New Forms and Features of Cyber Confrontations

Serghei Ohrimenco[1], Valeriu Cernei[2]

[1]Information Security Lab, Academy of Economic Studies of Moldova, Chisinau, Moldova
[2] Partner, IT Audit & Advisory, BSD Management SRL, Chisinau, Moldova
osa@ase.md, valeriu.cernei@bsd.md

Abstract. The evolution of the cyberspace domain and its accompanying management tools has ushered in an era characterized by the emergence of new forms of confrontation: cyber blockades and cyber sanctions. This development has paved the ways for enhanced capabilities in economic management, the expansion of diplomatic and trade relationships, and ultimately, the safeguarding of national interests at an unprecedented level. This paper presents the results of an analysis of these new categories, elucidating their interconnectedness, and highlighting the evolution and continued development of these two domains, particularly within cyberspace. The authors draw attention to the new dimensions of confrontation within the cyberspace realm, encompassing explicit and hidden threats to individuals, society, and the state.

Keywords: Cyberspace domain, Cybersecurity, Cyberconflict, Cybersanction, Cyber threats

1. Introduction

The interactions between users, information systems, and their components can traverse several distinct stages: cooperation, integration, competition, and confrontation. It is noteworthy that these stages span across various domains, including political, military, economic, technological, social, and ideological. Interaction and confrontation manifest themselves at multiple levels, encompassing the global, strategic, tactical, and individual spheres. The significance of this topic is greatly magnified in the context of each nation's quest to safeguard its national interests concerning cybersecurity [1]. A crucial observation arises from [2, 3], emphasizing the unique characteristics of the cyberspace domain when compared to other domains.

Firstly, cyberspace is a product of human creation. Secondly, military and civilian (diplomatic, trade, etc.) capabilities in other domains are managed through and by means of the cyber domain. Thirdly, distinguishing between military and civilian aspects of cyber operations is often challenging and occasionally impossible due to their intricate intertwinement. Fourthly, attributing operations conducted within cyberspace is an exceedingly complex endeavor (Fig.1).

Not too long ago, humanity recognized only two domains, namely land and sea. However, with the relentless advancement of science and technology, new domains such as aerospace, information, and most recently, cyberspace have emerged. It is imperative to fundamentally reevaluate the system for managing cyber risks in these new conditions [4-8].

2. Literature Overview

It is important to acknowledge that the first and the most comprehensive work on the subject of cyber blockades can be found in the works of [9-10], and [11]. A. Russel, in

particular, deserves commendation for spearheading the establishment and exploration of issues pertaining to the introduction and assessment of cyber blockades.

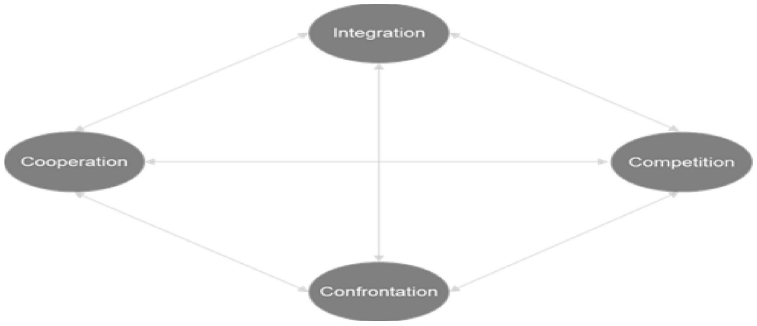

Fig. 1. Users-Systems interaction stages

The literature utilized in the preparation of this material can be categorized into several groups. Firstly, there are sources that analyze and elucidate the issues surrounding the genesis and subsequent development of domains, including cyberspace [5]. In [12], conflicts within cyberspace are dissected, with a particular emphasis on topics ranging from "Cyber Threats to Cyber Risks" to empirical analyses of cyber conflicts. Another noteworthy source is Nicholas Michael Sambaluk's book [1], which delves into facets of 21st-century technology. It elucidates how the United States and the Soviet Union sought to explore and exploit the space domain to advance national security goals, including intelligence data collection, communications, and guidance.

Secondly, there is an examination of the mechanisms underpinning political and economic confrontation – sanctions (unilateral, multilateral, and "smart" sanctions) [13]. In the book [14], sanctions are portrayed as an increasingly popular tool of foreign policy, not only at the multilateral level (within the UN) but also regionally (notably within the EU) and unilaterally. The book scrutinizes the contemporary practices of various actors and delves into the legality (or lack thereof) of their actions. In the subsequent book [15], the utilization of targeted sanctions as a central instrument to address challenges to international peace and security is discussed, which has become a defining feature of UN Security Council practice. [16], delves into the fundamentals of the concept of economic statecraft, as well as alternative concepts such as Foreign Economic Policy, International Economic Policy, Economic Diplomacy, Economic Leverage, Economic Sanctions, Economic Warfare, Economic Coercion, and more.

Thirdly, there are important theoretical developments of a politico-economic nature [17-20]. Among them, specific chapters in the book [21] stand out. These include Chapter 22, "Economics of Conflict: An Overview" (authored by Michelle R. Garfinkel and Stergios Skaperdas), and Chapter 27, "The Political Economy of Economic Sanctions" (written by William H. Kaempfer and Anton D. Lowenberg). The next important source [22] acknowledges that there can be no simple equation that reveals whether or not sanctions will be successful.

3. Research Methodology

The methodological approach adopted in this publication is grounded in a systemic perspective, wherein the research object is viewed as a system comprised of interconnected elements and a complex interplay of entities with their respective attributes and relationships.

The research concept was formulated, key objectives were defined and scrutinized, and statistical data was collected from monographic sources and companies' reports. This gathered information was subsequently subjected to an analysis employing game theory, econometric analysis, and modeling techniques.

Documents from the World Economic Forum [23-25], notably "The Global Risks Report 2023," underscore that the upcoming decade (2023-2030) will be characterized by a series of crises. A new term, "polycrisis," has been coined, denoting a scenario, where various risks intersect, and their interdependencies become acutely palpable. "Old" risks have evolved, including inflation, cost-of-living crises, trade disputes, social unrest, geopolitical tensions, and more. In tandem with these traditional risks, new challenges have arisen, encompassing high levels of government debt, diminished investments, deglobalization, and other factors. All of this underscores the necessity to reevaluate the mechanisms for assessing the impact of sanctions and conflicts in the cyberspace domain.

4. Analysis

As a result of the comprehensive analysis conducted, several key terms related to cyber blockades and its components interaction have been delineated and are presented further.

Cyberspace: This term encapsulates a physical network that can be used and manipulated to apply punitive measures against targets by obstructing their access to the data flow critical for both, security and prosperity.

Subjects: These actors utilize cyber blockades as instruments of international relations and sanctions due to their effectiveness and cost-efficiency in controlling the targets' access to modern networks. They can be executed in a manner that enhances the perpetrator's anonymity or deniability, thereby reducing the risk of retaliation. Additionally, various alternative courses of action can be employed to achieve similar results, particularly for non-state actors.

Cyber Blockade: A state arising from an attack on cyber infrastructure or systems that obstructs user access to cyberspace, and so impeding data transmission beyond geographical borders. Cyber blockades are recognized as legitimate instruments of international statecraft, and in accordance with other forms of blockades, may be considered acts of war (though the target state ultimately decides whether to classify them as acts of war and potentially escalate the situation). Cyber blockades are directed at entire states and usually seek to induce disruptions within critical infrastructure elements. Their primary objective is to prevent the transmission of data across geographical borders through the manipulation, control, or domination of cyberspace and associated technologies, causing political, economic, social, or psychological harm upon the adversary.

Effectiveness of Cyber Blockades: The success of a cyber blockade consists on its ability to prevent information transmission. The duration of the blockade is a secondary consideration, relevant only in terms of achieving the desired outcome. For instance, a blockade lasting some seconds may hold relatively little significance, while a blockade occurring in a critical moment (such as on an election day) or one persisting for several weeks or months can be highly effective, contingent on the objectives. Analogous to maritime blockades, maintaining a cyber blockade for a pre-defined period is not obligatory. What assumes paramount importance is the ultimate effectiveness of the blockade in realizing the stated goals.

To assess the trajectories of cyber warfare, the work presented by a consortium of authors from the RAND Corporation [26] offers valuable insights. Future war trends are delineated across several dimensions: geopolitical trends, military trends, space and nuclear trends, cyber trends, and deterrence trends. The analysis of information points to a complete

alignment of targets across all trends that the United States is anticipated to counter. These encompass Russia, China, North Korea, and Iran, in addition to non-state actors. This implies a complex array of questions, including the responses the United States has contemplated in reaction to cyber compromises of state information systems, whether past responses have substantially influenced the adversary's behavior, and how analogous incidents should be addressed in the future. Answers to these inquiries should be sought in forthcoming research endeavors.

5. Discussion

The new segment of the discussion focuses on the organization and execution of sanctions within the cyberspace domain, an area yet to be fully explored. Specifically, the new political and economic instrument, as well as a new means of exerting influence, has emerged: cyber sanctions. With the development of IT components that have shaped the digital landscape, cyberspace has evolved into a competitive arena among leading information-oriented nations and foremost producers of computer hardware and software. A constellation of challenges concerning the digital environment, spanning individuals, society, and states, has arisen [27-30].

Cyber sanctions are defined as economic and financial measures aimed at affecting behavioral change in target entities through malicious activities in cyberspace and/or intrusions [31-33]. An analysis of the theory and practice of interactions among various entities within the cyber sphere underscores that the concept of cyber sanctions represents a relatively new area of research within the global cyberspace domain.

Cyber sanctions, as a relatively new instrument of Governments, are likely to see increased use in the future. Governments and international organizations may refine their strategies for imposing cyber sanctions, potentially developing more standardized protocols and frameworks for their application. This could include defining clear criteria for when cyber sanctions are warranted and specifying the range of potential responses.

Moreover, as cyberspace becomes increasingly interconnected with critical infrastructure, the consequences of cyber sanctions could become even more profound. Governments already seek to impose sanctions that directly impact a target nation's critical infrastructure, such as its energy grid or financial systems. This raises complex ethical and humanitarian questions about the collateral effects of such sanctions on civilian populations.

Another important topic is the one related to future evolution of cyber blockades. As technology continues to advance, the nature and effectiveness of cyber blockades are likely to evolve. The integration of artificial intelligence, quantum computing, and autonomous systems into cyber operations may open up new frontiers in cyber warfare. These advancements could potentially lead to more sophisticated and stealthy cyber blockades, making them even harder to detect and mitigate.

The source attribution problem in cyberspace is expected to persist. Accurately identifying the source of a cyber blockade remains a complex challenge, and as state and non-state actors become more adept at concealing their origins, the difficulty of attributing cyberattacks will continue to pose diplomatic and strategic challenges.

Another direction of discussions is the global cooperation and norms in the cyberspace. The escalating use of cyber blockades, cyber sanctions, and cyberattacks in international conflicts lowers the pressing need for global cooperation and the development of norms in the cyberspace. The international community will likely intensify efforts to establish rules of behavior in cyberspace, similar to existing norms in conventional warfare. Building consensus on these matters will be challenging but vital for maintaining stability in the cyberspace.

And finally, the role of non-state actors would be crucial. Non-state actors, including hacktivist groups and cybercriminal organizations, are becoming increasingly influential in cyberspace. These groups can carry out disruptive actions independently or on behalf of state actors, blurring the lines between state-sponsored and non-state cyber activities. In the future, their roles in cyber blockades and cyber sanctions may grow, making it essential for governments and international organizations to develop strategies for dealing with these entities effectively. This includes enhancing cybersecurity measures to defend against attacks from both state and non-state actors.

6. Conclusion

The comparison of the impact of cyber blockades and sanctions suggests a fundamental transformation, transforming the "tool of war prevention" into a weapon of geo-economic warfare, accompanied by its attendant consequences. The achievement of declared political objectives now predominantly relies on the utilization of economic instruments, at times severe, and in some cases, even harsh measures.

In other words, the effectiveness of sanctions and blockades can be traced through the assessment of a complex set of indicators characterizing the contradictions of capital, which have intensified within leading global powers and between them.

Sanctions increases the contradiction between transnational capital and national labor. The reduction in real incomes among the most vulnerable societal groups threatens stable consumption and augments the demand for government expenditures. Simultaneously, channels of financing labor reproduction through borrowing in global financial markets constrict due to a "denial of any credit, credit guarantees, or other financial assistance."

The intricate interplay between cyber blockades, sanctions, and global capital underscores the evolving landscape of international relations and conflicts, with cyberspace occupying a pivotal role in reshaping the dynamics of modern warfare and diplomacy. This paradigm shift requires ongoing research and analysis to comprehend the full spectrum of implications and devise effective strategies for an increasingly interconnected world.

In conclusion, the evolution of cyber blockades and cyber sanctions is an ongoing and dynamic process. As technology continues to advance and cyberspace becomes increasingly integral to all aspects of modern life, the impact of these measures will likely intensify. Policymakers, cybersecurity experts, and international stakeholders must remain vigilant and adaptive in their efforts to navigate this complex and ever-changing landscape. This involves not only responding to current challenges but also proactively shaping the future of cybersecurity and international relations in the digital age.

References

1. Sambaluk N.M. (2019). Conflict In the 21st -Century: The Impact of Cyber Warfare, Social Media, And Technology. ABC-CLIO, LLC. ISBN: 978-1-4408-6000-3
2. Brantly A. F. (2016). The Decision to Attack Military and Intelligence Cyber Decision- Making. University of Georgia Press.
3. Richard A. Clarke, Robert K. Knake (2019). The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. Penguin Press.
4. Pogrebna G., Skilton M. (2019). Navigating New Cyber Risks: How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age. Palgrave Macmillan.
5. Friis K., Ringsmose J. (2016). Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives. Routledge.
6. Saffady W. (2020). Managing Information Risks: Threats, Vulnerabilities, and Responses. Rowman & Littlefield.

7. Andersen T. J. (2016). The Routledge Companion to Strategic Risk Management. Routledge.
8. Oh K.-B., Ho B., Slade B. (2022). Cybersecurity Risk Management; An Enterprise Risk Management Approach. Nova Science Publ. ISBN 978-1-68507-505-7, https://doi.org/10.52305/TNSD3712
9. Russell A. L. (2014). Cyber blockades. Georgetown University Press.
10. Russell A. L. (2015). Strategic anti-access/area denial in cyberspace. 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. doi:10.1109/cycon.2015.7158475
11. Russell A. L. (n.d.). The Physical Layer. Strategic A2/AD in Cyberspace, 26–39. doi:10.1017/9781316817001.003
12. Whyte Ch., Thrall A.T., Brian M. Mazanec B. M. (2020). Information Warfare in the Age of Cyber Conflict. Routledge.
13. 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..
14. Happold M., Eden P. (2016) Economic Sanctions and International Law: Studies in Int. Law. Hart Publ. 7
15. Biersteker T. J., Eckert S. E., Tourinho M. (2016). Targeted Sanctions: The Impacts and Effectiveness of United Nations Action. Cambridge University Press.
16. Baldwin D. A., Kapstein E. B. (2020). Economic statecraft. Princeton University Press.
17. Kirkham K. (2022). The Political Economy of Sanctions: Resilience and Transformation in Russia and Iran. Palgrave Macmillan.
18. Karatzogianni A. (2006). The Politics of Cyberconflict. Routledge.
19. Jasper S. (2012). Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security. Georgetown University Press.
20. Laurent S. Y. (2021) Conflicts, Crimes and Regulations in Cyberspace. ISTE Ltd, John Wiley&Sons
21. Sandler T., Hartley K. (2007). Handbook of Defense Economics: Defense in a Globalized World. vol.2, North Holland.
22. Jaeger M. (2018) Coercive Sanctions and International Conflicts: A Sociological Theory. Routledge
23. The Global Risks Report 2023. 18th Edition. https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
24. Digital Safety Risk Assessment in Action: A Framework and Bank of Case Studies. May 2023. https://www3.weforum.org/docs/WEF_Global_Coalition_Digital_Safety_Risk_Assessments_2023.pdf
25. Chief Risk Officers Outlook. July 2023. https://www3.weforum.org/docs/WEF_Chief_Risk_Officers_Outlook_2023.pdf
26. Raphael S. Cohen R. S., Chandler N., Efron S, Frederick B., Han E., Klein K., Morgan F.E., Rhoades A. L., Shatz H. J. (2020). The Future of Warfare in 2030. RAND Corp. ISBN: 978-1-9774-0295-0
27. Ohrimenco S., Cernei V. (2021). Shadow Digital Technologies Threats to National Security. Int. Sc. Conf. on Economic and Social Development "Economics, Management, Finance and Banking". Svishtov, 28-30 Sept. 2022, pp. 344-350. https://www.zbw.eu/econis-archiv/handle/11159/12318
28. Ohrimenco S., Borta G., Cernei V. (2021) Estimation of the Key Segments of the Cyber Crime Economics. 2021 IEEE International Conference on Problems of Info communications. Science and Technology PIC S&T '2021. Oct. 5-7, 2021. Kharkiv, Ukraine. DOI: 10.1109/PICST54195.2021
29. Lehto M., Neittaanmäki P. (2018). Cyber Security: Power and Technology. Springer Int. Publishing
30. Maurer T. (2018). Cyber Mercenaries: The State, Hackers, and Power. Cambridge University Press.
31. Miadzvetskaya Y. (2020). Challenges of the Cyber Sanctions Regime under the Common Foreign and Security Policy (CFSP). In: Security and Law Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Intersentia, pp. 277-298. DOI: 10.1017/9781780688909.012
32. Bossler A. M. (2019) Perceived Formal and Informal Sanctions on the Willingness to Commit Cyber Attacks Against Domestic and Foreign Targets, Journal of Crime and Justice, 42:5, 599-615, DOI: 10.1080/0735648X.2019.1692423
33. Walentek D., Broere J., Cinelli M., Dekker M., Haslbeck J. (2021): Success of Economic Sanctions Threats: Coercion, Information and Commitment, International Interactions, DOI: 10.1080/03050629.2021.1860034