Acta Universitatis Danubius
RELATIONES INTERNATIONALES

Hybrid Security in the Post-Modern Era: Challenges and Responses in International Relations

Andreea-Loredana Tudor[1]

Abstract: The contemporary international system faces a variety of security threats in the context of an international dynamic that is in constant change. Moreover, we can note the existence of economic interdependence, multipolarity and accelerating technological progress. Thus, the international society is faced with complex security challenges, including hybrid threats, escalating cyber conflicts, intensifying geopolitical competition and increasing vulnerabilities associated with climate crises and social instability. The transitional space between peace and war has expanded, transforming into a zone of unconventional conflict, characterized by threats such as propaganda, cyber-attacks and disinformation. Asymmetric practices adopted by certain states generate an intensification of concerns at the international level, determining an acute need for cooperation between state and non-state actors, with the aim of building a common front against hybrid threats. The concept of hybrid security has developed as a specific response to the postmodern era, aiming to combat conventional and unconventional attacks in a highly interconnected international system. This research aims to analyse, through a multidisciplinary approach, the reactions of the international community to such challenges, as well as the main instruments developed by leading global actors, such as the European Union and the North Atlantic Treaty Organization, in managing them. Also, through the scientific research carried out, the main types of hybrid threats are identified and examined, approached through the prism of classical theories of international relations. Finally, the article discusses aspects related to global governance in the context of a multipolar world and explores possible responses, both from a theoretical and applied perspective, to the stated security challenges. This scientific approach contributes to a

[1] PhD, Lecturer, "Dunărea de Jos" University of Galati, Romania, Address: 47 Domneasca Street, Galati, Romania, Corresponding author: andreea.tudor@ugal.ro.

deeper understanding of the adaptation and resilience mechanisms of the international system in the face of new forms of hybrid conflict.

Keywords: governance; hybrid warfare; hybrid security; resilience; proxy actors

1. Introduction

Although the 20th century has been characterized by the specialized literature (Kanwal, 2018, pp. 2-4) as the bloodiest century in history, and the Cold War brought much uncertainty and transformations to the international system, with the collapse of communism in Eastern Europe and the disappearance of the USSR, remarkable successes were recorded in this field. A new world order was established, characterized by the emergence of new international actors, the development of interdependencies on various levels and the establishment of unipolarism with the USA as the hegemon for the entire international system. However, the international system is facing paradigm shifts, the very concept of the nation-state undergoing transformations due to all the ethnic conflicts or insurgency movements (Murray & Mansoor, 2012, pp. 2-3).

The geopolitical dynamics have undergone numerous transformations, and depending on each period, the threats have been increasingly difficult to manage, demonstrating a fragility of the world order and the need for effective global governance, based on integrated dispute resolution mechanisms. So, if during the Second World War, totalitarian regimes justified aggression by exploiting ethnic and national rivalries, the bipolarity of the Cold War allowed the two superpowers, the USA and the USSR, to intervene by amplifying these tensions. Moreover, the very rivalry between the two superpowers shook the global order through tensions that led to the danger of a nuclear conflict (Ardemagni, 2024).

In the contemporary period, in an increasingly globalized world, security challenges or threats, as a result of interstate rivalry, no longer have only a conventional character. Today, their nature is diverse, of an economic, demographic, or societal nature. Moreover, the nature of the actors involved is different, with the emergence of non-state actors increasing, operating beyond the borders of states. Thus, state actors find themselves in the position of fighting against terrorist groups, cross-border crime networks or insurgent groups, which can cause regional or international instability. The digital revolution provides increased power to such groups, threatening security through cyber-attacks, propaganda or disinformation, making it

more difficult for states to protect their sovereignty and national security (Hartmann, 2017, pp.1-2).

The combination of conventional and unconventional techniques, capabilities and resources highlights the way certain states have operated in the last two decades. A hybrid approach of this kind is called by some specialists the "*fourth generation of warfare*" (Johnson et al., 2021, pp. 60-64). Some opinions claim that a number of states, for example, the USA, have been confident in the power of conventional force and, until recently, did not see the need to adapt measures to combat hybrid warfare. However, in accordance with the trends of state and non-state actors, hybrid warfare has become the main concern for states precisely because of tactics of this kind. Hybrid warfare represents a real threat, the seriousness of which is dictated precisely by its means of operation, by the diversity of actors, means and goals (Raugh, 2016).

The pursuit of national interests and the development of strategies by states such as the Russian Federation reflect the use of hybrid warfare as an effective tool to achieve geopolitical objectives. A telling example is the illegal annexation of Crimea by the Russian Federation in 2014, in violation of the territorial integrity of Ukraine and violation of international law, thus highlighting the potential of these tactics to destabilize the targeted regions. However, when the Russian Federation found that non-conventional methods were not sufficient to achieve its goals, it resorted to conventional military means, thus integrating conventional and non-conventional techniques. This strategic combination emphasizes the flexible and adaptable nature of hybrid warfare, making it a preferred option for achieving complex objectives in a dynamic international environment (Banasik, 2016).

2. Hybrid Threats - Brief Considerations

What exactly is hybrid warfare? After the illegal annexation of Crimea by the Russian Federation in 2014, the concept of hybrid warfare has gained increased attention in the specialized literature, becoming a priority subject of study. It is often described as characteristic of the 21st century, notable for its complexity. In parallel, hybrid threats have become an object of concern for both states and international and regional organizations, such as the United Nations, NATO and the European Union. Their efforts have focused on studying this phenomenon, developing effective means of combating and resilience, as well as on developing strategies aimed at strengthening the necessary capabilities to prevent such threats in the future. These

initiatives reflect a continuous adaptation to the challenges of a rapidly changing global security environment (Wither, 2016).

Hybrid threats are characterized by the integrated use of conventional and unconventional means, and their seriousness stems from the fact that they aim to capitalize on the vulnerabilities of adversaries. These include information manipulation, cyberattacks, economic pressures, embargoes, propaganda, disinformation and the use of *proxy actors*. The purpose of proxy actors is to allow states to carry out actions that support political, military or economic objectives, without directly assuming responsibility. They include private companies, hackers or criminal networks, being involved in cyberattacks and intelligence gathering and are used to reduce political risks, save resources and exploit specific expertise in cyberattacks, propaganda or other forms of indirect influence (Collier, 2017). Manipulation and disinformation are used to destabilize the internal cohesion of states by spreading fake news and amplifying social conflicts, thus weakening trust in institutions, an aspect that we can observe more and more often in as many situations as possible, the political sphere sometimes depending on these methods used. Cyber-attacks target critical infrastructures, compromising security and causing strategic dysfunctions; often serve political, economic or military purposes, being effective instruments of influence and indirect coercion. Economic pressures and embargoes are used to affect the economic stability of the adversary, while proxy actors are mobilized to carry out actions below the threshold of direct conflict. All these elements, coordinated and synchronized in the "*grey zones*" of war, complicate the responses of adversaries and create combined effects that destabilize, but without triggering a conventional conflict (Reichborn-Kjennerud & Cullen, 2016).

3. Theorizing the Concept of Hybrid War Through the Prism of International Relations Theories

For a better understanding of hybrid war, theorists of various international security trends have tried to place this war at the centre of international relations in order to be able to define it, to understand its mode of operation and the consequences it can determine on international actors. Therefore, starting from Carl von Clausewitz's definition of war, it "*is an act of violence intended to compel our opponent to fulfil our will*" (Clausewitz, 2017). Although this is the definition of war for the conventional form, in the case of hybrid war there is no violent component, it rather uses an interweaving of hard power instruments with soft power ones. However, one

aspect draws our attention - even in the absence of military force, hybrid war also aims to intimidate the opponent in order to pursue its own. With the modernization and progress of technology, cantered in a changed geopolitical context, the new form of war, which emerged after the Cold War and gained momentum after 2014, becomes a real threat to international security (Abdyraeva, 2020, pp. 13-14).

Realism offers a unique vision of the concept of hybrid war in the sense that a state will do anything possible for survival. As Hans Morgenthau stated (Morgenthau, 1973, pp. 5-18), the international system is dominated by anarchy, more precisely, a world order cannot be imposed in the absence of a world government. Thus, in this context, states pursue their own interests by maximizing power, security interests dominating any other goals. In this sense, the struggle for power and survival can determine behaviour that sometimes does not align with moral standards, especially in the case of weak states. Even if the realist vision centres on military capabilities as the main means of maximizing power, technological impediments or the geopolitical context can limit the use of the army in some situations. That is why realists, such as Morgenthau, argue that states can resort to alternative options for pursuing interests, such as hybrid warfare (Morgenthau, 1973, pp. 20-25). This method has an important advantage – that of using hard power together with soft power instruments, thus making the fight for survival more efficient, while also involving the civilian dimension that allows influencing the preferences of other states in accordance with its own interests, as Joseph Nye also mentions: "*Co-optive (soft) power is the ability of a country to structure a situation so that other countries develop preferences or define their interests in ways consistent with its*" (Nye, 1990). We can thus understand, by referring to the civilian dimension, that Nye's theory can be partially applied to hybrid warfare if we think about its means, namely propaganda and disinformation through which the adversary's citizens are manipulated, leading to the same result as in the case of conventional warfare, but without the use of force.

On the other hand, liberalism, which does not focus on the concept of power, brings into the centre of the analysis other actors besides states, namely non-state actors. Liberalism also addresses globalization and interdependence between states, and Andrew Moravcsik includes the most important principles of liberalism, namely "*The foundation of the liberal theory of world politics can be expressed in the form of three core assumptions, comprising the basic liberal claims about the essential social actors and their motivations, the relationship between state and civil society, and the circumstances under which states develop strategies and make choices in*

the international system" (Moravscik, 1992). Thus, we can explain hybrid war from the perspective of liberalism starting from the intrastate analysis and from the premise that each state acts according to preferences, but without being willing to resort to war. On the contrary, liberalism explains hybrid warfare by analysing internal regimes, highlighting the institutional and societal vulnerabilities exploited by aggressors to influence the policies of target states. Economic interdependence and international cooperation, pillars of liberalism, become both instruments and targets of hybrid warfare, while democratization and free access to information are manipulated to undermine legitimacy and internal cohesion. We can see that this is achieved either through disinformation, as Russian Federation did for example, transmitting that the UN recognized that Crimea belongs to Russia, or through this state's practice of supporting nationalist and Eurosceptic parties by practicing electoral propaganda, etc. (Filipec, 2019, pp. 59-62).

The constructivist theory is located in the middle of the relationship between the two theories mentioned above, even borrowing some characteristics from realists, also supporting "*international political anarchy, a central role of the state in shaping international policy, as well as uncertainty about the intentions of the other*" (Wendt, 1995, p. 72). Alexander Wendt's theory about the behaviour of states in the process of interaction, which can shape national identities and interests depending on its nature, is very important for understanding hybrid warfare from the perspective of the civilian dimension, more precisely, regarding propaganda and disinformation (Filipec, 2019, pp. 63-64). Identity plays a significant role in the constructivist analysis, with specialists arguing that identity can change depending on the options available to states (Wendt, 1995, p. 75), so that actions in the civilian dimension, such as disinformation and propaganda, are used to reconstruct identities, delegitimize the pillars of the target society and generate identity crises. By manipulating history, attacking democratic values and promoting narratives favourable to their own interests, aggressors destabilize internal cohesion and influence national perceptions, thus consolidating control over the targeted populations. For example, Russian education promotes distorted versions of the past, such as presenting the "*Great Patriotic War*" exclusively from the perspective of victory over Nazism, while collaboration with Nazi Germany under the Molotov-Ribbentrop Pact or the annexation of the Baltic states are ignored or reinterpreted as defensive measures. Such practices validate the constructivist theory of hybrid warfare to reshape identities for a distrust of cooperation or integration (Filipec, 2019, pp. 64-65).

Therefore, through the lens of these theories we can understand in a clearer way this concept of hybrid warfare, while also understanding how ideas, values and identities are used as strategic weapons. A theoretical understanding can thus help us to identify the main hybrid threats, their consequences on the international system, what hybrid security is and what are the measures adopted by different actors in order to counter this type of war.

By hybrid security we can thus understand as that component of international security that tries to respond to complex threats that include military, cyber or economic components. This concept integrates state and non-state resources in a flexible framework, adapted to prevent and manage modern conflicts, characterized by ambiguity and global interdependence (Ardemagni, 2024, pp. 7-8).

4. The International Community's Response to Hybrid Threats

In the current geopolitical context of instability, hybrid security is evolving as a central dimension in modern strategies, defined by the combined use of civilian and military means to destabilize adversaries and manipulate public perceptions. Recent conflicts, such as the one in Ukraine, have led states and regional or international organizations to focus their efforts against Russian Federation attacks that illustrate hybrid strategies that include disinformation campaigns, the use of paramilitary forces and the exploitation of institutional vulnerabilities. NATO recognizes the need for resilience in response, by coordinating military and civilian resources and involving civil society in transparent strategies. Advances in technology and the complexity of modern warfare emphasize the importance of rapid adaptation of strategic processes, as highlighted in the increasingly close relationship between NATO and the EU to counter hybrid threats (Hartmann, 2017, p. 1). The EU and NATO responds through initiatives such as the REPowerEU plan and cooperation with centers of excellence in countering hybrid threats, however, coordinated strategies are needed in the context of competition for critical resources and green technologies, which will further intensify the dimensions of hybrid conflicts (Geri, 2024, p. 15).

NATO took a first step towards giving special importance to hybrid security in 2016, when it launched a strategy to counter hybrid threats. Since the illegal annexation of Crimea in 2014, hybrid warfare has been high on NATO's agenda, a fact that was supported, including at the same year NATO's Summit in Wales, "*We will ensure*

that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces" (Wales Summit Declaration, 2014). Thus, following the discussions at the 2016 NATO Summit held in Warsaw, have been taken "*We have taken steps to ensure our ability to effectively address the challenges posed by hybrid warfare, where a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, are employed in a highly integrated design by state and non-state actors to achieve their objectives*" (Warsaw Summit Declaration, 2014), and the adoption of the Strategy for Countering Hybrid Threats was ratified. This document emphasizes the need for awareness of these threats by facilitating information exchange, strengthening the resilience of critical infrastructures, cybersecurity, and preparing society. The common framework of this strategy between the EU and NATO supports inter-institutional collaboration and strengthening the capacities of member states, while also aiming to deter and defend against hybrid attacks, with the aim of maintaining regional and international stability (Countering Hybrid Threats, 2016).

Last but not least, a decisive step of this initiative was the adoption of this strategy to raise NATO and the EU's awareness of the threatening nature of some practices used by hybrid warfare, as it was stated in the NATO Strategic Concept, adopted in 2022. It clearly and unequivocally indicates that Russian Federation uses hybrid warfare and identifies it as the main threat to the stability of the Euro-Atlantic area, "*The Russian Federation represents the most significant and direct threat to the security of the Allies and to peace and stability in the Euro-Atlantic area. It seeks to establish spheres of influence and direct control through coercion, subversion, aggression and annexation. It uses conventional, cyber and hybrid means against us and our partners*" (NATO Strategic Concept, 2022).

European Centre of Excellence for Countering Hybrid Threats[1], headquartered at Helsinki is considered one of the structures that effectively combat hybrid threats and enjoys the direct support of the EU and NATO. The main purpose of this centre is to strengthen the countering capacity of the Member States against hybrid threats.

[1] https://www.hybridcoe.fi/, accessed on 25.11.2024.

Currently the centre brings together 36 participating states and operates to provide expertise and share best practices to counter hybrid warfare. Also, this structure has an operational component, organising practical exercises for different hybrid threat scenarios, allowing the study of different hybrid attack patterns, awareness of the main vulnerabilities of states and study of lessons learned, on the one hand, and conducting joint simulations and exercises of combat and counteraction in the event of a hybrid attack to support interoperability and the exchange of best practices, on the other hand. All of this is intended to provide a common platform to anticipate, detect and respond effectively to hybrid challenges[1].

Last but not least, as a measure to combat hybrid threats, NATO has established rapid response units. The *NATO Response Force (NRF)*; is a multinational force, which comprising land, sea and air components, is flexible and capable of responding rapidly to a variety of crises and threats, including hybrid ones. It also includes a unit strictly specialized in the field of cyber defence, called *Cyber Rapid Reaction Teams (CRRTs)*, to ensure the protection of critical infrastructure[2]. From an operational perspective, the most important NATO exercise dedicated to hybrid response is *Exercise Locked Shields*, an annual exercise that allows specialists to acquire the necessary capabilities to protect critical infrastructure and national systems against complex attacks[3].

The European Union also responds to hybrid threats through a comprehensive strategy that combines resilience measures, international cooperation and political, economic and security instruments. These measures are intended to prevent, detect and counter hybrid tactics that include disinformation, cyberattacks, economic pressure and manipulation of critical infrastructure. It has adopted a series of measures and mechanisms to combat hybrid threats. One of the instruments was adopted in 2015, following the illegal annexation of Crimea, called *The East Task Force*, which is part of the Strategic Communications and Information Analysis Division, within the European External Action Service. The main goal is to counter disinformation, focusing on strengthening strategic communication, especially in the Eastern Neighbourhood. This task force brings together a number of experts, especially in Russia studies, who monitor disinformation campaigns and have as their main responsibility the dissemination of accurate information. Furthermore,

[1] https://www.hybridcoe.fi/coi-strategy-and-defence, accessed on 25.11.2024.
[2] https://www.nato.int/cps/en/natolive/topics_49755.htm, accessed on 25.11.2024.
[3] https://ccdcoe.org/locked-shields/, accessed on 26.11.2024.

The East Task Force promotes EU policies and in the Eastern Partnership countries to increase public awareness and understanding of the Russian Federation's disinformation operations, helping citizens in Europe and beyond to build resilience to digital information and media manipulation[1]. In the same year, the European External Action Service also established the *Very High Readiness Joint Task Force (VJTF)*, another task force of experts whose objective is to provide methods to respond rapidly to emerging threats, including hybrid attacks[2].

The EU contributes to strengthening resilience, one of the most important initiatives being the adoption in 2016 of the *NIS (Network and Information Security)* Directive, which has now been updated to NIS2, due to its ability to adapt to the complexity and sophistication of these types of threats. With increasing digitalization, the EU is constantly adapting the legal framework for Member States in the field of cybersecurity[3].

Last but not least, alongside educational and awareness-raising efforts through various programs to detect manipulation and disinformation, the EU constantly adopts economic sanctions to punish states such as Russia, which uses hybrid tactics. To date, 14 packages of economic sanctions have been adopted at EU level against Russia, since the illegal invasion of Ukraine on February 24th 2022[4].

5. Conclusions

Despite the numerous mechanisms and instruments adopted, the complexity of hybrid threats, the uncertainty and the speed of propagation make it difficult for state and non-state actors to effectively counter specific attacks. Such threats change the paradigm of traditional security, which makes current initiatives constantly adapt. In the absence of a clear international legal framework, the problem of coordination and the limitation determined by national sovereignties are part of the gaps in this area. Civic awareness is an important component and perhaps more effective education programs are needed at the level of each state.

[1] https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en, accessed on 28.11.2024.
[2] https://euvsdisinfo.eu/ro/, accessed on 28.11.2024.
[3] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, accessed on 28.11.2024.
[4] https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-packages-sanctions-since-february-2022/, accessed on 29.11.2024.

Factors such as globalization, digitalization or economic interdependence favour the propagation of hybrid warfare in the post-modern era by state or non-state actors who exploit vulnerabilities in a strategic manner. Disruption of supply chains, price manipulation, financial pressure or the use of critical resources as geopolitical weapons are just some of the practices of hostile actors to expand their influence. To counter these threats, states must adopt resilience measures, strengthen international cooperation and invest in the security of critical infrastructures and cyber education.

Non-state actors exert additional pressure to those who make efforts to counter hybrid warfare, amplifying the complexity of modern conflicts. Digital propaganda is used by terrorist groups such as ISIS for the purpose of recruitment and financing. Economic warfare is influenced by the actions of organized crime networks through crimes such as money laundering, destabilizing economies and financing conflicts. Moreover, the combination of conventional and non-conventional elements, a specific characteristic of hybrid warfare, is used by proxy actors, such as the Wagner Group, which, in pursuit of Russia's interests, carries out military operations, but also economic manipulation for regional destabilization.

Thus, in the current geopolitical context, characterized by instability and intensifying strategic competition, hybrid threats constitute a global challenge that requires coordinated measures. The international community must strengthen its cooperation through information sharing, developing resilience capacities and adopting integrated strategies that effectively counter hybrid tactics.

References

Abdyraeva, C. (2020). *The Use of Cyberspace in the Context of Hybrid warfare: Means, Challenges and Trends*. Working Paper no. 107. Wien: Austrian Institute for International Affairs.

Ardemagni, E. (2024, April). *Historical perspective and the terminology issue: defining post 2011 hybrid security actors*. Doha: Arab Center for Research & Policy Studies.

Banasik, M. (2016). A changing security paradigm. New roles for new actors - the Russian approach. *Connections: The Quarterly Journal*, 15(4), 31-43.

COI Strategy and Defense (n.d.). Hybrid CoE. Retrieved from https://www.hybridcoe.fi/coi-strategy-and-defence/, date: 25.11.2024.

Collier, J. (2017). Proxy actors in the cyber domain: implications for state strategy. *St. Antony's International Review*, 13(1).

Conceptul strategic al NATO 2022/NATO Strategic Concept 2022 (2022). Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ro.pdf, date: 25.11.2024.

Countering hybrid threats (2016). North Atlantic Treaty Organisation. Retrieved from https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en, date: 24.11.2024.

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (n.d.). European Commission. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive, date: 28.11.2024.

Filipec, O. (2019). Hybrid warfare: between realism, liberalism and constructivism. *Central European Journal of Politics*, 5(2).

Geri, M. (2024). Understanding Russian Hybrid Warfare against Europe in the energy sector and in the future "energy-resouces-climate" security nexus. *Journal of Strategic Security*, 17(3).

Hartmann, U. (2017, September). *The Evolution of the Hybrid Threat, and Resilience as a Countermeasure*. Research Paper 139. NATO Defense College.

Johnson, R., Kitzen, M., & Sweijs, T. (2021). *The conduct of war in the 21st century. Kinetic, connected and synthetic*. New York: Routledge.

Kanwal, G. (2018). *Hybrid Warfare: The Changing Character of Conflict*. New Delhi: Institute for Defence Studies and Analyses, Pentagon Press.

Locked Shields (n.d.). The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/locked-shields/, date: 26.11.2024;

Moravscik, A. (1992). *Liberalism and international relations theory*. Cambridge, Massachusetts: Center for European Studies, Harvard University.

Morgenthau, H. (1973). *Politics among nations. The struggle for power and peace*. New York: Alfred A. Knopf.

Murray, W. & Mansoor, P. (2012). *Hybrid warfare. Fighting complex opponents from the ancient world to the present*. Cambridge: Cambridge University Press.

NATO Response Force (n.d.). North Atlantic Treaty Organisation. Retrieved from https://www.nato.int/cps/en/natolive/topics_49755.htm, date: 26.11.2024.

Nye, J. (1990). Soft power. *Foreign Policy*, 80.

Questions and Answers about the East StratCom Task Force (n.d.). European Union External Action - The Diplomatic Service of the European Union. Retrieved from https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en, date: 28.11.2024.

Raugh, D. (2016). Is the hybrid threat a true threat? *Journal of Strategic Security*, 9(2).

Reichborn-Kjennerud, E. & Cullen, P. (2016). *What is Hybrid Warfare?* NUPI Policy Brief, 1. Oslo: Norwegian Institute of International Affairs.

Timeline - Packages of sanctions against Russia since February 2022 (2024). European Council - Council of the European Union. Retrieved from https://www.consilium.europa.eu/en/policies/sanctions-against-russia/timeline-packages-sanctions-since-february-2022/, date: 29.11.2024.

von Clausewitz, C. (2017). *On war*. Augsburg: Jazzybee Verlag.

Wales Summit Declaration (2014). Retrieved from https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease, date: 24.11.2024.

Warsaw Summit Declaration (2014). Retrieved from https://www.nato.int/cps/de/natohq/official_texts_133169.htm, date: 24.11.2024.

Wendt, A. (1995). Constructing International Politics. *International Security*, 20(1).

Wither, J. (2016). Making sense of hybrid warfare. *Connections: The Quarterly Journal*, 15(2).