SILENT WARFARE: UNDERSTANDING THE IMPACT OF CYBER BLOCKADES AND SANCTIONS

Serghei Ohrimenco
Laboratory of Information Security, Academy of Economic Studies of Moldova, Chisinau, Moldova
https:/orcid.org/0000-0002-6734-4321

Valeriu Cernei
Partner, IT Audit & Advisory BSD Management SRL, Moldova, Chisinau, Moldova
https:/orcid.org/0000-0003-3300-334X

JEL Category: **F52, H56**

Abstract

Traditionally, experts considered several blockades, including sea and land, with the development of aircraft transportation - air, and with the advent of space technology and special satellites - space. Also, information blockades have been introduced with the rapid development of computer technology and communication tools. Each type of blockade had its historical characteristics; they differed in costs and, of course, efficiency. In the second half and at the end of the 20th century, scientists operated the term cyber blockade and restrictions in cyberspace. The paper sequentially considers physical environments (domains): air, land, sea, outer space, information space, and cyberspace. Multiple definitions of cyberspace have emerged as this concept evolves and becomes more nuanced in response to rapid developments in the technical, technological, economic, and social dimensions of modern life. Due to their potential, cyber-attacks and cyber warfare have garnered significant attention considering the ongoing development of society and business. Cyber-attacks are carried out regularly - against government agencies, military and civilian departments, and private businesses. The growing dependence of countries on cyberspace can play a negative role in the process of confrontation. The enemy can attack those areas where cyberspace is a decisive element. The authors discussed the questions of cyber-blockade efficiency.

Keywords: *Cyber Domain, Cyberspace, Cyber Attacks, Cyber War, Cyber Blockade, Cyber Sanctions*

Address of the corresponding author:
Serghei Ohrimenco
osa@ase.md

1 INTRODUCTION

The organization and operation of sanctions in cyberspace is a new area that needs research. Cyber sanctions appeared as the new political tool and weapon of influence. With the development of information technologies, under the influence of which the digital environment forms, the latter has become an arena of competition between the leading states in terms of information. In the digital environment, a system of challenges forms for the individual, society, and the state.

Consequently, cyber sanctions researchers defined as economic and financial measures aimed at changing the targets' behavior using malicious actions in cyberspace and/or intrusions.

On the other side, a cyber-blockade is a specially created situation caused by an attack on cyberinfrastructure or information systems, creating obstacles to a state's access to cyberspace and preventing the transfer of data beyond geographic boundaries.

The duration of a blockade is a secondary factor that matters only from the point of view of creating and achieving the desired effect. Information on many actors at different levels related to the role of anonymity, the speed of a cyber-attack, and the cost of cyber-blocking are required to analyze and evaluate the “cyber blockade” category. All this represents significant deviations from experience.

Ultimately, cyber blockades can be a tool of international relations and sanctions. They are an effective and inexpensive method of the counterparties’ access control to modern critical infrastructure facilities and can be implemented in such a way as to increase the anonymity of the perpetrators of the attack or plausible deniability, thus reducing the risk of retaliation.

2 LITERATURE REVIEW

The main sources related to our research problems are the works of Alison Lawlor Russell (2014) and William D. Bryant (2016). Russell's book stands out in this series as it is the first to examine the phenomena of blockade operations in cyberspace, which are large-scale attacks on infrastructure or systems that aim to prevent an entire state from sending or receiving electronic data. Cyber blockades can take place through digital, physical, and/or electromagnetic means, and their emergence in cyberspace has significant implications for international law and our understanding of cyber warfare.

In examining this topic, we analyzed a long list of sources and grouped them into several categories. The first group consists of works that aim to investigate sanctions as an economic and political leverage to pressure certain states. That includes publications by the United Nations, the Organization for Economic Co-operation and Development (OECD), the Organization for Security and Co-operation in Europe (OSCE), and others. Some notable examples include works by Golnoosh Hakimdavar (2014), Lee Jones (2015), and David Cortright and George A. Lopez (2018).

The second group includes papers that discuss the traditional and new domains of conflict, particularly cyberspace. The military researchers' approaches in defining the composition and structure of cyberspace we consolidated into a distinct sub-group. It includes articles by Y.I. Starodubtsev, P.V. Zakalkin, and S.A. Ivanov (2020), Kovalev, A. P., Sotnik, S. A., and Sotnik, D. S. (2023), which explores the main objectives of technosphere warfare and ways of achieving them. They formalize the notion of cyber weapons and formulate an approach to estimating their combat potential while also considering the main factors that condition the need to form specialized services of the Armed Forces intended for combat actions in cyberspace. The work of (Jones, 2015) is also noteworthy.

It is significant to note the use of developed models for each domain, such as the Model of Gaining and Utilizing Land Superiority, the Model of Gaining and Utilizing Maritime Superiority, the Model of Gaining and Utilizing Air Superiority, the Model of Gaining and Utilizing Cyberspace Superiority, Domain Superiority Model, Complete Model of Local Cyberspace Superiority, and others. The model proposed by M. Libicki (2007) should also be analyzed and utilized separately.

Political and economic sanctions were being used long before our time. The chapter "The History and Effectiveness of Economic Coercion" by author Irina Bogdanova (2022) in the monograph is of interest, as it provides a historical overview of the sanctions used in international law and the protection of human rights. The temporal coverage of the history of economic coercion spans ancient Greece, the Roman and Byzantine empires, the Middle Ages, World War I, the period between World War I and II, the Cold War, and so on.

An additional source for researching historical aspects is the following book (Askari, 2003), which presents the history of economic sanctions.

3 RESEARCH METHODOLOGY

In the economic and political confrontation realm, a wide range of sanction mechanisms find application. Let us briefly consider the composition of economic sanctions. Economic sanctions include three directions: unilateral, multilateral by the UN or groups of countries, and new "smart" sanctions.

Unilateral sanctions include export sanctions (embargo); sanctions against import boycotts/tariffs and freezing diplomatic relations.

Multilateral sanctions by the UN or groups of countries include sanctions against arms trade (targeted/strategic sanctions), "comprehensive" sanctions (which are complemented by financial sanctions) and freezing of diplomatic relations.

"Smart" sanctions include financial sanctions and asset and investment freezes. Economic sanctions can have any objective combination (Alexander, 2009): modification of the target's behavior, retaliation, or punishment, or as a signal to the target or other third countries.

The "Global Sanctions Data Base (GSDB)" provided a classification of sanctions (Felbermayr, Kirilakha, Syropoulos, Yalcin, & Yotov, 2020). GSDB covers 729 publicly tracked, multilateral, plurilateral, and purely bilateral sanctions from 1950 to 2022 (GSDB-R3, 2023). In addition, GSDB classifies these sanctions based on three significant aspects. Firstly, by the type of sanctions considered (e.g., trade, financial, travel sanctions, etc.). Secondly, the political objectives behind the observed sanctions. In particular, the GSDB system groups the sanctions objectives into separate categories (e.g., policy change, regime destabilization, prevention of war, human rights, etc.) of registered policy objectives. Thirdly, the perceived degree of success for each identified sanction is covered by five categories ranging from unsuccessful sanctions to the full agreement by the target with the sender's demands.

GSDB defines sanctions as mandatory restrictive measures applied by individual countries, groups of countries, the United Nations, and other international organizations to eliminate violations of international norms. The final objective is to encourage target countries to change their behavior or limit their actions. GSDB classified sanctions according to three crucial parameters: the type, objectives, and success.

GSDB classifies sanctions by type into five categories covering trade, financial activity, arms, military aid, travel, and another category called “other sanctions”. The database also classifies sanctions based on their political objectives which include changing policies, destabilizing regimes, preventing wars, and promoting human rights, etc.

Lastly, the GSDB categorizes sanctions based on their perceived success degree, ranging from unsuccessful to fully achieving the sender's demands.

Overall, sanctions are a general tool used in economic and political conflict to modify the behavior of the target, seek revenge or punishment, or send a signal to the target or third-party countries. They can take various forms, including export sanctions, import boycotts/tariffs, asset freezes, investment freezes, etc. The GSDB provides a comprehensive classification of sanctions based on their type, political objectives, and perceived degree of success.

Table 1. Sanction types and impacted groups.

Type	Groups likely to be affected
Trade	• Export sanctions: producer groups and exporters harmed. Multiplier effects are likely in intermediate sectors. • Import sanctions: consumer groups (e.g. urban middle classes) and sectors reliant on imports harmed; import-competing industries may benefit. Embargoes on key commodities like oil may raise costs economy-wide. • Smugglers may receive windfall gains. • State agencies reliant on trade taxation may be harmed; revenues may also suffer if trade losses depress overall economic activity. • If sanctions cause exports to fall below imports, creating a balance of payments deficit, government intervention to depress import demand could slow economic activity, with further consequences.
Investment	• In the short term, local capitalists benefit because they may acquire departing foreign firms' assets cheaply, and since capital becomes scarcer, its returns increase. • In the longer term, lack of investment, technology transfer, and foreign expertise may depress productivity, profits, growth, and employment opportunities, particularly for skilled workers. Economy-wide multiplier effects are likely. • State apparatuses may be harmed directly if investment is an important source of foreign exchange, and indirectly if stunted growth damages tax revenues. • Disinvestment may depress demand for, and thus the value of, the local currency, depressing importers' purchasing power and increasing foreign debt repayment costs for both private and public borrowers
Aid and Finance	• Directly harms groups dependent on external aid/finance, e.g. for livelihoods or investment capital. Possible multiplier effects. • Directly harms state apparatuses dependent on overseas aid and loans; and indirectly the sectors upon which these resources would be spent.
Assets	• Harms those with assets frozen and their dependents.
Monetary (currency manipulation)	• Importers, exporters, and consumers (private and public) suffer from price volatility and alterations in buying power. • Private and public borrowers with foreign-denominated loans face higher repayment costs. • The government may suffer an ideological blow if the national currency has ideological resonance. • Non-tradable or subsistence sectors will be less affected.
Arms	• May constrain the state's capacity for war or domestic coercion. • As with import embargoes more generally, potential windfall gains for domestic producers and smugglers.

Source: Lee Jones (2015, p. 44)

4 ANALYSIS

4.1 Domains/Types of Blockades

Not so long ago, humanity only had two physical domains - land and sea - each with different physical characteristics. People could only explore the sea with the help of specific technologies such as sailboats, steamships, and nuclear submarines. People used land only with the help of technical tools such as wheels, plows, and so on. Significant changes occurred a century ago when a third physical domain appeared - aerospace. The launch of the first satellite in 1957 added a new domain - outer space. The development of the computer and communication technology industry and the creation of state and private information systems and networks served as the basis for another domain formation - the information domain. That created the prerequisites for the formation of cyberspace.

Figure 1 shows the interconnection of physical domains.

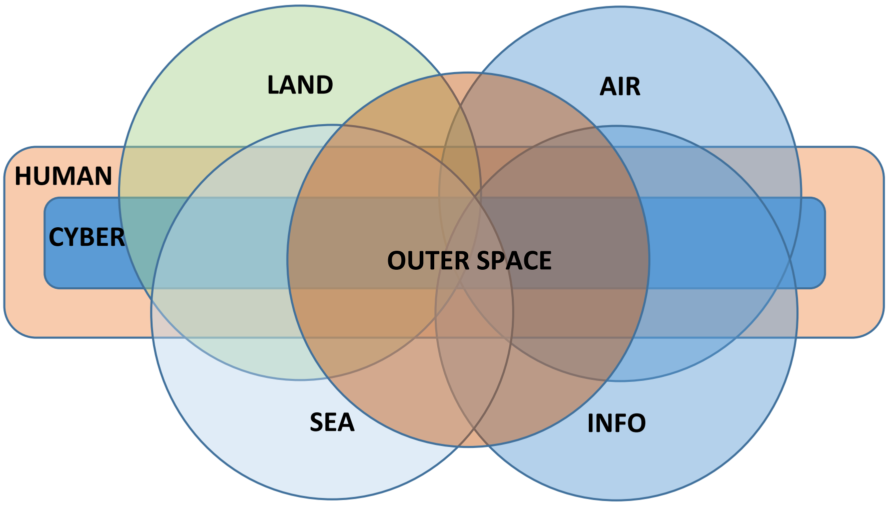

Figure 1 Domains Interconnections.

Source: Author's original work

Over time, a whole set of categories related to this domain appeared in common use - cybersecurity, cyber terrorism, cyber violence, cyber aggression, cybercrime, cyber victimization, cyber war, cyber defense, cyber-attack, cyber boycott, cyber blockade, cyber sanctions, computer zombie, cascade weapons, electronic bomb, and others.

It is to point out that the new domain is influential and has a very strong connection with all the others. Once technology is applied to every area of human life, these connections create significant dependencies between all domains. Moreover, this means that when affecting one domain, others will be affected also.

A very significant aspect in the domain and cross-domain confrontation is humans. Countries must use their people to overcome the challenges of being outnumbered, outdistanced, but mainly "outlearned" by adversaries. In the context of cyberspace management, agile and adaptive development through education and training is crucial to keep pace with the rapidly developing technical, technological, economic, and social aspects of life.

4.2 Cyberspace – a New Arena of Conflict

Recently, a sixth domain was added - cyberspace. Analysts propose numerous definitions for cyberspace, including one that describes it as a virtual environment in which digital information transmits over computer networks. Another definition is that cyberspace is a global domain within the information environment, consisting of interdependent information network infrastructures with stored and circulating data, including the Internet, data transmission networks, computer systems, and the processors and controllers used (Joint Staff, 2018). A review of several definitions of cyberspace has been conducted by Kuehl (2017). However, the author notes that over time, this category will change and become more specific depending on the rapidly developing technical, technological, economic, and social aspects of our lives. Other definitions include:

1. Electronic (including photo-electronic, etc.) environment through which information is created, transmitted, received, stored, processed, and destroyed (Godwin III, Kulpin, Rauscher, & Yaschenko, 2014).
2. A global area of the information space that represents an interconnected network of information system infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors, and controllers (JP 1-02, 2019).
3. A complex environment that enables interaction between people, software, and services using globally distributed devices and information and communication technology networks (Cybersecurity, 2012).

4. Software that operates in computer devices, information that is stored (and transmitted) in these devices, or information that is created by these devices. The equipment and buildings in which these devices are located are also part of cyberspace (ITU-T Recommendation X.1121, 2004).

A more precise definition of cyberspace is given in. Cyberspace is an artificial, heterogeneous technological system with a multitude of operational and technological management organs at various levels. The process of creating and operating this system is not predetermined by the requirements of a single management system but operates in the interests of various heterogeneous, including antagonistic, management systems. The properties depend both, on the characteristics of its elements and the volume and properties of the processes implemented in the interests of internal and external consumers.

Many experts consider this new domain from the perspective of a new sphere of armed conflict. Naturally, we are interested in actions related to the implementation of a blockade in this new domain - a cyber blockade. A cyber blockade is a specially created situation caused by an attack on the cyberinfrastructure or information systems that prevents a state's access to cyberspace, thereby preventing the transmission of data beyond its geographical borders.

It should be noted that there is a significant difference between a cyber-blockade and censorship or other forms of internal control that exist in government management practice. In this case, the government does not allow certain information to be obtained or transmitted, usually for reasons of internal stability. The cyber blockade must be effective in preventing the transmission of information, and the duration of the blockade is a secondary factor that only matters in terms of creating and achieving the desired effect. For example, a blockade that lasts only a few fractions of a second will have relatively little significance, but a blockade during a critical time (such as election day) or one that lasts for several weeks or months can be considered highly effective depending on the goals. As with a naval blockade, maintaining a cyber-blockade for a predetermined period is not mandatory. The important thing is the ultimate effectiveness of the blockade in achieving the desired goals.

Table 2. Similarities among Blockade Operations in Six Different Domains

	Maritime	**Aerial**	**Land**	**Space**	**Info**	**Cyber**
Actions	Prevent ingress/egress of ships or craft to or from ports or harbors	Prevent aircraft from entering airspace or No Fly Zone (NFZ)	Prevent entry to or exit from a specific city or region	Prevent entry into outer space	Prevent the transmission of information beyond national borders	Prevent the transmission of data beyond borders
Actors	States, independent territories	States, independent territories	States	States	States	States, non-state actors, individuals
Capabilities	Superior maritime capabilities; knowledge of the domain and opponent's vulnerabilities	Superior aerial capabilities; knowledge of the domain and opponent's vulnerabilities	Superior land capabilities; knowledge of the domain and opponent's vulnerabilities	Superior technological or economic capabilities; knowledge of opponent vulnerabilities	Historically sea-based capabilities to interfere with cables, knowledge of the domain, and opponent's vulnerabilities	Technological capability; knowledge of the domain and opponent's vulnerabilities
Presence of conflict	War or extant conflict	War or extant conflict	War	War or extant conflict	War	War or extant conflict
Role of neutrals	Rights protected	Rights protected	Rights protected	Rights protected	Rights protected	Neutrals are not specifically targeted, but consequences are difficult to predict

Source: (Russell, 2014, pp. 81, 184)

The following table provides a comparison of blockade operations in all domains.

It is considered necessary to provide the main conclusions drawn from the analysis of the category of cyber blockade presented.

Cyberspace is a physical network that can be manipulated to punish a counterparty by obstructing their access to the data flow necessary for security and prosperity. At the same time, cyber-blocking is an effective means of denial or hurdle of access to cyberspace.

A cyber blockade is a situation caused by an attack on cyberinfrastructure or systems that prevent government structures from accessing cyberspace, thereby preventing data transfer (input-output) beyond geographical boundaries. Cyber blockade is a legitimate tool of international state management and, like other types of blockades, can be considered an act of war (although ultimately the target state decides whether it wants to consider it as an act of war and potentially escalate the situation). Cyber blockades target entire states and attempt to cause mass disruptions in the functioning of critical infrastructure elements. The goal of the cyber blockade is to prevent the transfer of data beyond geographical boundaries by manipulating, controlling, or dominating cyberspace and related technologies to cause political, economic, social, or psychological harm to the opponent.

Actors use cyber blockades as a tool for international relations and sanctions as they are an effective and inexpensive method of controlling the opponent's access to modern networks. Moreover, that tool can be deployed with increased anonymity or enabling plausible deniability, thus reducing the risk of retaliation. In addition, there are alternative options for achieving the same result, especially for non-state actors.

States, proxy groups, non-state actors, or individuals can conduct cyber blockades if they have the resources and opportunities. However, non-state groups can also introduce a cyber-blockade if they possess the necessary technical skills to plan and coordinate a large-scale cyber-attack, targeting entire states. Physical attacks on cyber infrastructure require limited resources and expertise; at a minimum, perpetrators must be able to detect and destroy key cyberinfrastructure. Electromagnetic attacks are usually part of state warfare and require significantly more resources to achieve. Thus, depending on the cyber blockade scenario (through digital, physical, or electromagnetic attacks), the capabilities and resources to conduct a cyber-attack can vary from relatively low (physical destruction of cables or terminals) to high and very high (electromagnetic attacks).

Cyber blockades can affect all aspects of cyberspace technology, including power grids, power stations, landline phone services, mobile phone services, financial systems, and so on. Cyber blockades, like other blockades, are essentially non-violent, but they can result in damage, destruction, or death depending on their implementation scenarios and impact on targets. Targets classified as "limited" under international law, such as hospitals, will still be limited in cyberspace.

Cyber blockades can be efficient tools for achieving specific goals, but they are not always the preferred option for actors. Depending on the goals and circumstances, decision-makers may choose more specialized cyber-attacks that can achieve more precise and sophisticated results (e.g. espionage or the destruction of specific systems) while maintaining the integrity and security of other systems.

Cyber-blockades can be established relatively quickly and at a low cost, depending on the method of attack used.

Cyber-blockades are technically feasible against any country. However, they are easier to achieve against smaller countries. Developed countries usually have more connections to the cyber domain, creating a more resilient network of connections between that country and other countries.

Cyber blockades can be seen as a subset of information blockades because they are aimed at the transmission of information. However, information blockades have not received wide recognition, so this classification may not be the most useful for policymakers. In addition to being a subset of information blockades, cyber blockades should also be considered separately as they may occur in a specific domain. Therefore, cyber blockades can affect both individual domains and/or a subset of information domains, affecting two or more domains.

Cyber-blockades may exist, but they should not always be considered acts of war. Depending on the circumstances and context, which is crucial, a cyber blockade may be considered a complete blockade. However, a peaceful blockade is a form of coercive diplomacy, in which the blocking state declares that it does not seek to provoke war but rather to compel the blockaded state to yield to its demands. It is highly likely that at some point soon, the international community will attempt to introduce cyber blockades as a form of sanction against states that violate international law.

The increase in the number and diversity of actors in cyberspace creates repudiation challenges and enables attacks from anonymous platforms. Instead of relying on a traditional deterrence model, which may be insufficiently effective in cyberspace, states must focus on creating reliable information protection and backup systems.

Public-private partnerships are particularly important for cyber-blocking because the cyber domain is not purely public - it is owned and mainly managed by private corporations or individuals. At the same time, governments are tasked with protecting it as part of critical national infrastructure. Other types of blockades have affected the private sector to varying degrees (such as commercial ships, commercial airplanes, or even telegraph cables), but cyber blocking represents the first case where public and private interests are much interconnected.

As the topology of cyberspace and its actors change, so do the capabilities and vulnerabilities associated with cyber blockades. Technological progress reduces vulnerabilities in some areas, while changes in cyberspace itself are likely to uncover new vulnerabilities that cyber-threat actors will exploit.

5 CONCLUSIONS

Analysis of the impact of the sanctions (traditional and new "smart" ones) using institutional, economic, and cultural dimensions of processes that have been observed recently indicates the transformation of the "war-prevention tool" into a weapon of geo-economic warfare.

In other words, the mechanisms of sanctions and blockades can be followed through an assessment of the internal economic contradictions that have intensified, as well as between leading states. Sanctions reinforce and increase the contradiction between transnational capital and national labor; sanctions can disconnect the target state from global value chains, lowering its economic and fiscal capabilities; Sanctions can increase the contradiction between freedom and domination and push the population to government opposition, which inevitably takes repression measures to democratic tendencies in society and enforces its control over strategic sectors of the economy.

In conclusion, cyber blockades and cyber-restricted zones are serious problems in the modern world. They imply threats to national security, commercial interests, and freedom of expression. Therefore, states should develop reliable information protection and reservation systems, as well as establish public-private partnerships to effectively combat cyber threats.

However, as cyberspace topology and actors change, so do the opportunities and vulnerabilities associated with cyber blockades. Therefore, it is necessary to constantly improve and update protection systems and apply modern technologies for more effective counteraction against cyber threats.

WORKS CITED

Alexander, K. (2009). *Economic Sanctions: Law and Public Policy.* Palgrave Macmillan.

Askari, H. (2003). *Economic Sanctions: Examining Their Philosophy and Efficacy.* Praeger Publishers.

Bogdanova, I. (2022). *Unilateral Sanctions in International Law and the Enforcement of Human Rights: The Impact of the Principle of Common Concern of Humankind.* World Trade Institute Advanced Studies.

Bryant, W. D. (2016). *International Conflict and Cyberspace Superiority: Theory and Practice.* Routledge Cybersecurity. Retrieved from ISO/IEC 27032:2012. Retrieved 01 16, 2024, from International Organization for Standardization: https://www.iso.org/

Cortright, D., & Lopez, G. (2018). *Economic Sanctions. Panacea or Peacebuilding in a Post-Cold War World?* Taylor & Francis Group.

Felbermayr, G., Kirilakha, A., Syropoulos, C., Yalcin, E., & Yotov, Y. V. (2020, May 30). *WP 2020-02 The Global Sanctions Data Base.* Retrieved from Drexel University: https://drive.google.com/file/d/11djwEIr96SFt6YpMzo9gaB6ZJrOer8AX/view?pli=1

Godwin III, J. B., Kulpin, A., Rauscher, K. F., & Yaschenko, V. (2014). *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations.* US: New York and RF: Moscow: EastWest Institute and the Information Security Institute of Moscow State University.

GSDB-R3. (2023, Jun). *The Global Sanctions Data Base (GSDB) - Version 3, published in June 2023*. Retrieved from The Global Sanctions Data Base (GSDB): https://www.globalsanctionsdatabase.com/#Data

Hakimdavar, G. (2014). *A Strategic Understanding of UN Economic Sanctions International Relations, Law, and Development.* Taylor & Francis Group.

ITU-T Recommendation X.1121. (2004, Apr 29). *Series X: Data Networks and Open System Communications: Telecommunication security.* Retrieved from International Telecommunication Union: https://www.itu.int/rec/T-REC-X.1121/en

Joint Staff. (2018, Jun 08). *Cyberspace Operations.* Retrieved from Joint Publication 3-12: https://irp.fas.org/doddir/dod/jp3_12.pdf

Jones, L. (2015). *Societies Under Siege. Exploring How International Economic Sanctions (Do Not) Work.* Oxford University Press.

JP 1-02. (2019). *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication. Retrieved from https://irp.fas.org/doddir/dod/jp1_02.pdf

Kovalev, A., Sotnik, S., & Sotnik, D. (2023, Mar 03). Kovalev, A. P. (2023, 3). Space as a new sphere of armed struggle. Military Thought,. *Voyennaya Mysl*, 35-54. Retrieved from https://vm.ric.mil.ru/upload/site178/lCmCpEOiWw.pdf

Kuehl, D. T. (2017). Chapter 2: From Cyberspace to Cyberpower: Defining the Problem. In *Cyberpower and National Security* (p. 17). Washington, D.C.: National Defense University Press. Retrieved from http://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSP-Exports/Cyberpower/Cyberpower-I-Chap-02.pdf?ver=2017-06-16-115052-210.

Libicki, M. (2007). *Conquest in Cyberspace: National Security and Information Warfare.* New York: Cambridge University Press.

Russell, A. (2014). *Cyber blockades.* Georgetown University Press.

Starodubtsev, Y., Zakalkin, P., & Ivanov, S. (2020). Technosphere War as the Main Way of Conflict Resolution in the Context of Globalization. *Military Thought* (10), 16-21.