Strategic Issues of Application of Information and Communication Technologies in the Military and Political Sphere

Nataliya P. Romashkina [1]

[1] *Primakov National Research Institute of World Economy and International Relations (IMEMO), Russian Academy of Sciences, 23, Profsoyuznaya Str., Moscow, 117997, Russia*

Abstract

The article presents the results of the analysis of strategic problems corresponding to information and cyber security in the military-political sphere. The study justifies the consideration of the ensuring international information security problem as a part of a broader topic of global international security. The problem of using information and communication technologies (ICT) for military and political purposes to carry out hostile actions and acts of aggression is presented. The importance of ensuring the information security of military facilities as a part of the critical infrastructure of the state is indicated. The article identifies strategic threats to information security in the military-political sphere, the signs of their presence and the possibility of their implementation. The article presents the analysis of the First UN Committee activities on the development of mechanisms of international governance in this area. Finally, it explores the possibilities of creating an international regime to prohibit information (including cyber) weapons in response to urgent global challenges to international security and strategic stability.

Keywords

Information and communication technologies, international security, information security, cyber security, information weapons, cyber weapons, information threat, nuclear weapons, strategic stability

1. Introduction

In recent decades, information and communication technologies (ICT) have become a catalyst in all areas of human life. The all-encompassing importance of new technologies in the modern world was most acutely outlined by the 2019-2021 coronavirus pandemic, when entire industries, economics, science and education switched to online work. For the first time in a new environment, sessions and intersessional consultations at the United Nations were held in a virtual format. All states recognize the unprecedented benefits of ICT, but the avalanche-like growth of threats in this area has led to a deep awareness of the fact that unregulated use of ICT can pose a serious threat to international security, peace and stability. The problems of international information security (IIS) and cybersecurity became an integral part of global international security, and information and communication technologies began to have a significant impact on it. That is why various aspects of international information security have been on the agenda of the First Committee of the UN General Assembly, which considers issues related to threats to peace and international security and discusses ways to strengthen them, for more than 20 years [1, 2, 3].

The issues of the harmful use of ICT in the military-political sphere are the most difficult within the framework of international organizations. For the first time, an indication of ICT threats in relation not only to the civilian, but also to the military field was contained in the United Nations 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 international documents at the UN level, which pose normative restrictions on such illegal activities, have been adopted. As a result, information

BIT-2021: XI International Scientific and Technical Conference on Secure Information Technologies, April 6-7, 2021, Moscow, Russia

EMAIL: romachkinan@yandex.ru
ORCID: 0000-0002-3725-9759

tools for creating a destructive effect in the military-political sphere are constantly being improved, and new ICT weapons are being developed for military warfare, reconnaissance confrontation, electronic warfare, etc., for intervention in the internal affairs of states, for harmful effects on objects of critical state infrastructure and, in particular, on objects of the military-industrial complex [4, 5].

2. The problem of using information and communication technologies for military and political purposes

Currently, the problem of the development and application of information and communication technologies for destructive military-political purposes is indicated in the documents of many countries and is established not only at the domestic level, but also at the international level, including the UN agenda [6, 7].

For example, the 2013 report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) notes: “Threats to individuals, businesses, national infrastructure and Governments have grown more acute and incidents more damaging. The sources of these threats comprise both State and non-State actors. In addition, individuals, groups, or organizations, including criminal organizations, may act as proxies for States in the conduct of malicious ICT actions. The potential for the development and the spread of sophisticated malicious tools and techniques, such as bot-nets, by States or non-State actors may further increase the risk of mistaken attribution and unintended escalation. The absence of common understandings on acceptable State behaviour with regard to the use of ICTs increases the risk to international peace and security" [8].

The 2015 GGE report highlighted the following issues of the application of information and communication technologies for military-political purposes: ICT should be used exclusively for peaceful purposes, and international cooperation should be aimed at preventing conflicts in the information space; states must not use intermediaries to carry out computer attacks and should not provide their territory for these purposes; states must fight against the use of hidden malicious functions - "bookmarks" - in IT products. Current and potential threats in the Report include the activities of a number of states to build capacity in the field of ICT for military purposes, the increased likelihood of using ICTs in future conflicts between states, and the ICT attacks on critical infrastructure and related information systems of States [9].

The 2021 report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security notes: “Negative trends in the digital domain could undermine international security and stability… States recalled that a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in future conflicts between States is becoming more likely. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. States also concluded that any use of ICTs by States in a manner inconsistent with their obligations under the framework, which includes voluntary norms, international law, and CBMs, undermines international peace and security, trust and stability between States, and may increase the likelihood of future conflicts between States [10].”

The use of ICT for military and political purposes to carry out hostile actions and acts of aggression is the most problematic issue in the context of ensuring national and international security, which becomes the cause of interstate contradictions. In particular, this is due to the fact that ICT is an extremely "convenient" instrument of influence, which provides almost unlimited opportunities for affecting various issues in the field of international relations, world politics and economics. Moreover, actions can be disguised as criminal or terrorist in such a way that identifying the real source, target and even the final object of influence becomes a very difficult task [1, 11].

Thus, the urgency of the problem of the ICT military-political use for destructive purposes is justified by the comprehensive nature of the permanently developing ICT, which give rise to improvement and development of a new class of weapons and, consequently, to the emergence of a new class of threats in the military-political sphere [12, 13].

Therefore, an effective regulatory system in the digital environment is required, including coordinating actions of the leading actors as well as international and domestic mechanisms, supported by the UN.

2.1. Information technologies as an instrument in politics

Currently, the use of ICT becomes one of the most important elements of the military and political potential of states that supplements and sometimes even replaces traditional political and diplomatic means and weapons. Under conditions of simultaneously developing processes of the arms control regime destruction and the growing contradictions in relations between the great powers, the importance of military power and informational technologies of military and dual use, being key factors of competition and confrontation, persists and even increases [14, 15].

Security of ICT systems, which have become an important factor in ensuring the state sovereignty, defense capabilities and security, are strategically important for most countries of the world [16, 17]. This involves a threat of the accelerated development (race) of information weapons both for interference in the internal state affairs as well as for military purposes [18] (Table 1).

ICT can provoke the outbreak of interstate military conflict, primarily due to the possibility of disproportionate response to threats and attacks (e.g., the affected party may use real weapons in response). In addition, the conflict may arise by mistake, as there are currently no universal methodology, criteria and principles for identification of perpetrators, classification of cyberattacks and investigation of incidents. As a whole, it significantly reduces the level of strategic stability [19, 20, 21].

Table 1
The problem of using ICT for military and political purposes to carry out hostile actions and acts of aggression

Threat	Signs of threat	Threat implementation opportunities
Development of ICT weapons	Accelerating the militarization of the ICT space	*ICT for military applications*: fight against command and control systems; reconnaissance confrontation; electronic confrontation; military means to facilitate information operations
	Inclusion of the ICT sphere in the integrated battlefield in the strategies of some countries	
	Offensive cyber weapons and cyber troops in more than 30 states	
	Buildup of offensive and defensive information operations by NATO countries	
	Plans to create cyber warfare assets in 140 countries	
	Difficulty in identifying the author of an ICT attack, the possibility of using a "false flag"	
Use of ICT for hostile military-political purposes, to interfere in the internal affairs of states	*Examples of interference*:	*Alternative means of influencing the enemy:* *economic* (ICT-impact on industrial and financial facilities);
	Solidarity Revolution, Poland, 1980-1990	
	"Velvet Revolution", Czechoslovakia,1989	
	"Bulldozer Revolution", Yugoslavia, 2000	
	Preparation of an ICT invasion, Afghanistan, 2001	

	Rose Revolution, Georgia, 2003	*informational* (propaganda broadcasting, Internet, SMS, etc.) for preparation and conduct of riots, anti-government demonstrations, political actions, coups
	Military invasion using ICT, Iraq, 2003	
	Orange Revolution, Ukraine, 2004	
	Tulip Revolution, Kyrgyzstan, 2005	
	Jasmine Revolution, Tunisia, 2011	
	Twitter Revolution (Lotus Revolution), Egypt, 2011	
	Civil war, Libya, 2011	
	"Euromaidan", Ukraine, 2013-2014	
	"Socket Revolution", Armenia, 2015	
	War, Syria, 2011 - present time	
	Preparation of a coup d'état, Venezuela, 2019	
	Preparation of a coup d'etat, Belarus, 2020	

2.2. Cyber threats in the strategic military sphere

Up to date, dozens of countries already have a software to attack national critical infrastructure's (CI) facilities. At the same time, the threat indicator for the APCS is currently assessed by experts as critical or high. Malware is currently being developed in many countries, but 83% of all sites used to spread "malware" are located in just 10 states. The leader of this ranking is the U.S., 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 national and global levels [22, 23, 24]. Thus, such malware can be considered as a 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.

Threats are intensified by NATO's decision to apply Article 5 of the Alliance's Charter in response to cyber attacks [25]. The issues of coordination of measures taken in response to information operations recognized as acts of force remain unresolved. As a result, information wars of some states against others may be similarly destructive as the traditional wars, and the use of new technologies can become the catalyst of interstate military conflict involving the use of strategic and nuclear weapons. 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, the fundamental change of the underlying principles doesn't appear to be necessary, since 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, supercomputers, autonomous operation capabilities of various systems and subsystems, automated decision-making systems, artificial intelligence for military purposes being subject to ICT attacks, and the means of cyber-electromagnetic activities being actively improved in developed countries, primarily in the USA [1, 11, 26].

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 that may significantly lower 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. The trend towards spreading such views has also arisen with the help of modern ICTs, which make it possible to influence a huge audience in a relatively short time and without serious economic costs. 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 applying malicious technologies, including state and non-state actors along with lone-wolf hackers. As a whole, it increases the level of uncertainty and instability [27, 28, 29].

One of the most important global problems is the information security of military facilities as a part of CI and most importantly nuclear weapons systems. There are several types of threats that create the problem of ensuring the ICT security for military-industrial complex facilities (Table 2).

Table 2
The problem of ensuring information security for military facilities as a part of critical infrastructure

Threat	Signs of threat	Threat implementation opportunities
Development of ICT tools for malicious effects on military-industrial complex objects	ICT threats to the military organization and infrastructure, including strategic weapons, missile attack warning system (EWS), nuclear command and control system, missile defense, air defense	Cyberattacks on military or related civilian infrastructure; physical damage to the software, element base, communication lines and networks of the military facility; 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; uncertainty among commanders and personnel about the smooth and efficient operation of systems
	Attacking robotic weapons, artificial intelligence at military facilities, automated decision-making systems etc. that may be subject to cyber attacks	
	Transfer of strategic troops in different countries to digital technologies for information transmission, making them more vulnerable to malicious information technology	
Reduction of the strategic stability level	The impact of ICT development on the growing probability of:	
	• An erroneously authorized ballistic missile launch	
	• The use of Internet to provide false information from the Ballistic Missile Early Warning System about enemy ballistic missile launches due to the growing sophistication of cyber attacks	
	• Damage or destruction of communication channels, interference in the control system of arms, including nuclear forces	
	• Reducing the confidence of military decision makers in the operability of the command and control systems	
	The impact of the increased likelihood of disabling or destroying nuclear weapons through ICTs on the future of nuclear disarmament and nonproliferation processes	
	Influence of ICT factors on the level of strategic stability	

3. International information security as a part of global security problem

The avalanche-like increase in threats resulting from the malicious use of information and communication technologies in the political, military, economic and social spheres has led to a deep awareness of the fact that new 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 that excludes the possibility of violating the rights of individuals, society and the state in the information sphere, and protects from destructive and illegal impact on the elements of national critical information infrastructure, has become an integral part of international security. The latter can be defined as a system of international relations, which is based on the universal compliance with recognized principles and norms of international law by all states and excludes the use of force or threat as an instrument to resolve controversial issues and disagreements between them.

Therefore, the principles of international security that provide for the assertion of peaceful coexistence, 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 to the sovereign rights of every nation, and fair political settlement of international crises and regional conflicts, certainly involve the establishment of international information security. Such a system designed to counter threats to strategic stability and to ensure equal partnership in the global digital environment, can be considered as a set of international and national institutions that regulate the activities of various subjects of the global information space, including the UN.

There are many reasons to discuss issues related to ICT development in the main areas of UN activity: peace and security, human rights, and sustainable development. Besides the work on advances in ICT in the context of international security, other aspects discussed in various UN bodies 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.

Since the effective functioning of the collective security mechanism enshrined in the UN Charter is an integral part of international security, the problem of IIS maintenance has been included in the agenda of one out of six main committees of the UN General Assembly (UNGA), known as the First Committee dealing with disarmament and related international security issues. This is the place where states discuss threats to peace and seek ways to resist them. 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 many reasons that justify the expediency and importance of IIS issues discussion in the First Committee of the UNGA. We will specify 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 real armed conflicts, their escalation and, consequently, of large-scale war. Thus, the problem of ensuring information security is strategic, and the level of ICT security has a significant impact on the level of strategic stability. Therefore, it is necessary to search for additional mechanisms of global governance in this area. In the absence of agreement between states, the number and scale of such threats will increase. At the same time, the discussion within the framework of the First Committee of the UNGA allows to develop trust-building measures along with principles and norms of responsible state behavior in the digital space that can reduce the risk of conflicts and their escalation. Such activities enable focusing on the coordination and support of ICT security capacity building and avoiding superiority of one or several states over most others in the ICT space (the "digital gap").

Second, analysis of precedents of ICT attacks on critical state infrastructure proves that their number and scale are growing exponentially year after year. Cyberattacks on resources and objects critical for country's vital activity can lead to a negative and even catastrophic impact on security systems, health care, public administration, the military sector and the economic potential of the state that underlines necessity for the discussion of the responsible state behavior in the information sphere within First Committee of the UN General Assembly.

Third, despite the development of national and regional instruments for regulation of ICT space activities, not a single country in the world, up to date, is able to ensure its full protection against ICT threats with no state borders and can solve the related problems alone. Therefore, discussion at the UN level is of vital importance. The emphasis on coordination between states and various stakeholders, which is now covered in many national and regional cyber and information security strategies, is also reflected in the processes happening within the framework of the First Committee of the UNGA. At the same time, the results of the work at the global level influence national and regional norms and principles, which can also contribute to the promotion of peace and stability.

At the end of 2018, the UN First Committee established two parallel discussions on international information security processes, held within the UN Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), initiated by Russia, and the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security (GGE), proposed by the United States. The reports of both groups adopted by consensus that sum up the results of two years of work became important results in the process of providing IIS in the difficult conditions of a pandemic. They included the report of the OEWG, dated by March 12, 2021, and the report of the GGE dated by May 28, 2021.

The report of the OEWG can be considered as the success of the work of the Group, which has opened a new format for negotiations on the security in the digital space that was initiated by Russia in 2018. The activities of the second convocation of OEWG on security issues related to the ICTs and their use will continue in 2021–2025. The demand for the Russian idea of consolidation of such a mechanism in the UN structure in the long term was confirmed by the UN General Assembly Resolution 75/240, adopted on December 31, 2020.

In the GGE Report, which was the result of a compromise, the Russian delegation managed to achieve a reflection of the provisions fundamental for the Russian Federation, including the most critical problems such as attribution of incidents in the ICT space, international legal regulation of this area, the necessity of further work on the rules of the responsible behavior of states with the UN assistance, and the possibility of developing legally binding norms.

However, disagreement over the advisability of developing international legal norms aimed to regulate the use of ICT for military purposes still has a negative impact on the achievement of compromise between states and the 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, rather than legalize and regulate such conflicts.

During the analysis and forecasting of the ways to solve the problem of using information and communication technologies for military and political purposes to carry out hostile actions and acts of aggression, one has to take into account the most important geopolitical characteristics of the modern stage that do not promote the efficiency of the process. They are related to the lack of cooperation between the "great powers" in this field and to the lack of transparency in relations between states, making it difficult to assess the commitment of countries to the norms and principles of behavior in the digital space. Moreover, the lack of clear incentives and specific benefits for agents, which comply with the norms, significantly hinders the development of an international regime for the management and control of harmful ICTs. Thus, it is relevant to expand the research corresponding to the evaluation of existing rules applicable to the information space and to the identification of additional effective norms. 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 to monitor dangerous ICT incidents. Interdisciplinary and multidisciplinary analysis of existing threats to IIS along with scientific forecasting and planning of future dangers by the scientific and expert community thus become even more important nowadays.

Thus, the following conclusions can be drawn.

1. The use of ICT for military and political purposes to carry out hostile actions and acts of aggression; the destructive ICT impact on elements of critical infrastructure; the interference in the internal affairs of states, and the violation of public stability through ICT are reasonably identified as the most dangerous threats in Russian documents and require the development of additional mechanisms of international governance.
2. Due to the scale of ICT threats in the strategic military sphere, the work of foreign policy departments is necessary to agree at the international level on the lists of critical military (nuclear) infrastructure. An attempt to affect this infrastructure with the ICT will be regarded as a disarming strike with corresponding consequences.
3. UN work is needed to shape an ICT arms control regime that may include:

- Specific measures to build confidence and security in the ICT field,
- Prohibition of ICT attacks on specific objects, particularly in the military sphere,
- Regulations that limit and/or forbid offensive ICT capabilities,
- Measures to control the proliferation of ICT weapons,
- International standards on means and methods to prevent and eliminate cyber conflicts,

• Development of a convention on the prohibition of the ICT harmful use in the field of nuclear weapons.

4. Acknowledgements

I would like to thank Prof. Nikolay I. Turko, Doctor of Military Sciences and Technical Sciences for insightful discussion, valuable suggestions, and revision of the manuscript.

5. References

[1] Romashkina N.P., Markov A.S., Stefanovich D.V. International Security, Strategic Stability and Information Technologies – Moscow, IMEMO, 2020. – 98 p. ISBN 978-5-9535-0581-9 DOI:10.20542/978-5-9535-0581-9. (in Russ).

[2] XII International Forum Partnership of State, Business and Civil Society at Providing International Information Security (Garmisch-Partenkirchen, Germany April 16–19, 2018). International Affairs: A Russian Journal of World Politics, Diplomacy and International Relations. 2018. Special Issue. 146 p. URL: https://interaffairs.ru/virtualread/garmish2018/ publication.pdf (in Russ).

[3] D. Kosiur, Understanding Policy-Based Networking, 2nd. ed., Wiley, New York, NY, 2001.

[4] Axelrod R., Iliev R. Timing of Cyber Conflict. In: Proceedings of the National Academy of Sciences of the United States of America, 111 (42014), January 28, 2014: 1298–1303.

[5] Harris S. @War: The Rise of the Military-Internet Complex. - Eamon Dolan/Houghton Miffl in Harcourt, 2014. 288 p.

[6] Clarke R.A., Knake R. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins, 2010, 312 p.

[7] Information Security Threats during Crisis and Conflicts of the XXI Century / A.V. Zagorskii, N.P. Romashkina, eds. – Moscow, IMEMO RAN, 2016. – 133 p. DOI: 10.20542/978-5-9535-0461-4. URL: https://www.imemo.ru/publications/info/information-security-threats-during-crisis-and-conflicts-of-the-xxi-century.

[8] United Nations A/68/98*, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&Lang=E.

[9] United Nations A/70/174, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Note by the Secretary-General, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=E.

[10] United Nations A/AC.290/2021/CRP.2, Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report. URL: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[11] Informational Security Problems in Modern International crises and conflicts of XXI century / A.V. Zagorski, N.P. Romashkina, eds. – Moscow, IMEMO RAN, 2016. – 183 p. DOI: 10.20542/978-5-9535-0477-5. URL: https://www.imemo.ru/files/File/ru/publ/2016/2016_037.pdf.

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

[13] Mulvenon J. Toward a Cyberconflict Studies Research Agenda. IEEE Security & Privacy. 2005, V.3, N 4, pp. 52-55.

[14] Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 287 p. DOI: 10.5772/intechopen.71396.

[15] Petrenko S. Cyber resilient platform for internet of things (IIoT/IoT)ed systems: survey of architecture patterns. Voprosy kiberbezopasnosti. 2021. N 2 (42). P. 81-91. DOI: 10.21681/2311-3456-2021-2-81-91.

[16] Molander R., Riddile A., Wilson P. Strategic information warfare: a new face of war. Library of Congress Cataloging in Publication Data, RAND (Firm), 1996. 33 p. URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR661.pdf.

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

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

[19] Futter A. Hacking the Bomb: Cyber Threats and Nuclear Weapons. - Georgetown University Press, 2018, 216 p.

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

[21] Markov A.S., Sheremet I.A. Enhancement of Confidence in Software in the Context of International Security. CEUR Workshop Proceedings, 2019, V. 2603, pp. 88-92.

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

[23] L. A. Maglaras, K.-H. Kim, H. Janicke and etc. Cybersecurity of critical infrastructures. ICT Express, 2018 (18) (PDF) Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. URL: https://www.researchgate.net/publication/328077921_Threats_Countermeasures_and_Attribution_of_Cyber_Attacks_on_Critical_Infrastructures.

[24] M. Evans, Y. He, L. Maglaras, and H. Janicke. Heart-is: A novel technique for evaluatinghuman error-related information security incidents.Computers & Security, 2018 (18) (PDF) Threats, Countermeasures and Attribution of Cyber Attacks on Critical Infrastructures. URL: https://www.researchgate.net/publication/328077921_Threats_Countermeasures_and_Attribution_of_Cyber_Attacks_on_Critical_Infrastructures.

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

[26] Schwab K. The fourth industrial revolution: what it means and how to respond? // The Fourth Industrial Revolution: A Davos Reader. Foreign Affairs Special Collection. January 2016. P. 3–11. URL: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrialrevolution.

[27] Nye J.S. The information revolution and soft power. Current History. V. 113. No. 759. 2014.

[28] Skopik F., Pahi T. Under false flag: using technical artifactsfor cyber attack attribution. Cybersecurity. 2020. P. 3 – 8.

[29] Romashkina N., Stefanovich D. Strategic Risks and Problems of Cyber Security. Voprosy kiberbezopasnosti [Cybersecurity issues], 2020, No 5 (39), pp. 77-86. DOI: 10.21681/2311-3456-2020-05-77-86. (In Russ.)