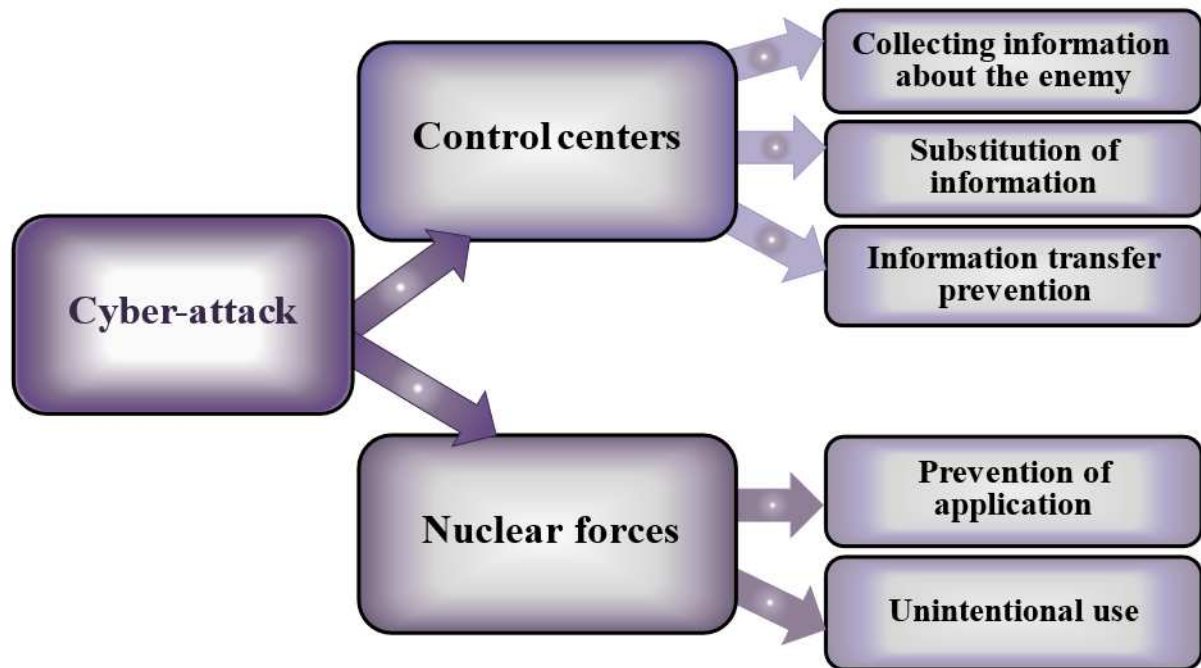
- 1) malware introduced via an external network infrastructure using public networks or by connecting covertly to closed networks,
- 2) malware introduced via physical media, either deliberately (“their own agents”) or by spoofing devices used by operators of certain systems and subsystems,
- 3) radio-electronic warfare (REW) equipment for tactical and strategic purposes of various types of basing,
- 4) “tabs” in the element and software base of the equipment at the stage of its creation and delivery to the enterprises that carry out production and final assembly in the interests of the relevant customers,
- 5) deception of sensors collecting information of all types used in the EWS, combat control, as well as various management decision support systems.

A peculiarity of malware used, including in military operations (ICT weapons, cyberweapons), is the inability to reliably identify the enemy's target, even if the software itself has already been detected. Identical samples of ICT weapons can be

⁹³ Author's definition.

used both to gather information and to exert cyber influence on the systems they have infiltrated.

Figure 4.5. Cyberspace and nuclear weapons



Sources: Stoutland P., Pitts-Keefer S. nuclear weapons in the New Cyber Age // Nuclear Threat Initiative (NTI). 2018 URL: https://media.nti.org/documents/Nuclear_Weapons_in_the_New_Cyber_Age-Russian_Translation.pdf; Romashkina N. Strategic instability in the ICT era: crisis or new norm? // RIAC, 2019. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-nestabilnost-v-epokhu-ikt-krizis-ili-novaya-norma/>.

Another feature of cyber weapons that is somewhat similar to nuclear weapons is the separation of the delivery vehicle and payload: the same product can be used to introduce malicious software, both for surveillance and information gathering and for intercepting control of weapon systems or disabling command networks. Thus, there is a kind of fork in decision-making by both attacking and defending parties: after a successful delivery of a relatively “harmless” software payload to the defender's network, if tensions between the parties escalate, an attempt to replace the “harmless” payload with a “strike” one is possible. In this case “defender” can timely detect the initial attack and in the absence of reliable information about plans of “attacker” make its own return or reciprocal strike, thus already not limiting itself to cyberspace. Naturally, in this situation we are talking about networks directly related to nuclear weapons and state survival.

In this connection it seems appropriate to further detail the classification according to the purposes of hostile influence: gathering information about the enemy; “spoofing” information used by the enemy; disabling the enemy's equipment; preventing the use of the enemy's nuclear forces; and the unintentional use by the

enemy of his nuclear forces, primarily against third countries. With this classification in mind, it is possible to assess the various elements of types of nuclear forces in terms of their vulnerability.

Separately, we can distinguish four main categories of actors operating at the intersection of the ICT space and nuclear weapons: states, their “proxies” (associated nonstate organizations), private structures (terrorist and commercial) and the so-called “lone wolves”. States have the greatest potential, but in the context of nuclear weapons they are also the most vulnerable, acting as the main potential victim. Non-state actors tend to be involved in inter-state struggles. Private actors can use cyber weapons to blackmail nuclear powers or offer their services to provide them with defense capabilities. Soloists may try to monetize their skills by displaying them in the most flamboyant way, or they may be driven by ideological or emotional motives. At the same time, the same actor's approach to cyberspace and ICT-enabled activities (including conventional warfare) may differ significantly. For example, in terms of the possibility of using intermediaries, demonstrating one's own capabilities, comments by officials on the facts of offensive or defensive operations using ICTs, and approaches to assessing the seriousness of cyber incidents and investigating them.

4.2.2. Objects of impact: control centers

As already noted, the most catastrophic consequences can be caused by interference with the control systems of nuclear forces, as well as the EWS. The control loops of individual elements of nuclear deterrence forces and means are separated, but at a certain stage all decisions are made at the level of the highest military and political leadership of the country. Accordingly, the quality and timeliness of the information that reaches the decision-making centers, as well as the speed and integrity of communicating orders to units and combat crews, directly determines the effectiveness of the response to the emerging situation.

Another serious threat is the use of electronic warfare for the purpose of “deceiving” MWS and missile defenses.

The problem of vulnerability of nuclear weapons command and control systems is exacerbated by the high degree of readiness of the SNF for action. Theoretically, a devastating “disarming” strike can be delivered with cyber weapons. At the same time, awareness of the risk of a cyber-attack by a “likely adversary” creates an incentive to strengthen the protection of SNF control networks against acts of illegal interference, regardless of their sources, which generally contributes to the maintenance of strategic stability. A similar problem may arise regarding the missile systems of third nuclear powers. For them, nuclear weapons are of exceptional value, and the threat of their loss in the event of a breach in the channels of command delivery is as serious as possible. In order to avoid a scenario of a decapitating cyber

strike, it is possible to delegate the authority to use nuclear weapons to lower levels of command, which further exacerbates the danger: a reaction to a false alarm or a false understanding of the operational situation on the part of the executive officer may entail a nuclear escalation, and an increase in the number of authorized commanders obviously leads to a proportional increase in such a threat. Clearly, ICT-enabled attacks significantly increase such risks.

One of the traditionally thorny questions of nuclear deterrence again arises in ICT threats and in general the impact of breakthrough technologies on nuclear weapons: what degree of readiness is the most “stabilizing”? In the case of Russia and the United States, a high launch readiness for intercontinental-range ballistic missiles remains the optimal solution because it guarantees retaliation that keeps a likely adversary from a first strike. Thus, the guarantee of inevitable retaliation outweighs the threat of an accidental launch in the eyes of the top military and political leadership of the two countries. At the same time, both Russia and the United States are making significant investments in building the most “survivable” retaliatory strike capability (including “deep”).

The availability of cyberweapons, digital warfare, and the desire of state and nonstate actors to gain an advantage over a potential adversary by damaging its nuclear weapons (the concept of “launch prevention”) or creating conditions for their mistaken use are real factors that must be considered.

4.2.3. Objects of impact: combat systems

ICT threats are also present at other echelons of the command and control and operational use of nuclear forces. To assess threats, it seems appropriate to consider the following factors:

- digitalization of the element base,
- connectivity with other elements of the information and communications infrastructure of the armed forces and beyond,
- the degree of combat readiness, including in the context of the availability of ready-to-use nuclear warheads directly on carriers.

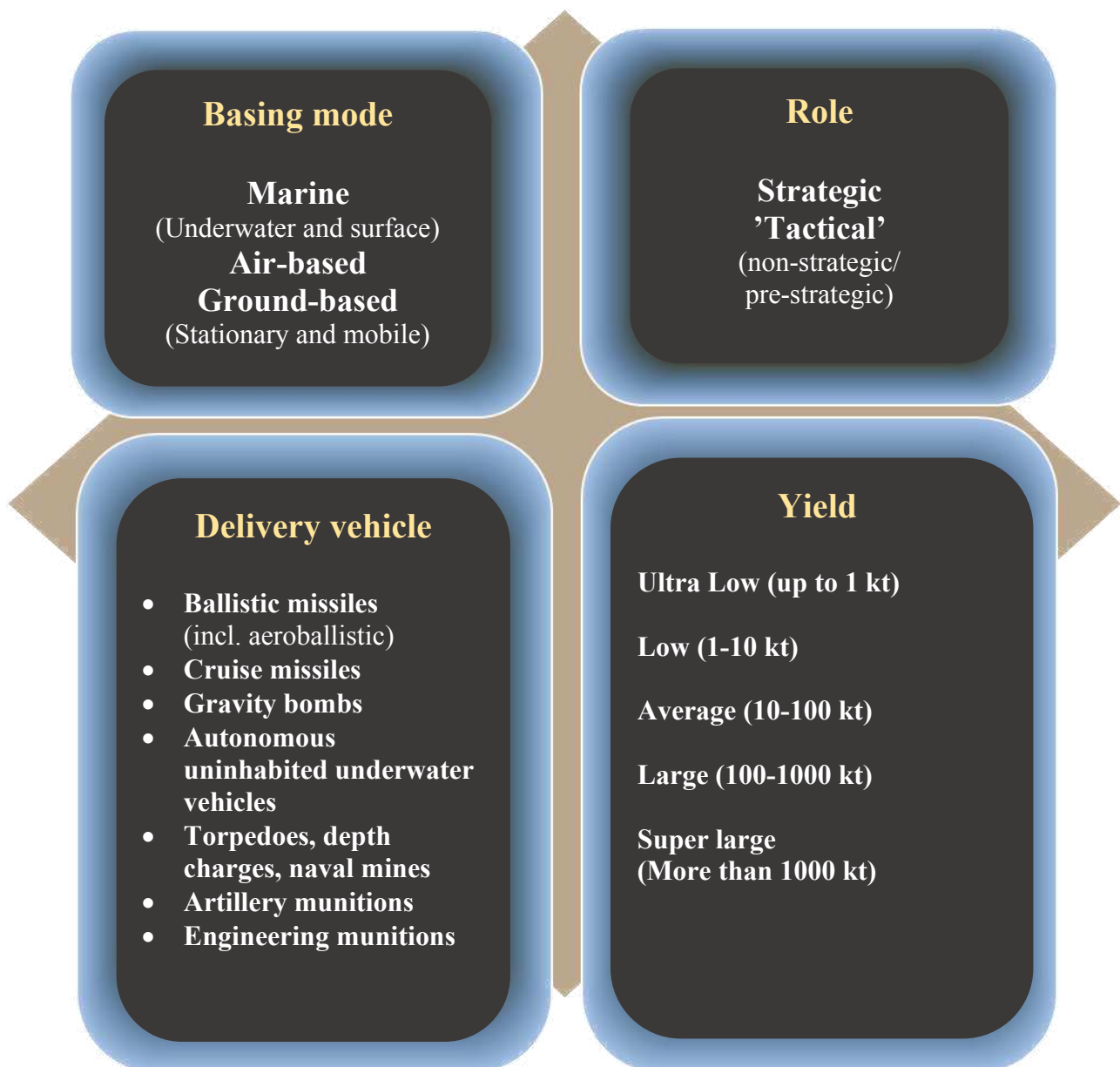
An attempt to directly divide nuclear forces into several conditional subgroups is presented in Figure 4.6.

Interference can affect both control circuits at the unit level, as well as launchers themselves, sea carriers of missile weapons (including submarines) and aircraft of tactical and strategic aviation, as well as munitions and warheads themselves. Of course, we can hardly speak here about “attack of the first type” according to the classification presented in the first part of this section, that is, through malware introduced through an external network infrastructure using public networks or through covert connections to closed networks. Unless in some particular subdivision, in violation of all possible instructions and regulations, internal

automated workstations and control systems will be allowed to interface with external networks (which, however, cannot be ruled out).

However, an undercover spoofing of data carriers (“type two attack”) is quite possible. This threat is real for all types of nuclear forces, although submarines, air-missile carriers, and mobile surface-to-air missile systems on combat patrol are less susceptible to it.

Figure 4.6. Classification of nuclear forces



Source: Encyclopedia of the Strategic Rocket Forces // Official website of the Ministry of Defense of the Russian Federation. URL: <http://encyclopedia.mil.ru/encyclopedia/dictionary/listrvsn.htm>.

It is the carriers that have left their basing sites and, accordingly, the multilayered defense against all types of influence from the enemy that become a real target for an “attack of the third type” using EW. Modern EW facilities can also have a directed impact on enemy information and communication systems by generating targeted jamming. In this case the main threat is disruption of communication channels as well as distortion of information necessary for targeting. Considering the high level of technological sophistication of modern nuclear weapon delivery vehicles, one cannot rule out that the effect of using radio-electronic interference can also prevent the launching of various missile weapons directly by means of radio-electronic disruption of weapon control systems and facilities, as well as destruction, erasure or distortion of software and information in the ACS⁹⁴. Obviously, tactical nuclear weapons carriers, regardless of their type of basing, can be subjected to significant radio-electronic interference at the stage of entering their positioning areas and at the missile launching sites.

The problem of “bugs” in both hardware and software is clear and understood by all the services involved⁹⁵, which is reflected in very strict approaches to the licensing of relevant products used in the production and deployment of various systems of weapons and military equipment. At the same time, no one is immune to mistakes, and here imports substitution in the truest and harshest sense of the word becomes an extremely important task. There is no reliable information about the number of foreign components in various nuclear weapon carriers and delivery vehicles, but it can be assumed that the more mass-produced a product (especially in the case of non-nuclear and export versions), the more likely a “Type 4 attack” is, due to the increased opportunities for a possible enemy to obtain information about the architecture of various weapons systems.

Irony on the part of the media and individual experts over the low-tech media used in the field of strategic nuclear forces⁹⁶ has become widespread. At the same time, perhaps this approach is one of the most effective ways to protect critical military infrastructure from cyber-attacks. At the same time, to reduce the cyber threat, it is advisable to use only national equipment and software that is as incompatible as possible with international standards.

⁹⁴ Evolution of Electronic Warfare // Official Website of Rostec State Corporation. URL: <https://rostec.ru/analytics/evolyutsiya-radioelektronnoy-borby/>.

⁹⁵ GOST R ISO/MECH 27001-2006. Information Technology. Methods and Means to Ensure Security. Information Security Management Systems Requirements; GOST R ISO/IEC 15408-1-2002 Information Technology (IT). Methods and Means to Ensure Security. Information Technology Security Assessment Criteria.

⁹⁶ The Pentagon's Huge Atomic Floppies // Time. 2016. May 25, 2016. URL:

<https://time.com/4348494/pentagon-nuclear-floppy-disks/>. The US Department of Defense Uses Old Floppy Disks // TK Zvezda. 2016. May 27. URL:

https://tvzvezda.ru/news/vstrane_i_mire/content/201605270448-hoer.htm.

4.2.4. The artificial intelligence factor

All the above threats are further amplified by the development of AI technologies, machine learning, and the autonomous operation capabilities of various systems and subsystems.

Artificial Intelligence (AI) – a set of technological solutions that allows to simulate the cognitive functions of a person (including self-learning and search for solutions without a predetermined algorithm) and obtain results when performing specific tasks that are comparable, at least, to the results of human intellectual activity. The set of technological solutions includes information and communication infrastructure, software (including that which uses machine learning methods), processes and services for data processing and solution search; AI technologies – technologies based on the use of AI, including computer vision, natural language processing, speech recognition and synthesis, intelligent decision support and promising AI methods⁹⁷.

Machine Learning (ML) is a branch of the theory of AI, the subject of which is the search for methods of solving problems by learning in the process of solving similar problems. To build such methods the means of algebra, mathematical statistics, discrete mathematics, optimization theory, numerical methods, and other branches of mathematics are used⁹⁸.

The MWS is a critical area for autonomous analysis and decision making. The main tasks for AI technologies in this case are threat assessment and damage prediction, which can help develop correct response scenarios based on the scale of the attack, its source, and possible intentions. Machine learning and related technologies will serve as decision support as we move into a response, particularly in organizing maneuvering to draw forces and assets out from under enemy strikes, optimizing planning for a retaliatory strike. Merging data from different sources and updating information in real time improves the quality of combat management and situational awareness⁹⁹. However, it is for this reason that the use of cyber weapons represents a significant threat: In fact, the risks outlined in this chapter are multiplied.

In addition, there is a threat of an absolute substitution of “human” analysis of the operational situation due to the formation of assessments and decisions of military personnel solely based on the proposals of the automated system. In fact, a human being is present in the procedure for assessing the situation, making decisions, and using weapons, but all his decisions are made under the powerful influence of “machine” data. In such a situation it is possible to increase the negative

⁹⁷ National Strategy for the Development of Artificial Intelligence for the Period until 2030, Approved by Presidential Decree No. 490 of October 10, 2019.

⁹⁸ Mironov, A.M. Machine Learning, Part 1. URL: http://www.intsys.msu.ru/staff/mironov/machine_learning_vol1.pdf.

⁹⁹ Handbook of Multisensory Data Fusion: Theory and Practice / Edited by M. Liggins, D. Hall, J. Llinas (2nd ed.). Taylor & Francis, 2009.

consequences of a hostile external influence on the information systems that provide input data to automated decision-support tools, as well as the systems that directly carry out the preparation of these decisions.

An effective use of machine learning, machine vision, and similar technologies for airborne subsystems of nuclear weapons delivery systems now seems to be primarily associated with targeting missions. With the help of automated image processing and analysis it is possible to recognize types of targets quickly and effectively, clarify their location, the presence of vulnerabilities – and ultimately to optimize the number of warheads used¹⁰⁰. AI in command-and-control systems of munitions would provide high accuracy and maneuverability unpredictable for defensive systems. For example, hypersonic gliding cruise missiles have understandable difficulties with external control during flight due to speeds and plasma cloud formation – resulting in the need for effective on-board solutions. Overcoming missile defense can also be more effective with the use of smart decoys and random changes in flight trajectory. That said, the race in sophistication between the defending and offensive sides will be endless, and cyber, EW, or other non-kinetic intercept methods by deceiving the smart warhead are also likely to be developed. Recall that the first battle of EW tools in the area directly related to nuclear weapons took place back at the dawn of the “atomic era” in the late 1940s. One of the methods of protection against nuclear strikes was the creation of ground-based generators of radar clutter, whose radiation could “deceive” the radar altimeter of the nuclear bomb and lead to untimely or incorrect triggering of the initiation mechanism¹⁰¹. It is very likely that this battle of the electronic “sword” and “shield” continues.

Full autonomy is also a breakthrough technology for combat operations in the ocean depths. For example, an ocean multipurpose system can be used as a means of delivery of nuclear warheads, according to some sources, of super-large, megaton class, which at the same time creates a threat of catastrophic consequences of such a system getting out of control due to hostile cyber interference¹⁰². Another threat (underwater as well as in other environments) is the unintended collision of several autonomous systems of various likely adversaries. How “nuclear robots” would behave in such a situation is difficult to predict, but in the case of aggressive interaction, there could probably be attempts to attack using ICT. Thus, it is possible to impose sets of deliberately distorted data (“type-5 attack”) on both an advanced early-warning system that uses automatic analysis of information from various sources and an intelligent logistics management decision-support system. Such an action could lead in the first case to an incorrect assessment of the situation and, consequently, to an incorrect response. In the second case such an attack could result

¹⁰⁰ The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risks / Ed. by V. Bulanin. SIPRI, 2019. C. 94-95.

¹⁰¹ Keeney L. 15 Minutes: General Curtis LeMay and the Countdown to Nuclear Annihilation. – New York, 2011. C. 46.

¹⁰² The Poseidon Submersible Will Be Able to Carry a Warhead with a Capacity of Up to Two Megatons // TASS. 2018. May 17. URL: <https://tass.ru/armiya-i-opk/5208267>.

in the disabling of weapons and military equipment and the corresponding destruction of nuclear capabilities. A fully automated nuclear retaliatory strike process is technologically feasible, and in the event of a rapid degradation of strategic stability, the decision to pre-delegate authority to autonomous subsystems may well be taken – but in such a situation, the entire spectrum of ICT threats poses completely apocalyptic risks.

At the same time, the key threat to both automated retaliation and individual autonomous nuclear weapons carriers appears to be the introduction of deliberately false information into the data processing systems (“type 5 attack”), leading to the incorrect functioning of the corresponding analytical subsystems.

4.2.5. Fundamentals of Russia's Nuclear Deterrence Policy and cyber-nuclear communications

June 2020 saw the public release of the Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence¹⁰³ – for the first time ever. Its main importance is in the broadening of nuclear-related sections of the ‘general’ Military Doctrine of the Russian Federation. It is a specific type of strategic planning document, regularly prepared and updated for different areas, including civilian, and is used as a basis for development and acquisitions planning, the legislative process and other bureaucratic work.

It is important to take note of the conditions set out in the Basic Principles document that might lead to nuclear use by Russia. In general, the list of conditions follows the traditional Russian approach: nuclear weapons prevent the use of Weapons of Mass Destruction and/or large-scale aggression against Russia and/or its allies. However, there is an important update. Now threats to the nuclear weapons themselves are considered a condition for nuclear retaliation.

Paragraph 19c of the Basic Principles states: “attack by an adversary against critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces response actions”. This effectively means any interference of any kind against civilian or military infrastructure, which would undermine nuclear retaliation capability. There is a wide consensus within the Russian expert community that this also includes possible cyber threats as well as other non-nuclear dangers. It is commonly understood that “critical sites” include military and civilian government command posts, nuclear forces battle management system, nuclear forces infrastructure and EWSs. Malicious interference with these sites could lead to catastrophic consequences.

¹⁰³ Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence. URL: https://www.mid.ru/ru/foreign_policy/international_safety/disarmament/1434131/?lang=en.

In general, the threat of cyber-attack against Nuclear Command, Control and Communications (NC3) have been discussed at length¹⁰⁴ over last several years with all the five nuclear weapon states seemingly factoring this threat into their deterrence policies. In the United States, a formulation is included in the 2018 US Nuclear Posture Review: “*Significant non-nuclear strategic attacks include, but are not limited to, attacks on the USA, allied, or partner civilian population or infrastructure, and attacks on US or allied nuclear forces, their command and control, or warning and attack assessment capabilities*”¹⁰⁵.

It is challenging to find links between cyber threats and nuclear use in public Chinese documents, especially given the No First Use policy declared and maintained by Beijing. Nevertheless, there are statements¹⁰⁶ comparing consequences of cyber-attacks to those of nuclear bombs. Research of the entanglement between non-nuclear and nuclear weapons related systems suggests that there is a serious cyber ‘flavour’ in such risks, and China must be looking for ways to address those¹⁰⁷.

French “vital interests”¹⁰⁸ that are protected by nuclear weapons are intentionally ambiguous, but Paris pays great attention to the cyber domain. The link between cyber and nuclear threats is mentioned among the principles of the Paris Call for Trust and Security in Cyberspace¹⁰⁹.

While in the UK the possible cyber threat to NC3 and nuclear weapons systems themselves is acknowledged by officials¹¹⁰, nothing suggests that such attacks might be considered among “the most extreme threats” to be deterred by nuclear weapons¹¹¹. However, London, without any doubt, will be interested in reducing the risks of nuclear use because of cyber interference.

¹⁰⁴ URL: <https://www.nti.org/about/programs-projects/project/addressing-cyber-nuclear-security-threats/>.

¹⁰⁵ Nuclear Posture Review. February 2018. Office of the Secretary of Defense. URL: <https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF>.

¹⁰⁶ Andrew Browne. China: Cyber-attacks Are Like Nuclear Bombs. The Wall Street Journal. April 22, 2013. URL: <https://www.wsj.com/articles/SB10001424127887323551004578438842382520654>.

¹⁰⁷ James M. Acton, Tong Zhao, Li Bin. Reducing the Risks of Nuclear Entanglement. September 12, 2018. Carnegie Endowment for International Peace. URL: <https://carnegieendowment.org/2018/09/12/reducing-risks-of-nuclear-entanglement-pub-77236>.

¹⁰⁸ Speech of the President of the Republic on the Defense and Deterrence Strategy. 7 February 2020. URL: <https://www.elysee.fr/en/emmanuel-macron/2020/02/07/speech-of-the-president-of-the-republic-on-the-defense-and-deterrence-strategy>.

¹⁰⁹ The 9 principles. Paris Call For trust and security in cyberspace. URL: <https://pariscall.international/en/principles>.

¹¹⁰ House of Lords Select Committee on International Relations Rising nuclear risk, disarmament, and the Nuclear Non-Proliferation Treaty. Government Response. Parliament UK. URL: <https://www.parliament.uk/globalassets/documents/lords-committees/International-Relations-Committee/NPT-and-Nuclear-Disarmament/Government-Response-Rising-nuclear-risk-disarmament-and-the-Nuclear-Non-Proliferation-Report.pdf>.

¹¹¹ Guidance The UK's nuclear deterrent: what you need to know. 17 February 2022. Gov.UK. URL: <https://www.gov.uk/government/publications/uk-nuclear-deterrence-factsheet/uk-nuclear-deterrence-what-you-need-to-know>.

Decision-makers and military must now account for the use of cyber weapons, hostilities in cyberspace, and the desire of state and non-state actors to gain an advantage by damaging nuclear weapons and the delivery systems of their adversaries. The vulnerability of nuclear weapons control systems is ‘enhanced’ by the high readiness of the nuclear forces. Theoretically, a crushing ‘decapitating’ and even ‘disarming’ strike could be delivered using cyber weapons. At the same time, awareness of the risk of a cyber-attack incentivizes the need to increase the protection of nuclear forces-related networks from acts of unlawful interference, regardless of their source, which contributes to maintaining security.

Understanding the threats, and the challenge by China, France and the UK provides an opening for potential joint actions, including within the P5 format: a forum of these five countries, recognized as nuclear-weapon states within the Nuclear Nonproliferation Treaty. One such action could be a statement of mutual understanding of the consequences of the interference with NC3 and aspiration to avoid actions that might be perceived as such interference by adversaries and partners.

There is a significant challenge with dealing with risks in the cyber domain, namely the attribution of the ‘perpetrator’. This is complicated by the fact that near-identical cyber tools can be used for espionage (collecting information) as well as for attacking the systems they have penetrated. A discussion on procedures for attack attribution and cyber weapon ‘dissection’ within the P5 might offer a platform for practical cooperation. Still, the main challenge is traditional: political will, or rather absence of such to participate in such discussions. ‘Cyber’ has become a toxic subject in relations between Russia, China and ‘the West’ due to mutual accusations and counteraccusations over election meddling, espionage and other ‘grey area’ actions. It will be naïve to expect a swift breakthrough. Nevertheless, cyberspace is officially becoming an operational domain for the military. Counterintuitively, it paves a way towards confidence building and risk reduction measures akin to ‘classic’ military domains. The nuclear domain is where such measures are of existential importance, so P5 countries should be ready for selective engagement.

The P5 format provides the best possible forum for inclusive discussions on nuclear doctrines and threat perceptions. Given the growing common understanding of the nexus between cyber and nuclear risks, the P5 countries can come up with a set of basic principles that deter nuclear use. The major principle should be to avoid making statements and building or acquiring weapons that might be seen as a push towards obtaining the very capability their P5 partners and adversaries are concerned with to undermine nuclear retaliation capacity. Such principle could be augmented with another one: a requirement to explain intended missions for the capabilities that are perceived as threatening, should any P5 country express such concerns. Addressing the cyber-nuclear nexus therefore offers an unexpected opening for P5

collaboration and preserving the stability of deterrence between the nuclear weapon states.

4.3. The Problem of Attribution of Computer Attacks in the Process of Ensuring Strategic Stability

An important aspect of attribution is the growing inequality of countries in cyberspace due to different financial capabilities, level of access to the Internet, development of breakthrough technologies in data storage and processing, etc. Furthermore, the US policy striving for achieving and consolidating dominance in cyberspace, rather than reducing such disparities, makes it much more difficult to solve the problem. Also, some United States officials claim that for the US, as the world leader in ICT, the problem of attribution of cyber-attacks is solved¹¹². However, its results are not accepted by the Russian Federation and many other countries. For example, the press secretary of the Russian president, D.S. Peskov¹¹³ and Secretary of the Security Council of the Russian Federation N.P. Patrushev¹¹⁴ have repeatedly referred to the lack of evidence in accusing Russia of conducting destructive cyber-attacks. It should be noted that the consequences of such accusations have a negative impact on bilateral relations between Russia and the United States, as well as on international political processes, on the level of strategic stability and global security.

Thus, the problem of attribution of cyber-attacks, analysis of current trends in this area are most pressing today. In addition, the issues under study correlate with the latest doctrinal documents of Russia, which entered into force in 2021: the National Security Strategy of the Russian Federation¹¹⁵ and the Fundamentals of State Policy of the Russian Federation in International Information Security¹¹⁶.

4.3.1. Conceptual framework and problems of attribution of cyber-attacks

The annual increase in computer attacks has become truly global. For example, according to the German web portal sicherheitstacho.eu, the number of identified attacks per day is already about 40 million, and the financial losses in the world next year are estimated at \$8 trillion (which exceeds the losses from the pandemic in two years)¹¹⁷. One of the most famous examples of cyber-attacks that caused significant national damage is the Olympic Games cyber operation (also known by its malicious

¹¹² Leon Panetta. *Defending the Nation from Cyber-Attack*, Business Executives for National Security, New York City, October 11, 2012.

¹¹³ Kommersant No. 230 dd.15.12.2020, p. 6.

¹¹⁴ Kommersant No.61 dd. 08.04.2021, p. 1.

¹¹⁵ National Security Strategy of the Russian Federation (Approved by Presidential Decree No. 400 dd. 2 July 2021.). URL: <http://www.kremlin.ru/acts/bank/47046>.

¹¹⁶ Fundamentals of State Policy of the Russian Federation in international information security (approved by Presidential Decree No. 213 dd. 12 April 2021 URL: <http://www.kremlin.ru/acts/bank/46614>).

¹¹⁷ See, for example, OECD: *Damage to the World Economy*. TASS. 17.09.2020. URL: <https://tass.ru/ekonomika/9478165>.

component Stuxnet) in 2010, which suspended Iran's state nuclear program and is attributed to US and Israeli cyber groups. These and other facts of damage from external computer attacks prove the relevance of the conceptual framework of attribution.

The concept of attribution (Latin *attributio* – attribution, establishment) has long been applicable as a subject of copyright to determine the reliability of a source, for example, in the field of art and journalism. The term has also long been used in social psychology to ascribe characteristics to social objects based on observations. However, in the field of cybersecurity, the term is still at the stage of formation; it does not yet exist in the information security standards of GOST, IEC, ISO, ITU or NIST, etc.

In various sources, the concept of cyber-attribution (cyber-attack attribution, cyber attribution) is usually reduced to a *set of procedures for identifying the source of an attack for attributing responsibility*. Forensic experts often operate with technical aspects of attribution, abstracting from politics, while international legal institutions operate with accusatory ones. Therefore, the attribution is divided into two components:

- technical (forensic), which has a function of definition,
- legal has a prescriptive function.

It is the junction of the two directions that gives rise to the point of bifurcation in the accuracy and reliability of the intermediate conclusions, and to potential variability of the conclusion (Table 4.2). However, in any case, attribution is associated with a high level of subjectivity and uncertainty, that is, it is a risk-oriented space.

Table 4.2. Comparison of components of cyber-attack attribution

Type of attribution	Function of attribution	Document	Reliability of attribution	Methods of attribution	Indicators, criteria of attribution
<i>Technical</i>	Definitions (detective)	Political certificate	High	Monitoring, control of resources and processes	Quantitative, qualitative Qualitative
<i>Legal</i>	Prescriptive	Technical report	Low	Compliance, analysis of motivation	Qualitative

Source: Table constructed by the author.

An important classification feature of attribution is the publicity factor. For example, attribution can be open, hidden (intra-state) or partially hidden (bilateral), etc. In some cases, attribution may not include the legal side at all, that is, it may be limited to protecting information resources from cyber-attacks.

On the other hand, the absence of a technical component of attribution leads to groundless claims. For example, the accusation of Russia of cyber-attacks on the IT infrastructure of the Austrian Ministry of Foreign Affairs, which was later dismissed¹¹⁸ or Moscow's accusations of cyber-attacks affecting the US elections, which were also followed by an official admission of a lack of evidence¹¹⁹. However, numerous statements about Russia's guilt have led to a sharp deterioration in relations between Russia and the West, and the sanctions imposed “for Russia’s interference with the elections” are causing really financial and reputational damage to the country.

The important aspects of the attribution problem are the objective reasons for the need to address it for security purposes, as well as the complexity of identification and authentication.

Regarding the first aspect, the issue of attribution has now become the most important geopolitical factor. Failure to solve this problem generates increasing threats to the national security of the country large-scale theft of intellectual property, incidents with critical and military items, financial losses, negative impact on public opinion, reputational damage to the state, etc. The countries that have a toolkit of attribution, more accurately assess international processes, and have a geopolitical advantage. Moreover, the development of methods to identify the source of computer attacks becomes a condition for the successful development of the ICT industry, because in technical terms it is an integral part of information security management, and more specifically Threat Intelligence, also has legal and financial significance for business processes.

The complexity of intrusion source identification and authentication is discussed in various sources, where the authors describe the problem at basic levels of systematisation: 1) political, 2) legal, 3) organizational, and 4) technical.

1. According to the authors, the political level is decisive in international relations, as many organizational and technical issues can be solved to some extent depending on the “goodwill” of states. This level marks the first, according to A.V. Krutskikh, special representative of the President of Russia on international

¹¹⁸ See State actor' hack on government IT systems is over. Theregister.com. 14.02.2020. URL: https://www.theregister.com/2020/02/14/austria_foreign_ministry_hack_turla_group_allegs.

¹¹⁹ US DoJ Press Release 21-229. 9.08.2021. URL: <https://www.justice.gov/opa/pr/joint-statement-departments-justice-and-homeland-security-assessing-impact-foreign>.

cooperation in information security – triumphant¹²⁰ progress: this year, the United Nations managed to agree on declaratory rules for responsible behaviour of countries in ICT. However, many political issues still require joint work on international platforms. In particular, the Russian Foreign Ministry notes a lack of dialogue on the increasing number of violations of the rights of Russian citizens traveling abroad, especially programmers. At the same time, as Russian President V. Putin has stated, 80 inquiries to US authorities regarding computer attacks have gone unanswered. A similar situation is with attempts to cooperate with the EU on cybersecurity issues and combating disinformation¹²¹. Unfortunately, Russia has recently been confronted with a number of similar facts even at the level of summits¹²² and meetings¹²³. Thus, the general trend is of objective concern.

2. International law is the second most important barrier to identifying the source of cyber-attacks, as two important issues are not solved: legal assessment of military aggressor in cyberspace (according to Clausewitz – physical violence towards people, which is not peculiar to cyberspace) and boundaries of cyberspace (the opportunity of their demarcation and delimitation, accordingly). This makes it difficult to assess deterrent, defensive or offensive countermeasures. The situation may be complicated by claiming that the indicted state is in cooperation with the accusing state, and, consequently, the growing distrust between countries.

Let us highlight the typical problematic situations of political attribution due to the lack of regulations:

- the indicted state denies involvement in the computer attack,
- the indicted state denies any connection with the identified attackers operating in its territory,
- the indicted state denies being able to influence attacks transiting and emanating from its territory,
- the accusing state finds it difficult to justify the target of the response (individuals, organization, state) in cyberspace,
- the accusing state finds it difficult to justify the area (political, economic, or military measures) and level of response (protection, deterrence, offensive actions) in cyberspace,
- the accusing state finds it difficult to justify the kinetic military action in response to unfriendly actions in cyberspace.

¹²⁰ See, for example UN Countries Advocate for Continued Work. TASS. 13.03.2021. URL: <https://tass.ru/politika/10895625>.

¹²¹ See, for example, Brussels avoids dialogue with Moscow. TASS. 28.10.2021. URL: <https://tass.ru/politika/12794331>.

¹²² See, for example, Refusal to invite the Russian Federation to the cybersecurity summit. TASS. 13.10.2021 URL: <https://tass.ru/politika/12653233>.

¹²³ See, for example, Virtual Counter-Ransomware Initiative Meeting. Whitehouse.gov. 13.10.2021. URL: <https://www.whitehouse.gov/briefing-room/press-briefings/2021/10/13/background-press-call-on-the-virtual-counter-ransomware-initiative-meeting/>.

Regarding the latter situation, various sources justify different positions, from extremely aggressive (“attack as a right to war”), to moderate (when evidence equating a cyber-attack to armed attack). At the same time, there are known instances where kinetic weapons¹²⁴ have been used against the source of cyber-attacks. Besides, the EU has established sanctions for cyber-attacks¹²⁵, and top US policy makers have repeatedly stated that the US may resort to a military operation in response to particularly dangerous cyber-attacks.

3. Organizational and technical problems of attribution have a blockchain nature because there are no international standards for mutual monitoring and control of actions and de-anonymization on the Internet. However, these issues have a solution within individual countries and political alliances. Often the interaction is beyond the identification of targeted computer attacks and is limited to the exchange of information, for example, at Interpol, on the financial fraud of individual criminal elements.

4. Technical barrier to attribution is the most difficult to address, which is caused by the intrinsic properties of the Internet: initially decentralized segmented network architecture; IPv4 addressing limitations; wide range of software applications and anonymization services, including communication rental services; black market of malicious resources and services; support of insecure protocols (which can be used to change address). The authors emphasize the critical structural complexity of software systems, objectively resulting in vulnerabilities related to registration of actions and authentication control, including those that allow cryptographic certificates to be compromised. The abovementioned network and software complexities are under the scrutiny of many scientists and computer system developers, so it is reasonable to assume that technological problems that once seemed unsolvable will be successfully solved.

Overcoming these barriers is in general a subjective factor: employee errors, unprofessionalism, and characteristics of the socio-technical style of programmers and operators of cyber-attacks, which are amplified in crisis situations (for example, in the environment of deceptive systems). And this again emphasizes the need for global community to cooperate closer.

The following methods are used to make it more difficult to identify the source of a cyber-attack:

- masking the cyber-attack and activities of the cyber group (OPSEC),
- redirecting the investigation on false evidence to a third party, called a False Flag attack, which is characterized by specific patterns. At the same time, in some cases, the subject of attack may not control the tracking

¹²⁴ Official Israel Defense Forces Twitter. 5.05.2019. URL: <https://twitter.com/IDF/status/1125066395010699264>.

¹²⁵ EU Council Decisions (CFSP) 2019/797 and 2019/796 of 17 May 2019.

(trace registration) of its activity, so often such attacks can have the opposite effect.

4.3.2. Key actors of cyber-attack attribution

The issue of attribution is in the focus of government agencies, private companies in the information security (IS) and computer forensics industries, as well as academic communities and associations. Note that the most effective attribution can be achieved through close interaction between public services and private IS companies. For example, public services, unlike commercial companies, have limited access to specific technical data (e.g., debugging data of developers) and often rely on narrowly focused experts for their investigations. At the same time, private firms tend to have other incentives (profit, self-marketing, moral incentives), not so much political ones. On the other hand, public companies can use additional legal mechanisms (for example, to summon a particular person to court or put out a search for them) and the technical resources of the country and allied states and partners. Some countries have developed national systems to detect and prevent computer attacks (e.g., GosSOPKA in Russia and Einstein 3 in the United States), as well as state and industry incident response centers.

Western countries actively pursue bloc politics, as evidenced by some of ICT incident information sharing initiatives, such as the Cybersecurity Information Sharing Act in the United States, the ENISA Cybersecurity Information Sharing Act, and the NATO Cybersecurity Information Sharing Act. Currently, about 30 private IS firms, most of which are in the United States, publish attribution reports (Table 4.3). Analysis of the attribution reports shows that 99% of them are published in 10 countries, and 90% by US organizations. Among the academic schools dealing with cyber-attack attribution are universities in the United States and NATO countries, such as the Stanford University initiative, integrated with private partner First Draft¹²⁶. Not surprisingly that on the association's web portal, two-thirds of the attribution reports focus on blaming Russia, and the rest on blaming China. A similar situation is seen in other attribution reports (Table 4.4, Figure 4.7).

¹²⁶ About attribution. news. URL: <https://attribution.news/about/>.

Table 4.3. Attribution report sources

Organization	Country	Organization type	Website example
<i>Cisco (Talos)</i>	USA	Public company	https://blog.talosintelligence.com/2018/02/group-123-goes-wild.html
<i>CrowdStrike Holdings</i>	USA	Public company	www.crowdstrike.com/blog/meet-the-adversaries/
<i>FireEye (Mandiant)</i>	USA	Public company	www.fireeye.com/current-threats/apt-groups.html
<i>MITRE</i>	USA	Public company	https://attack.mitre.org/groups/G0006/
<i>NSA</i>	USA	Federal service	www.nsa.gov/What-We-Do/Cybersecurity/Advisories-Technical-Guidance/
<i>Palo Alto Networks</i>	USA	Public company	https://www.paloaltonetworks.com/unit42/threat-intelligence
<i>SecureWorks (Dell)</i>	USA	Public company	www.secureworks.com/research/threat-profiles
<i>Kaspersky Lab</i>	Russia and others	Public company	www.securelist.com/all/?category=908

Source: Table constructed by the author.

Table 4.4. Countries mentioned in foreign attribution reports

Organization that published a report	Accused countries
<i>Attribution News</i> ¹²⁷	China, Russia
<i>CrowdStrike</i> ¹²⁸	China, Russia, Iran, North Korea, India, Pakistan, Vietnam, South Korea
<i>Microsoft</i> ¹²⁹	China, Russia, Iran, North Korea, Vietnam, Turkey
<i>MITRE</i> ¹³⁰	China, Russia, Iran, North Korea, Lebanon, Pakistan, Vietnam, India, Nigeria, UAE and clearly not identified
<i>NATO</i> ¹³¹	75% – China, Russia, Iran, North Korea

Source: Table constructed by the author.

¹²⁷ The attribution. news project. URL: <https://attribution.news/studies/>.

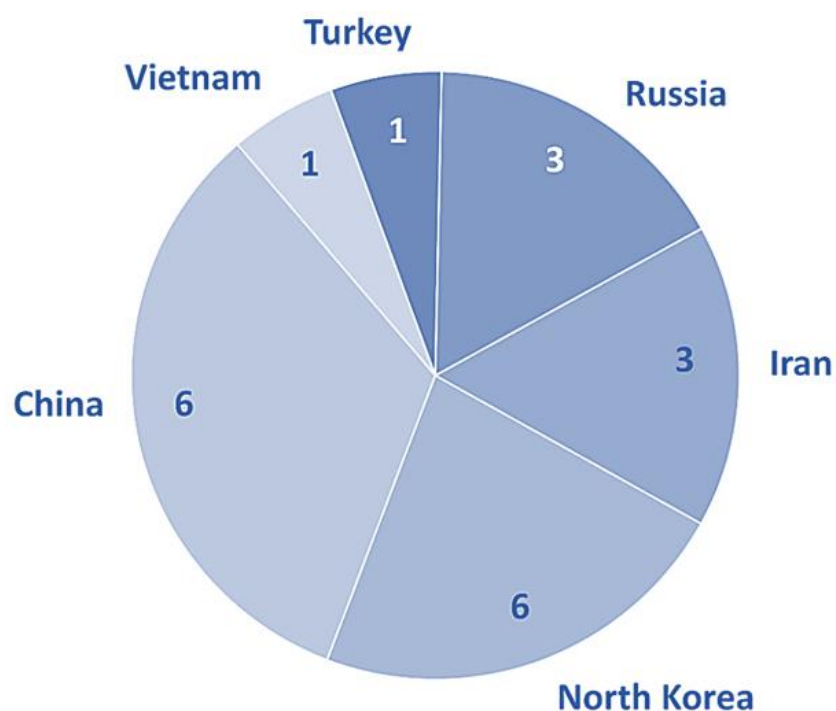
¹²⁸ CrowdStrike 2021 Global Threat Report. URL: <https://www.crowdstrike.com/global-threat-report/>.

¹²⁹ Microsoft Digital Defense Report (October 2021). URL: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFii>.

¹³⁰ MITRE ATT&CK v. 10. URL: <https://attack.mitre.org/groups/>.

¹³¹ NATO CCDCOE, Tallinn Paper No.12. 2021 URL: https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf.

Figure 4.7. Countries mentioned in Microsoft's 2021 report



Source: Microsoft Digital Defense Report (October 2021).

Public national research programs have focused on cyber attribution issues:

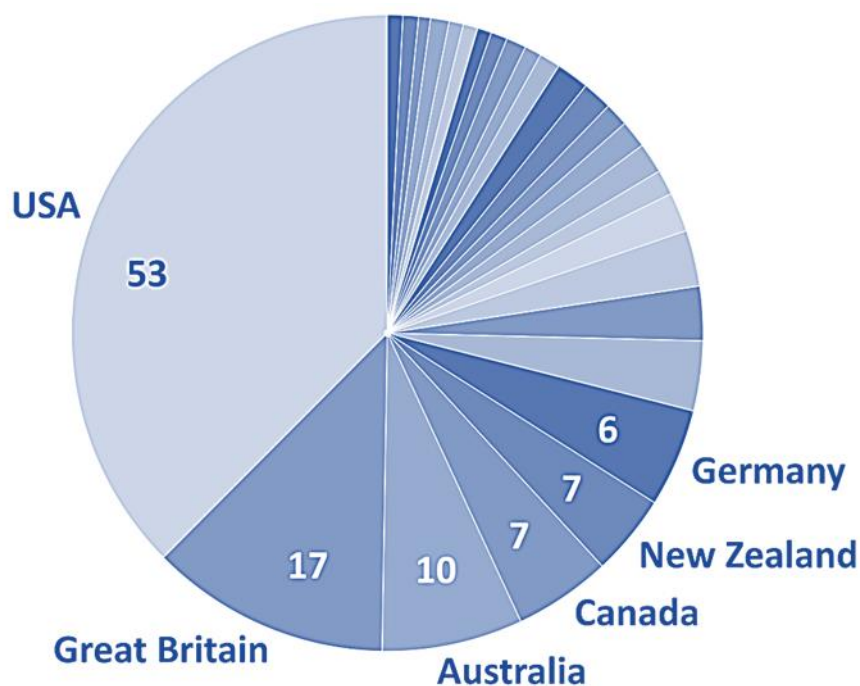
- DARPA-Enhanced Attribution¹³², a US Department of Defense research project to develop technologies for continuous global monitoring and heterogeneous data collection, multilevel analysis, and sharing of heterogeneous data on multiple offensive cyber operations,
- The EU-funded WOMBAT research project (Worldwide Observatory of Malicious Behaviors and Attack Threats)¹³³ to create network traps to collect and analyze data on the network architecture of cyber operation, various financial and address information to attribute the perpetrators of a cyber-attack,
- information project of the US non-governmental organization MITRE – ATT&CK (Adversarial Tactics, Techniques & Common Knowledge), which allows for forming a profile of cyber groups on methods and means of cyber-attacks (after the attack).

Thus, the problem of attribution of cyber-attacks at the present stage is extremely politicized and reflects mainly the interests of the United States, its allies, and partners. It is noteworthy that this conclusion is also made in the NATO Tallinn publication on cybersecurity (Figure 2).

¹³² DARPA Enhanced Attribution Program. URL: <https://www.darpa.mil/program/enhanced-attribution>.

¹³³ The WOMBAT Project. URL: <http://www.wombat-project.eu/>.

Figure 4.8. Countries engaged in cyber-attack attribution



Source: Tallinn Paper No. 12. 2021.

4.3.3. The object and subject of cyber-attack attribution

It can be argued that the problem of attribution of cyber-attacks has already become a field of science. In this case, the object of the problem, as a rule, are targeted computer attacks that serve the interests of a particular country. They are often called APT attacks (APT – Advanced Persistent Threat). Typically, there are several characteristics of APT attacks, such as selectivity of target, multiplicity (iteration), the ability to penetrate neighboring network segments, the use of zero-day vulnerabilities, stealth, infrastructure support, broad functionality, scalability, high quality code. In fact, such attacks are part of offensive cyber operations that can covertly last for a long time. Experts believe that APT attacks have governmental support, are ordered, and financed by specific countries.

Currently, the most popular scheme for describing an APT attack is the Cyber Kill Chain, developed by Lockheed Martin, which treats an APT attack as a military operation comprising seven stages: reconnaissance and planning, creation of cyber weapons, delivery, operation, horizontal development, creation of control, execution of targeting.

Defining an APT attack is important for identification by the relevant attributes that will eventually become evidence and proof and can be related to the structural characteristics of a cyber-attack (e.g., programming style or botnet features),

functional (e.g., typical hacking, control, and cloaking techniques), and informational (e.g., statements, political and economic motivations).

The largest classification to date – profiles of 130 APT cyber groups – was presented by a non-government American company MITRE.

The profiles described do not include information about ART groups funded by the United States, its allies, and partners (see Table 4.5).

2. The *subject of the cyber-attack attribution problem* is methodological support, which includes two classes of methods:

- methods that describe the attribution process for justifying a verdict,
- methods that assess the significance of cyber-attack attributes to identify a source.

Analysis of methodological support is important to assess the involvement of countries in the development of attribution methodology, as well as the degree of publicity of research results.

Methods describing the attribution process are used to implement a structured hypothetical analysis of information (mainly a variation of the brainstorming, survey or logical analysis method¹³⁴) to make diplomatic decisions.

There are two directions in conceptual modeling of attribution.

The first includes models reflecting the logic of experts asking questions and making hypotheses, forming answers, or choosing the most significant ones. The main tasks of modeling are collection, analysis of data in order to obtain evidence; making decisions on imposing responsibility on the intruder; communication (publication of the verdict and plausible evidence); post responses.

These models include Q-model, diamond model, CAM-model, etc. The most popular is the Q-model of structured analysis. This is a descriptive and informal model based on the analytic “brain” cycle (hypothesis-discussion-action). The following assumptions are made:

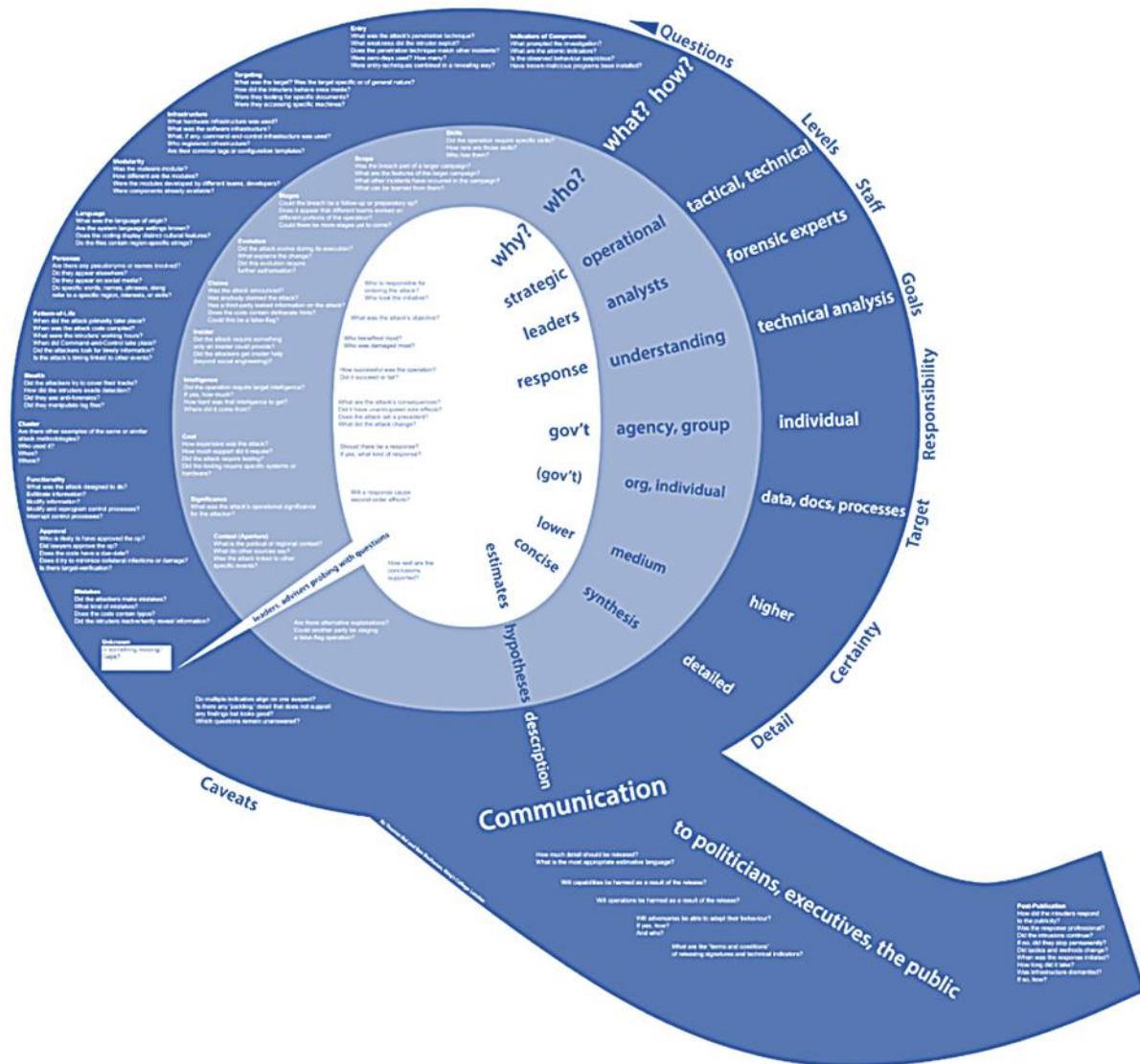
- attribution is complex (non-linear) and partially iterative,
- attribution is made at three interrelated levels: tactical (how the attack occurred technically), operational (how the attack is organized), and strategic (what might the motives be),
- attribution ends with the communication: deciding about publicity,
- the effectiveness of attribution is limited by resources (technological, economic, time, qualification), which are, among other things, relevant to the damage,

¹³⁴ FBI Intelligence Cycle Graphic. URL: <https://www.fbi.gov/image-repository/intelligence-cycle-graphic.jpg/view>.

- analysis of attribution sub-tasks is performed to help decision makers take weighted decisions, with conclusions having some uncertainty.

Visually, the operation of data collection and analysis is represented by three rings, and the conclusion (in the form of a decision to publish a verdict) is creatively illustrated by the tail of the letter Q (Figure 4.9).

Figure 4.9. Q-model of cyber-attack attribution



Source: Rid T., Buchanan B. *Attributing Cyber Attacks* // *The Journal of Strategic Studies*. – 2015. - Vol. 38 (2015). - No. 1-2, 4-37. DOI: 10.1080/01402390.2014.977382.

Cluster models involve sub-areas of analysis, which can be studied in parallel engaging different groups of experts: 4C-model, variations of MICTIC-model, multifactor model, etc. MICTIC is the most elaborated one (Table 4). It includes six classes of attribution tasks: investigation of malware, infrastructure support, control servers, application debugging data, intelligence data, and motivation analysis.

Solving these tasks in parallel provides the most complete evidence and formulate the proof.

The advantage of conceptual models of the second type is that they can be detailed up to the mathematical simulation. The disadvantage is the fundamental dependence on the qualifications and motivation of experts.

Table 4.5. MICTIC structure

Mnemonics	Name	Description	Methods
<i>M</i>	Malware	Malware analysis	Antivirus checks, code analysis
<i>I</i>	Infrastructure	Attack infrastructure research	Monitoring, reverse tracing, trap creation
<i>C</i>	Control server	Management server identification	Forensic Analysis
<i>T</i>	Telemetry	Debugging data collection and analysis	Quality Management and Information Security
<i>I</i>	Intelligence	Obtaining data operationally	HUMID, OSINT
<i>C</i>	Cui Bono	Motivation analysis (“who benefits from this?”)	Structural hypothesis analysis, etc.

Source: Table constructed by the author.

Methods evaluating the significance of cyber-attack attributes create a theoretical basis of forensic procedures to obtaining objective (and even quantitative) indicators:

- Pattern analysis methods (signature methods), where there is an obvious indicator of a compromise or incident fact peculiar to the attacker, such as a reliable characteristic (hash) of a malicious file, command-and-control infrastructure identifiers, physical or network computer address (especially in locations where the Internet is legally prohibited),
- heuristic methods based on behavioral characteristics or anomalies, such as a group of hackers suddenly demonstrating in-depth knowledge in some features of cryptography and attack motives,
- combinations of these methods.

The most popular nowadays are heuristic approaches, in particular, actively developing North American project MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) on the construction of cyber-attack classifications, countermeasures, description of cyber groups, automation tools, report forms, etc. The current version of ATT&CK includes description of 14 target stages (originally called “tactics”), methods and techniques (“techniques” according to MITRE), as well as their implementations (procedures). This allows building a base of “behavioral profiles” of APT attacks, as well as cyber groups (if linked to cyber-attacks). The target stages reflect modern APT attacks in detail and include resource utilization, initial access, execution, persistence, privilege escalation, evasion, credential access, network exploration, adjacent network access attempts, data collection, management (command and control), data extraction, and impact.

In general, the methodology (like any abstract reflection of reality) is highly dependent on source data. Nowadays, receipt of different data is not restricted: direct, indirect, iterative with feedback, qualitative and quantitative, obtained by passive interception, by influence, provocation or as a result of misinformation, etc. Accordingly, they are characterized by different levels of reliability, which affects the uncertainty of simulation result and high level of international risks.

Obtaining representative (complete) raw data involves, on the one hand, access points (e.g., to communication channels and cloud) and, on the other hand, the ability to handle large amounts of unstructured data (“big data”).

The above analysis of cyber-attack attribution leads to the conclusion that a new multidisciplinary scientific trend (including issues of international law and technological development in the fourth industrial revolution period), affecting the sphere of global security, has emerged.

Success in attribution largely depends on objective territorial, scientific, technological, political, and economic factors that provide different opportunities for countries and military-political blocs, both in collecting evidence and in analyzing the same through “big data” processing, AI, super- and quantum computing.

Analysis of publicly available scientific research and information projects on cyber-attack attribution suggests that there is a divergence of evidence and conclusions between political blocs and alliances, which ultimately results in distrust, critical deterioration of international relations and decrease in the level of international security and strategic stability. This situation proves the need to develop a system for regulation of international information security in general and to overcome the barriers of attribution. This will make it possible to create an

international regulatory framework and mechanisms of international monitoring and control of cyber-attacks, which has been advocated by Russia for many years¹³⁵.

¹³⁵ Syromolotov O. Russia and the United States are able and ready to negotiate. Ria.ru. 03.11.2021. URL: <https://ria.ru/20211103/syromolotov-1757632718.html>.

CONCLUSION

The rapid development of ICTs has been going on for many years, and their introduction into all types and branches of the armed forces continues. It is a healthy and generally positive process. However, examination of threats in this area and timely response to identified problems, acceptable transparency in concrete solutions and demonstration of successes should accompany scientific and technological progress in the military field.

The most dangerous information threats to international security and stability are the use of ICT weapons for military and political purposes to carry out hostile actions and acts of aggression; destructive ICT impact on elements of critical state infrastructure; interference in the internal affairs of a sovereign state, reducing social stability, inciting interethnic and international discord through ICT. The presence of these dangers requires the search for additional mechanisms of international governance.

In the context of strategic stability, nuclear missile security requires special attention. All nuclear powers are modernizing them, seeking to introduce new computer technology. More and more components of military nuclear infrastructure – from warheads and their delivery vehicles to command-and-control systems, communications, command, and control systems for nuclear forces - depend on sophisticated software, making them potential targets for ICT-attacks.

This gives rise to potential risks, in particular, associated with an increase in probability:

- The BMs launch or the prevention (blocking) of a launch is erroneously authorized,
- The use of the Internet of Things (IoT) to provide false information from the MWS about enemy BM launches due to the growing sophistication of ICT-attacks,
- Damage or destruction of communication channels, interference to the command, control and monitoring system of the Armed Forces,
- The reduction of military decision makers' confidence in the operability of systems and the perception of some action as an initial step in the transition to a mutually assured destruction environment.

It is not possible to unambiguously identify any particular elements of the nuclear forces that are most susceptible to ICT threats. However, it is possible to identify the factors that have the greatest impact on vulnerability. These should include interaction with “public networks”; geography of combat duty; hardware components; “artificial intelligence”; qualification of operators; “human factor”. In any case, the protection of strategic weapons, air defense and missile defense

systems, communications, command, and control of nuclear weapons from ICT is an urgent global problem of our time.

In this regard, it is advisable to conduct a regular expert assessment and reassessment of the level of ICT threats in relation to various systems and subsystems of control and combat use of nuclear weapons.

Due to the scale of threats and the catastrophic consequences of the implementation of ICT threats to nuclear weapons, foreign policy agencies need to work actively to agree at the international level on lists of critical infrastructure of nuclear forces, the attempt to affect which using ICT will be regarded as an attempted disarming strike with appropriate consequences for the attacking party.

An important step toward including ICT threats in the dialogue on strategic stability could be the preparation of an appropriate section in the Glossary of Key Nuclear Terms, which the Nuclear Five agreed to refine during a conference in Washington in September 2016¹³⁶.

In parallel, work should continue at the UN to develop an ICT-weapons control regime that could include:

- specific confidence- and security-building measures in the ICT sphere,
- banning ICT-attacks on specific targets, including military and especially nuclear targets,
- limitation and/or rejection of offensive ICT capabilities,
- measures to control the proliferation of ICT weapons,
- international norms on the means and methods of preventing and eliminating cyber conflicts,
- the development of a convention banning the malicious use of ICTs in the field of nuclear weapons.

¹³⁶ Joint Statement from the Nuclear-Weapons States at the 2016 Washington, DC P5 Conference, Washington, DC, September 15, 2016 // The Ministry of Foreign Affairs of the Russian Federation URL: https://www.mid.ru/web/guest/adernoie-nerasprostranenie/-/asset_publisher/JrcRGi5UdnBO/content/id/2451010.

BIBLIOGRAPHY

Monographs

1. Борзенков А.С., Веселов В.А., Есин В.И., Шеремет И.А. Вопросы обеспечения стратегической стабильности в советско-американских и российско-американских отношениях: теоретические и прикладные аспекты. – М.: МАГУ, 2019. – 144 с.
2. Информационные вызовы национальной и международной безопасности / И.Ю. Алексеева и др. Под общ. ред. А.В. Федорова, В.Н. Цигичко. – М.: ПИР-Центр, 2001. – 328 с. ISBN 5-94013-006-2.
3. Лысенко Н. Наведение баллистических ракет. – М.: МГТУ им. Н. Э. Баумана, 2016. – 448 с.
4. Петренко С.А., Ступин Д.Д. Национальная система раннего предупреждения о компьютерном нападении / Под ред. С.Ф. Боев. – Иннополис: Издательство «Афина», 2017. – 439 с. ISBN 978-5-9909868-0-0.
5. Проблемы информационной безопасности в международных военно-политических отношениях / Под ред. А.В. Загорского, Н.П. Ромашкиной. – М.: ИМЭМО РАН, 2016. – 183 с. ISBN 978-5-9535-0477-5. DOI: 10.20542/978-5-9535-0477-5.
6. Ромашкина Н.П. Стратегическая стабильность в современной системе международных отношений. М.: Научная книга, 2008. – 288 с.
7. Ромашкина Н.П., Марков А.С., Стефанович Д.В. Международная безопасность, стратегическая стабильность и информационные технологии. – Москва, ИМЭМО РАН, 2020. – 98 с. ISBN 978-5-9535-0581-9. DOI: 10.20542/978-5-9535-0581-9.
8. Россия и дилеммы ядерного разоружения. Под ред. А.Г. Арбатова, В.З. Дворкина, С.К. Ознобищева – М.: ИМЭМО РАН, 2011. – 237 с. ISBN 978-5-9535-0323-5.
9. Суперкомпьютерные технологии в науке, образовании и промышленности / Под ред. В.А. Садовниченко, Г.И. Савина, В.В. Воеводина. – М.: Издательство Московского университета, 2009. – 232 с. ISBN 978-5-211-05719-7.

10. Угрозы информационной безопасности в кризисах и конфликтах 21 века. – М.: ИМЭМО РАН, 2015. – 151 с. ISBN 978-5-9535-0450-8.
11. Clarke R.A., Knake R. Cyber War: The Next Threat to National Security and What to Do about It. – New York: HarperCollins, 2010. – 320 p.
12. Futter A. Hacking the Bomb: Cyber Threats and Nuclear Weapons. – Georgetown: Georgetown University Press, 2018. – 208 p.
13. Harris S. @War: The Rise of the Military-Internet Complex. – Boston: Houghton Mifflin Harcourt, 2014. – 263 p.
14. Information Security Threats during Crisis and Conflicts of the XXI Century / Eds.: N.P. Romashkina, A.V. Zagorskii. Moscow: IMEMO, 2016. – 133 p. ISBN 978-5-9535-0461-4. DOI: 10.20542/978-5-9535-0461-4.
15. Nuclear Proliferation: New Technologies, Arms and Treaties / ed. by A. Arbatov, V. Dvorkin; Carnegie Moscow Center. – Moscow: Russian Political Encyclopedia (ROSSPEN), 2009. — 272 p.
16. Petrenko S. Cyber Security Innovation for the Digital Economy a Case Study of the Russian Federation. – River Publishers, 2018. – 492 p.
17. Probabilistic Modeling in System Engineering / A. Kostogryzov (ed.). – London: IntechOpen, 2018. – 290 p. DOI: 10.5772/intechopen.71396.
18. Wheeler D. A., Larsen G. N. Techniques for Cyber Attack Attribution. – Alexandria, VA: Institute for Defense Analyses Alexandria, 2003. – 84 p.

Articles

1. Арбатов А.Г. Роль ядерного сдерживания в обеспечении стратегической стабильности. Гарантия или угроза / Московский центр Карнеги. 2019. 28 января.
2. Арбатов А.Г. Угрозы стратегической стабильности – мнимые и реальные / А. Г. Арбатов // Полис. Политические исследования. – 2018. – № 3. – С. 7-29. DOI: 10.17976/jpps/2018.03.02.
3. Арбатов А.Г. Разоружение – утопия или императив пост-вильсоновской эпохи? / РСМД. 2018. 16 января.
4. Арбатов А.Г. Ядерный потолок // Военно-промышленный курьер ВПК. – 2014. – № 26 (544). 23 июля. – С. 4-5.

5. Бендерский Л.А., Любимов Д.А., Рыбаков А.А. Анализ эффективности масштабирования при расчетах высокоскоростных турбулентных течений на суперкомпьютере RANS/ILES методом высокого разрешения // Труды Научно-исследовательского института системных исследований Российской академии наук. – 2017. – Т. 7. – № 4. – С. 32-40.
6. Бойко С.М. Основы государственной политики Российской Федерации в области международной информационной безопасности: регулирование и механизмы реализации // Международная жизнь. – 2018. – № 11. – С.23-35.
7. Гареев М. А., Турко Н. И. Война: современное толкование теории и реалии практики // Вестник Академии военных наук. – 2017. – № 1. – С. 4-10. ISSN: 2073-8641.
8. Карцхия А.А., Макаренко Г.И., Сергин М.Ю. Современные тренды киберугроз и трансформация понятия кибербезопасности в условиях цифровизации системы права // Вопросы кибербезопасности. – 2019. – № 3 (31). – С. 18-23. // DOI: 10.21681/2311-3456-2019-3-18-23.
9. Крутских А. В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. – 2007. – Т. 5. – № 13. – С. 28-37. ISSN: 1728-2756.
10. Крутских А. В., Стрельцов А.А. Международное право и проблема обеспечения международной информационной безопасности // Международная жизнь. – 2014. – №. 11. – Стр. 20-34. ISSN: 0130-9625.
11. Лукацкий А. В. Определение источника кибератак // Индекс безопасности. – 2015. – Т. – № 2. – С. 73-86. ISSN: 1992-9242.
12. Марков А.С., Фадин А.А. Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet // Проблемы кибербезопасности. – 2013. – № 1. – С. 28-36. ISSN: 2311-3456.
13. Марков А.С., Ромашкина Н.П. Проблема выявления источника (причастности) кибератак - фактор международной безопасности // Мировая экономика и международные отношения, 2022, том 66, № 12, стр. 58-68. DOI: 10.20542/0131-2227-2022-66-12-58-68.
14. Марков А. С., Шеремет И. А. Безопасность программного обеспечения в контексте стратегической стабильности // Вестник Академии военных наук. – 2019. – № 2. – С. 82-90. ISSN: 2073-8641.

15. Петренко А.А., Петренко С.А. НИОКР Агенства DARPA в области кибербезопасности // Вопросы кибербезопасности. – 2015. – № 4 (12). – С. 2-22. ISSN: 2311-3456.
16. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. – 2019. – №. 1 (29). – С. 2-9. DOI: 10.21681/2311-3456-2019-1-2-9.
17. Ромашкина Н.П. Глобальные ИКТ-угрозы в военно-политической сфере // Международная жизнь. – 2020. – Спецвыпуск. Международная конференция «Киберстабильность: подходы, перспективы, вызовы». – С. 162-168.
18. Ромашкина Н.П. Космос как часть глобального информационного пространства в период военных действий // Вопросы кибербезопасности. – 2022. № 6 (52). – С. 100-111. DOI 10.21681/2311-3456-2022-6-100-111.
19. Ромашкина Н.П. Международно-правовой режим контроля над кибероружием в будущем миропорядке: угрозы и перспективы // Дипломатическая служба. – 2023. № 2. С. 150-161. DOI: 10.33920 / vne-01–2302–07.
20. Ромашкина Н.П. Новые технологии: вызовы международной безопасности и стабильности // Безопасные информационные технологии. Сборник трудов Десятой международной научно-технической конференции. – 2019. Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет). Москва. – С. 329-334.
21. Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения. – 2020. т. 64, № 12. С. 25-32. DOI: 10.20542/0131-2227-2020-64-12-25-32.
22. Ромашкина Н.П. Стратегическая стабильность: новые вызовы инфосферы // РСМД. – 2017. 23 ноября.
23. Сангалов В. А. Угрозы национальной безопасности России в информационной сфере // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2015. – №. 8-3. – С. 161-167. ISSN: 1997-292X.
24. Стефанович Д.В. Космос как предчувствие // Россия в глобальной политике. – 2020. – Т. 18. – № 5. – С. 187-196. ISSN: 1810-6439.

25. Стефанович Д.В. Ядерно-кибернетические комплексы // Российский совет по международным делам. – 2017. 7июля.
26. Стефанович Д.В. Ядерное измерение киберугроз // Российский совет по международным делам. – 2019. 5 августа.
27. Стрельцов А. А. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности // Международная жизнь. – 2017. – №. 2. – Стр. 87-106. ISSN: 0130-9625.
28. Шерстюк В. П. XIV Научная конференция Международного исследовательского консорциума информационной безопасности // Международная жизнь. – 2017. – №. 14. – Стр. 42-180. ISSN: 0130-9625.
29. Acton J.M., Zhao T., Bin L. Reducing the Risks of Nuclear Entanglement. September 12, 2018. Carnegie Endowment for International Peace.
30. Axelrod R., Iliev R. Timing of cyber conflict // Proceedings of the National Academy of Sciences. – 2014. - Vol. 111. – №. 4. – Pp. 1298-1303.
31. Barabanov A., Grishin M., Markov A., Tsirlov V. Current Taxonomy of Information Security Threats in Software Development Life Cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). IEEE (17-19 Oct 2018, Almaty, Kazakhstan). 2018. Pp. 356-361. DOI: 10.1109/ICAICT.2018.8747065.
32. Barabanov A. V., Markov A. S., Tsirlov V. L. Statistics of software vulnerability detection in certification testing // Journal of Physics: Conference Series. – 2018. Vol. 1015. – №. 4. DOI: 10.1088/1742-6596/1015/4/042033.
33. Barabanov A. V., Markov A. S., Tsirlov V. L. Topical issues of revealing vulnerabilities and undeclared features in software // High Availability Systems. – 2018. – Т. 14. – №. 3. – Pp. 12-17. DOI: 10.18127/j20729472-201803-03.
34. Barabanov A.V., Markov A.S., Tsirlov V.L. On the systematics of information security of software supply chains // Information Technology Security. – 2019. – Т. 26. – № 3. DOI: 10.26583/bit.2019.3.06.
35. Boyko S.M. Foundations of the State Policy of the Russian Federation in the Field of International Information Security: Regulation and Mechanisms of Implementation // International Life. – 2018. – № 11. – Pp.23-35.

36. Browne A. China: Cyber-attacks Are Like Nuclear Bombs. *The Wall Street Journal*. April 22, 2013.
37. Dacier M., Pham V. H., Thonnard O. The WOMBAT Attack Attribution method: some results // *International Conference on Information Systems Security*. Berlin, Heidelberg: Springer, 2009. – Pp. 19-37.
38. Fitton O. Cyber operations and gray zones: Challenges for NATO // *Connections*. – 2016. – T. 15. – №. 2. – Pp. 109-119. DOI: 10.11610/Connections.15.2.08.
39. Grotto A. Deconstructing Cyber Attribution: A Proposed Framework and Lexicon // *IEEE Security & Privacy*. – 2019. – T. 18. – №. 1. – Pp. 12-20. DOI:10.1109/MSEC.2019.2938134.
40. Howard M., Lipner S. *The Security Development Lifecycle: A Process for Developing Demonstrably More Secure Software*. Microsoft Press, 2006. – 25 p.
41. Lin H. Attribution of malicious cyber incidents: From soup to nuts. Hoover Working Group on National Security, Technology, and Law. Aegis Series Paper No 1607. 2016. 26 September. – 56 p. URL: https://www.hoover.org/sites/default/files/research/docs/lin_webready.pdf.
42. Markov A.S., Sheremet I.A. Enhancement of Confidence in Software in the Context of International Security // *CEUR Workshop Proceedings*. – 2019. Vol. 2603. – Pp.88-92.
43. Mulvenon J. Toward a cyberconflict studies research agenda // *IEEE Security & Privacy*. – 2005. Vol. 3. – №. 4. – Pp. 52-55.
44. Nunes E. et al. Argumentation models for cyber attribution // *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 2016. – Pp. 837-844.
45. Reed M., Miller J. F., Popick P. Supply chain attack patterns: Framework and Catalog // *Office of the Deputy Assistant Secretary of Defense for Systems Engineering*. – 2014. – 88 p.
46. Rid T., Buchanan B. *Attributing Cyber Attacks* // *The Journal of Strategic Studies*. 2015 Vol. 38. Nos. 1-2. – Pp.4-37. DOI: 10.1080/01402390.2014.977382.

47. Romashkina N.P. New Technologies: Challenges to International Security and Stability // CEUR Workshop Proceedings. Selected Papers of the X Anniversary International Scientific and Technical Conference on Secure Information Technologies (BIT 2019). – 2019. Vol. 2603. – Pp.65-69.
48. Russia and Global Information Security Challenges. XII International Forum “Partnership of the State, Business and Civil Society in Ensuring International Information Security” Garmisch-Partenkirchen, Germany April 16-19, 2018 // International Life, 2018. Special Issue. – 180 p.
49. Skopik F., Pahi T. Under false flag: using technical artifacts for cyber-attack attribution. Cybersecurity. 2020. Pp. 3-8.
50. Stefanovich D. Artificial intelligence advances in Russian strategic weapons // The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Vol. III. South Asian Perspectives. – Stockholm: SIPRI, 2020. – Pp.25-29.
51. Stefanovich D. Proliferation and threats of reconnaissance-strike systems: a Russian perspective // The Nonproliferation Review. – 2020. Vol. 27. Issue ½. DOI: 10.1080/10736700.2020.1795370.
52. Stefanovich D. Russia's Basic Principles and the Cyber-Nuclear Nexus // The European Leadership Network. 2020. 14 July.
53. Varenitca V., Markov A., Naschokin P. Topical Issues Related to Certification Tests of Information Security Tools. CEUR Workshop Proceedings, 2021, V 3035. Pp.193-202.

ABOUT THE AUTHORS

Romashkina Natalia Petrovna – Head of the Information Security Problems Group of the International Security Center of the Primakov Institute of World Economy and International Relations, PhD in Political Science, romachkinan@yandex.ru.

Markov Alexey Sergeevich – Professor, Department of Information Security, Bauman Moscow State Technical University, Doctor of Technical Sciences, laureate of the Government Prize in Science and Technology, CISSP, a.markov@bmstu.ru.

Stefanovich Dmitri Viktorovich – Researcher at the International Security Center of the Primakov Institute of World Economy and International Relations, stefanovich@imemo.ru.

Научное издание

Romashkina Natalia Petrovna
Markov Alexey Sergeevich
Stefanovich Dmitri Viktorovich

INFORMATION TECHNOLOGIES
AND
INTERNATIONAL SECURITY

Монография

ISBN 978-5-9535-0613-7



9 785953 506137

Подписано к опубликованию 31.05.2023 г.
Объем 6,3 а.л.

Издательство ИМЭМО РАН
Адрес: 117997, Москва, Профсоюзная ул., 23