



Public-private partnerships in National Security. A case study in the context of the war in Ukraine: 2022-2024

Dragan, Iryna¹

Correo: gggira2013@i.ua

Orcid: <https://orcid.org/0000-0002-6906-5000>

Panfilova, Tetiana²

Correo: tetiana.panfilova.71@gmail.com

Orcid: <https://orcid.org/0000-0002-7924-8716>

Chistiakova, Iryna³

Correo: i.m.chistyikova@op.edu.ua

Orcid: <https://orcid.org/0000-0002-0182-9334>

Tatarinov, Roman⁴

Correo: r.v.tatarinov@gmail.com

Orcid: <https://orcid.org/0009-0007-3672-6099>

Abstract

The aim of the research was to analyze the political implications of public-private partnerships on Ukraine's national security, using case study methodology and review of documentary sources. The war in Eastern Europe has passed through different stages. Since February 2022, with the so-called "special military operation" the Russian Federation invaded Ukraine, violating the national sovereignty of this country and all norms of public international law guaranteeing relations between civilized sovereign states. As in any war, a key element in the defense of national sovereignty lies in the strategic partnership of the public sector, with private enterprise, to confront the invader. In the case of Ukraine, this strategic partnership involves collaboration between the government and various private companies such as Microsoft, Palantir Technologies and Northrop Grumman, especially in areas such as: cybersecurity, production of inputs, paramilitary organizations, and logistical support of troops on the front lines. It is

¹ Department of Sustainable Development Methodology Institute for demography and life quality problems of the National Academy of Sciences of Ukraine. Ukraine

² Department of State Policy and Governance, Lviv Polytechnic National University. Ukraine

³ Department of International Relations and Law, National University «Odesa Polytechnic». Ukraine

⁴ Department of International Relations, Public Communications and IT law State University of Intelligent Technologies and Telecommunications. Ukraine



concluded that by implementing PPPs, the government was able to improve military infrastructure, develop new defense technologies and optimize military training.

Keywords: Public-private partnerships; National security Policy; war in Ukraine; Private companies; Strategic thinking.

Asociaciones públicas y privadas en la seguridad nacional. Un estudio de caso en el contexto de la guerra en Ucrania: 2022-2024

Resumen

El objetivo de la investigación fue analizar las implicaciones políticas de las asociaciones públicas y privadas en la seguridad nacional de Ucrania, mediante la metodología del estudio de caso y la revisión de fuentes documentales. La guerra en Europa del este ha transcurrido por diferentes etapas. Desde de febrero de 2022, con la llamada “operación militar especial” la Federación Rusa invadió a Ucrania, violando la soberanía nacional de este país y todas las normas del derecho internacional público que garantizan las relaciones entre estados soberanos civilizados. Como en toda guerra, un elemento clave en la defensa de la soberanía nacional, está en la asociación estratégica del sector público, con la empresa privada, para hacer frente al invasor. En el caso de Ucrania, esta asociación estratégica implica la colaboración entre el gobierno y varias empresas privadas como Microsoft, Palantir Technologies y Northrop Grumman, especialmente en áreas como: la ciberseguridad, producción de insumos, organizaciones paramilitares y el apoyo logístico de las tropas en el frente de batalla. Se concluye que, al implementar las asociaciones públicas y privadas APP, el gobierno pudo mejorar la infraestructura militar, desarrollar nuevas tecnologías de defensa y optimizar el entrenamiento militar.

Palabras clave: asociaciones públicas y privadas; política de seguridad nacional; guerra en Ucrania; empresas privadas; pensamiento estratégico.

Introduction

Warfare in human history does not only unfold through the dialectical clash between antagonistic states striving for domination, subjugation, and, in certain

cases, the ontological annihilation of the other. It is also a multidimensional struggle involving private organizations in strategic alliance with warring states, forming a public-private partnership (PPP) where private companies participate with various offensive or defensive purposes. In the specific case of Ukraine, these PPPs aim to strengthen national security as a public good, which logically derives from national sovereignty, currently threatened by post-Soviet Russian imperialism.

More specifically, as explained by the International Labor Organization (2008):

Public-private partnerships are voluntary collaborative initiatives between various actors in the public sector (state) and the private sector (non-state), in which the parties agree to work together to achieve a common purpose or undertake specific tasks. Partnerships can have different objectives, such as advancing a cause, implementing standards or codes of conduct, or exchanging and coordinating resources and technical knowledge. (2008, p. 01)

As is well known to the international public opinion, the war in Ukraine has unfolded in various geopolitical stages, beginning with the preparation for war, marked by the events of Euromaidan, a historic day of Western civic protest that culminated in the resignation of pro-Russian President Viktor Yanukovich on February 22, 2014; followed by the Russian annexation of the Crimean Peninsula, justified by the Russian or pro-Russian narrative as a means to protect the rights of Russian speakers in this territory, which is an integral part of Ukraine's geography, on March 18, 2024. On that date, “On March 18, two days after the publication of the referendum results, Putin officially formalized the invasion by signing a bill that incorporated Crimea into the Russian Federation” (BBC News Mundo, 2022, parr., 06).

The second stage of the war began with the large-scale invasion of Ukraine by the Russian Federation on February 24, 2022, resulting in devastating consequences for this sovereign and independent country and its civilian population⁵. Initially, the Kremlin and its propaganda apparatus presented the conflict as a “special military operation” aimed at “protecting Russian speakers in eastern Ukraine”, but it quickly transformed into one of the most significant land wars in Europe since World War II.

As reported by the Center for Preventive Action (2024), over the more than two years of large-scale invasion, the fighting has resulted in over 190,000 military casualties and a significant number of civilian victims, with UN estimates indicating more than 26,000 civilian deaths as of August 2023. According to data provided by Dodds *et al.* (2023), this war has caused massive destruction of infrastructure and displaced millions of people, with over 6 million refugees and 3.7 million internally displaced persons, leading to an unprecedented complex humanitarian crisis in the Eastern European region.

In this complex context of an ongoing war, in which Ukraine is fighting for its own existence as a national state, the aim of the research was to analyze the political implications of public-private partnerships in Ukraine's national security, using a case study methodology and reviewing scientifically validated documentary sources. The documented cases of three PPPs were specifically studied: Microsoft, Palantir Technologies, and Northrop Grumman, international

⁵ For a full picture of the humanitarian impact of the war on Ukraine's civilian population, we recommend consulting the United Nations report (2024), Available online at: <https://www.ohchr.org/sites/default/files/documents/countries/ukraine/2024/24-07-02-OHCHR-39th-periodic-report-Ukraine.pdf>.

companies with extensive experience in the fields of cybersecurity, big data analysis, intelligence, and national defense, among other aspects.

The present specific objective of the research is also expressed in the formulation of three central questions that will be answered, even if partially, throughout this scientific article. These questions are: How have public-private partnerships influenced the formulation and implementation of national security policies in Ukraine during the war with Russia? What political challenges have public-private partnerships faced in addressing national security needs in a context of armed conflict? And, finally, how has the involvement of private actors in national security affected the balance of power and accountability between the Ukrainian government and companies in the defense and security sector?

This article, which combines documentary research with political reflection and critical thinking on equal terms, is divided into five (05) particular but connected sections aimed at addressing its research objective. In the first section, the documentary background of the research and the theoretical framework are presented; in the second, the details of the methodology employed; in the third section, descriptions of the case studies in terms of PPPs are provided; subsequently, in the fourth, the results are analyzed and discussed. Finally, the main conclusions and recommendations of the article are presented to our esteemed readers.

1. Selected Literature and Theoretical Framework

Since the Russian invasion of Ukraine in February 2022, there has been a significant production of literary and audiovisual material regarding this military conflict, widely disseminated in international press due to its geopolitical

implications for Europe and the rest of the world. This information production manifests in press releases, scientific articles, monographs, and books that explore the situation from various dimensions, such as the human rights of the civilian population affected by the conflict, the geostrategic aspects of the struggle, the legal implications of the invasion, the responses of power actors involved in the war, and the issue of national security, among other aspects.

Moreover, the topic of public-private partnerships (PPPs) also has a wealth of literature, as can be corroborated by any review of the subject in specialized databases such as Scopus, WOS, Prisma, or BASE, to name a few. What may be relatively novel is the study of PPPs in the specific context of the war in Ukraine. Considering this conglomerate of sources, contemporary historians and social scientists must critically process a diversity of sources ranging from specialized literature on the subject to press releases and opinion articles.

Therefore, this section has a dual purpose: on one hand, to present authors and works regarding the war in Ukraine and the PPPs that engage in strategic alliances with the government of Kyiv to strengthen national security against the onslaught of the invading army. On the other hand, to expose to the reader our theoretical and epistemological position that served as an interpretative model of reality, in a situation that is not only described in scientific terms but also, and crucially, affects the lives of the authors of this article, who, in their ontological condition as Ukrainians, have seen their daily lives impacted by the rigors of a war driven by the devastating actions of post-Soviet Russian imperialism.

1.1. War in Ukraine: Narratives and Meanings

The narratives surrounding the war in Ukraine are numerous and varied. According to discourse scholars like van Dijk (2009), it ultimately depends on the

political and ideological context of the media and authors who produce and reproduce this information, never in a neutral manner, but through the prism of their interests and geopolitical and ideological positions. Furthermore, war is a multidimensional phenomenon that disrupts all daily activities in the country where it unfolds, serving as its main theater of operations. In this sense, the literature presented below addresses different aspects of the conflict from the perspective of Ukraine's suffering.

For instance, the scientific activity that represents one of the main engines of a country's development has been significantly affected by the war in Ukraine, as confirmed by the article "The Impact of the War in Ukraine on Science and Universities," which examines how the Russian invasion has impacted scientific production in Ukraine. Authors Ganguli and Waldinger (2023) highlight a decrease of at least 10% in the publication of high-impact articles by Ukrainian scientists since the onset of the conflict. This decline is attributed to the loss of human capital, as many nationally and internationally recognized researchers have been displaced or have lost their lives, as well as to the destruction of scientific infrastructure. Additionally, the study underscores the strategic importance of preserving human capital and infrastructure to ensure the future of research in the country, suggesting that if the war continues, the current situation could have long-term negative effects on Ukraine's scientific output.

Perhaps one of the dimensions most impacted by the Russian army's presence in Ukraine pertains to human rights and humanitarian issues in general. Indeed, the article titled "Humanitarian Principles Are Under Fire in Ukraine" by Norman (2024) explores how the conflict threatens humanitarian principles in the country. Interviews with humanitarian aid workers document the challenges faced

by humanitarian institutions in maintaining neutrality and objectivity in times of war. At the same time, this study highlights the urgent need to adapt humanitarian aid practices and policies to the geopolitical realities of the conflict to ensure that interventions are effective and that the fundamental rights of victims are respected. The author raises legitimate questions about the sustainability of humanitarian aid in the context of prolonged conflicts and the importance of accountability (Norman, 2024).

Another relevant document for the specific purposes of this research is "Regional Cooperation in Central Europe after Russia's Aggression against Ukraine," by the Polish Institute of International Affairs (2024), as it addresses the political and economic consequences of the war on European regional cooperation. Generally, the study examines how Russian aggression has led Central European countries to redefine their political and economic relationships, seeking greater collaboration in defense and security. In their conclusions, the authors argue that the war has created a sense of urgency to strengthen regional cooperation while simultaneously developing joint defense strategies to address common threats. This analysis is crucial for understanding how the conflict has reshaped geopolitical power dynamics in Europe and influenced the security policies of neighboring states involved in the conflict.

As indicated in the report:

The large-scale Russian invasion of Ukraine in 2022 affected the dynamics of regional political cooperation among Central European states. This was not due to a change in the eastern or security policies of these countries at a strategic level under the influence of the war, but rather to the divergent policies pursued before its outbreak. Therefore, it highlighted the inability of members of some alliances to act together and justified the hardening of cooperation, among other things. Two

years later, this condition persists. (Polski Instytut Spraw Międzynarodowych, 2024, p. 05)

Meanwhile, Ruppert's report (2024), "In Search of a Formula for Lasting Peace in Ukraine", focuses on the efforts of Ukraine and its allies to establish a sustainable peace framework to end this war. In this regard, the authors emphasize the importance of creating security structures that disincentivize future Russian aggression and, under certain security and respect conditions, promote stability in the region. Within the dialectical set of political and diplomatic strategies being considered to ensure a peaceful future for Ukraine, the need for a comprehensive diplomatic approach that includes international cooperation and the strengthening of democratic institutions in the country is emphasized.

1.2. Public-Private Partnerships in Ukraine's National Security

In all countries, national security is a complex issue that is normally developed through a system in which, under the coordination of the State through its Ministry of Defense or equivalent, a defense system is built in which different levels of government participate together with private enterprise. For example, an official document on the national security strategy of the government of Spain (Government of Spain, 2016) states that:

National Security is defined in a comprehensive and broad way, as it is understood as the action of the State aimed at protecting the freedom and well-being of its citizens, guaranteeing the defense of Spain and its constitutional principles and values, as well as contributing together with our partners and allies to international security in the fulfilment of the commitments assumed. (2016, p. 01).

This definition gives clear clues about what national security means in the contemporary world. In principle, it is a question of the integral protection of territoriality and of the nation that inhabits it, but at the same time it is also a question of the defense of the rule of law against the internal and external threats that permanently oppose its empire. In ontological or essential terms, national security is the guarantee of the freedom and well-being of citizens in the face of the historical enemies of democracy and human rights. But, above all, it is the first geopolitical and geostrategic step to guarantee the international security that serves as the basis of the current world order. Thus, without a solid national security strategy, the existence of any sovereign nation-state is not guaranteed.

On the other hand, a reading of the work of Novytskyi, Shcherbyna, Pyvovarov, Kartamysheva and Lysodyed (2022) shows that Ukraine's national security doctrine goes in the same direction as the definition promoted by the government of Spain. However, in the conditions of the current war, the principle of national security, which is included in Ukraine's legislation, is expressed in the strategic principle "security for oneself through security for all". In this vein, Ukraine aspires to become a member state of the European Union and the North Atlantic Treaty Organization NATO, supporting collective security and defense, as well as the democratic principles and values that identify these multilateral institutions. Moreover, Ukraine respects the borders and sovereignty of all countries, does not participate in any territorial violations of neighbouring countries, and does not allow violations of the geographical integrity of its own borders.

Having clarified the above, we now review the fundamentals of public and private PPP partnerships in matters of national security. The document of the

International Labor Organization (International Labor Office, 2008) explains what the key basis for the construction of PPPs is, and that is that, to achieve success, public and private partnerships must be located in an adequate legal and institutional framework. Thus, the creation and operation of the association or strategic alliance responds to the objectives and purposes for which it was created, but, in addition, it is compatible with the principles and values of the constitution of the State in which the association is developed, otherwise the association may be illegal or not appropriate to the general interests of society.

In recent national security studies, there are fields and dimensions in which PPPs are common and necessary phenomena. This is the case, for example, with cybersecurity governance.

Governance is a priority area of cybersecurity. Cooperative interaction between public and private actors is a necessary (although not sufficient) condition for its effective management, because the causes of the problem lie in shared responsibilities between the State and society. This perspective is the foundation of international standards, which advocate the design of cyber policies that are inclusive of business and social interests, aiming to generate environments of trust that favor their collaborative approach. (International Telecommunication Union, World Bank, Commonwealth Secretariat, Commonwealth Telecommunication Organization, and NATO Cooperative Cyber Defense Center of Excellence, 2018, p. 14)

In this vein, Carr's (2016) article Public-private partnerships in national cyber-security strategies also highlights that cooperation between the public and private sectors is essential to ensure cybersecurity in the United Kingdom and most Western countries, because 80% of critical infrastructure is owned by individuals,

which means that its security depends largely on cooperation with technology companies. This symbiotic relationship is particularly important in the current Ukrainian context, where the war has highlighted the need for a rapid and effective response to cyber threats and, at each moment, highlights the need to strategically strengthen PPPs to maximize their impact on national security and international governance.

Broadly speaking, in the context of the war in Ukraine, public-private partnerships (PPPs) have emerged as a crucial mechanism for strengthening national security, with all that it entails in terms of collective security and global security. According to an article entitled "Public-private collaboration for national security: challenges and opportunities" authored by Soroka, Danylenko, Sokiran, Levchenko, and Zubko (2023), PPPs are essential to ensure the effectiveness of protection and defense measures, allowing the private sector to contribute resources and technology, which is essential in an environment of growing threat. The collaborative approach in the relationship between government and private companies not only optimizes the available resources, but also fosters innovation in the development of defense technologies and military infrastructure, necessary to confront the external aggression of Russian imperialism. For these reasons, a good PPP must be developed under the following strategic criteria:

- 1) sharing of risks and responsibilities, in which both parties, the public and private sectors, share the risks and responsibilities associated with the execution of the project or the provision of services.
- 2) financial transparency (to comply with this, it is necessary to conclude a detailed agreement on the financing and management of the funds, which will ensure not only transparency, but also the effective use of resources).
- 3) innovation (the private sector can provide know-how and innovation, thus ensuring a more effective solution to problems).

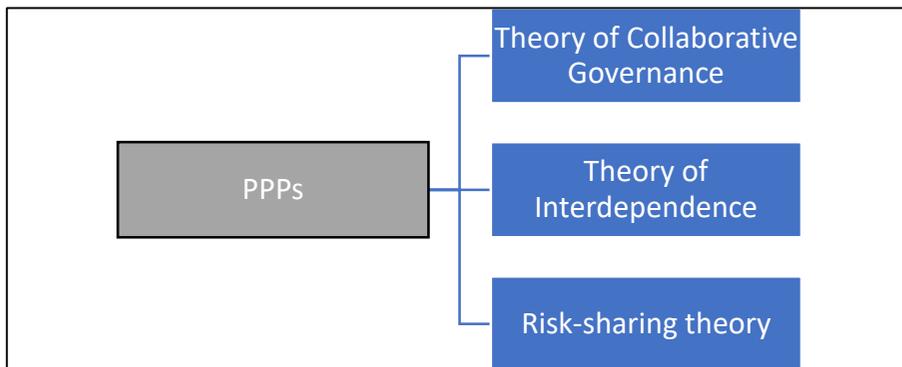
- 4) duration, as such partnerships usually involve a long period of cooperation, ensuring stability and long-term benefits for both parties.
- 5) socio-economic impact (public-private partnerships can contribute to socio-economic development through the creation of new jobs, improved quality of services and infrastructure development) (Soroka et al., 2023, p. 47).

In short, it is clear that PPPs are not only a business for private companies that profit by offering technological goods and quality services to the public sector, it is fundamentally a strategic alliance that must be structured harmoniously in respect for laws, values and social institutions as a condition of possibility for strengthening the capacities of the state in the face of the multifactorial threats that affect Ukraine's national security and collective well-being.

1.3. Some theories on collaboration between the public and private sectors in the field of national security. Comprehensive vision

Within the theoretical universe available to explain the scope and meanings of PPPs, we focus on three theories, due to their versatility to adapt to the categorical imperatives of this research. These theories are:

Table 1. Theories that explain public and private partnerships



Source: prepared by the authors (2024).

In the first case, according to Barandiarán, Canel, and Bouckaert (2022), collaborative governance theory postulates that national security and the construction of public policies in general is most effectively achieved through the cooperation of multiple actors, including the government, the private sector, and organized civil society. It argues that, in a complex and dynamic environment, the exchange of information and resources among these actors is essential to combat emerging threats. Finally, collaborative governance emphasizes the importance of building relationships of trust while also creating a collaborative framework to coordinate responses to crises and security challenges.

In this order of ideas, a favorable climate for governance and collaborative governance can only be achieved in a scenario of consolidated social capital that favors relationships of trust and respect between the actors involved in a program, project or policy: "In this endeavor, the intangible resource of trust acquires special relevance because advancing in the participation of different actors in public policies involves giving value to the contribution that they can lend" (Barandiarán *et al.*, 2022, p. 251).

As for the theory of organizational interdependence, it considers that the public and private sectors are interrelated in the firm purpose of guaranteeing national security. In particular, the private sector plays an important role in managing critical infrastructure and essential services that in many circumstances the government cannot manage. In a context of crisis, interdependence means that governments must rely on the capacities and resources of the private sector to ensure the security of the nation, which in turn requires a clear regulatory framework that fosters cooperation. According to Tokatlian and Pardo (1990), the theory emphasizes the need to align the interests of both sectors to maximize the

effectiveness of security policy in the context of increasingly conflictive international relations.

Finally, for risk-sharing theory, cooperation between the public and private sectors in the framework of national security is based on the idea that risks related to security threats must be managed jointly, since they often exceed the capacities and resources of the state to contain them effectively. This means that governments and businesses must share not only the benefits, but also the risks and costs of implementing effective security measures. For Rincón (2012), this theory promotes the creation of strategic partnerships, eliminates unilateral liability, encourages innovation in risk management, and simultaneously ensures that both parties are committed to protecting national security.

2. Research methodology

The methodological structure of this research combined three qualitative tools to process the information collected under equal conditions and, therefore, produces knowledge with an acceptable level of veracity on the subject. At first, the documentary research technique is used, which, according to Arias (2009), involves the process of searching, retrieving, analyzing, criticizing, and interpreting secondary information obtained from printed, audiovisual, or electronic sources.

The documentary method allows researchers to access information previously recorded by others, facilitating research on a specific topic by collecting relevant and reliable data. In addition, Arias (2009) emphasized that documentary research can be done at different levels, such as exploratory, descriptive, or explanatory and, in all cases, it is the basis to produce knowledge

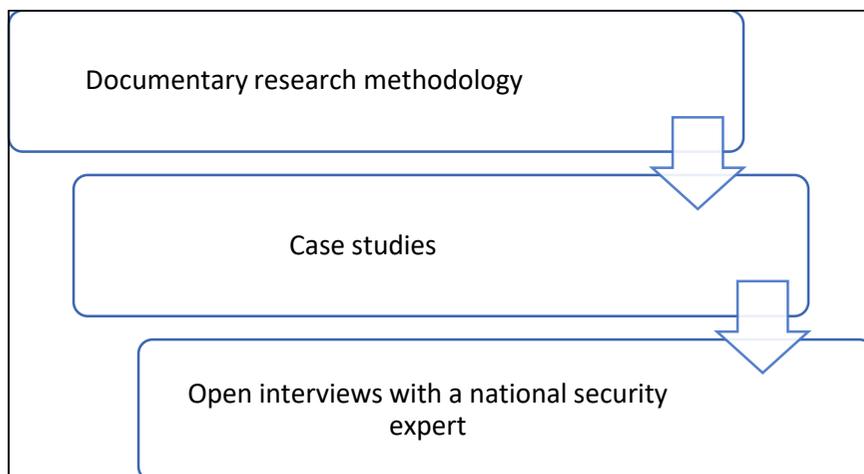
in different disciplines. This type of research is based on dialectical hermeneutics of proven sources, which ensures that they can be accessed at any time for analysis and comparison. In summary, the literature review was, for the authors of this research, an important tool to know the subject in depth, based on evidence in various fields of knowledge.

Next, the method of case studies was used as a condition of possibility to know the phenomenon of study in the theory and in the contextual reality where the war takes place. As is known in the scientific community, the case study method is a research strategy that allows a particular phenomenon to be explored in depth within its real context. As reported by Jiménez (2012), the study of the particularity and complexity of a singular case commonly serves to understand its activity in important circumstances. This inductive tool is widely used in the social sciences and is characterized by the systematic collection of data through multiple sources, which facilitates detailed and contextualized analysis.

Basically, three cases of PPPs in the context of war were analyzed. These cases were especially useful to understand complex situations where we sought to understand not only the what, but also the how and why of certain phenomena. By focusing on a specific case, researchers can identify patterns and generate hypotheses that can be explored in future research on the topic.

Finally, an open interview was conducted with a national security adviser, which is part of the formulation of the national resistance and liberation strategy developed by the Ukrainian army to defeat the invading troops. As it is logical to suppose, this character preferred to remain anonymous for security reasons.

Table 2. Methodological tools of the article



Source: prepared by the authors (2024)

Finally, all the information collected was processed by the research team through a polyphonic dialogue that connects, in an intertextual and reflexive way, the documentary sources, the results of the case study and the informed opinion of the authors of the article, under a close look at the critical analysis of the discourse, a methodology that allows the researcher to be committed to his or her own social reality, to overcome positivist neutrality and, on the contrary, to assume a legitimate political position in favor of vulnerable social groups that have been affected in the exercise of their human rights. In the words of van Dijk:

The critical analysis of political discourse goes even further: it takes an explicit position in favor of dominated groups, and offers analytical tools to enunciate, expose and criticize the discourse of the elite and its persuasive power in the construction of consensus and ideological hegemony. It therefore aspires to contribute to the conditions of social and political resistance against the often-subtle forms of domination in contemporary societies. (1998, p. 16)

Although this research is not a discourse analysis per se, this critical approach is a powerful tool for uncovering the ideologies, asymmetrical power relations, and rhetorical strategies behind the texts and speeches of the political leaders of Russian imperialism. When it is possible to critically address the language used, grammatical structures, assumptions, and meanings, researchers can reveal how political discourse constructs and perpetuates narratives, to legitimize the *status quo* and shape public opinion based on its strategic objectives. This type of analysis requires reflection on the part of the researcher, who must be aware of his or her own biases and ideologies and how they affect the interpretation of the discourse. In addition, critical analysis of political discourse must be firmly rooted in social, historical, and cultural contexts to avoid drawing conclusions that are simplistic or inconsistent with reality. Ultimately, this method provides valuable insights into power dynamics and struggles for meaning in the political realm, in the material and symbolic dimension.

3. Case study of PPPs in the context of the war in Ukraine 2022-2024

3.1. Microsoft case

During the ongoing war, Microsoft has played an important role in supporting Ukraine's national security strategy, particularly through its technological contributions and cybersecurity measures. According to a report by this corporation: "The company has provided more than \$540 million in free services, technical support, and grants to strengthen Ukraine's digital infrastructure" (Gills, 2023). This support is essential to ensure that Ukraine's government institutions and critical infrastructure can operate effectively despite the ongoing conflict. By moving critical government information to the cloud,

Microsoft helped mitigate the impact of several Russian cyberattacks and ensure the continuity of many public administration processes, even when physical capabilities are compromised by enemy action.

In addition, in the words of Burt (2022), collaboration between Microsoft and the Ukrainian authorities has been critical in addressing the growing cyber threats posed by Russian actors in the scenario of a hybrid war. Microsoft's Threat Intelligence Center (MSTIC) reported that more than 200 cyberattacks attributed to Russia were launched against Ukraine during the war, including 40 discrete cyberattacks targeting hundreds of computer systems (Burt, 2022). In response to these threats, Microsoft established secure lines of communication with Ukrainian cybersecurity officials, facilitating the sharing of real-time threat intelligence and technical countermeasures. This proactive management of the collaborative governance model has been recognized as an important factor in improving Ukraine's cyber defense capabilities during the critical period of the war (Advisor, 2024).

As we were able to consult with Advisor (2024), Microsoft's initiative also creates a broader framework for public-private partnerships in cybersecurity. As also noted in Microsoft's blog (Gills, 2023), indeed, the successful cooperation with the government of Ukraine to defend against Russian cyberattacks underscores the importance of international cooperation to strengthen Ukraine's cyber defense. This PPP enhances Ukraine's current security posture, while setting a precedent for future international partnerships in cybersecurity, demonstrating how technology companies can play a critical role in national security strategies in times of crisis.

However, for the authors of this scientific article, there are still many questions to be asked about the cooperation strategy between Microsoft and different bodies of the Ukrainian government, such as: What are the main achievements of the collaboration between Microsoft and the Ukrainian government in terms of security? How has Microsoft's investment in Ukraine's digitalization impacted during the war? What kind of cyberattacks has Ukraine faced and how has Microsoft responded? What specific recommendations has Microsoft made to protect Ukrainian organizations from cyberattacks? How has the relationship between Microsoft and Ukraine evolved since the start of the war? According to Advisor (2024), many of these questions cannot be answered openly because they are a sensitive issue that concerns national security.

3.2. Palantir Technologies Case

According to Bergengruen (2024), Palantir Technologies has become a key player in supporting Ukraine's national security strategy during the ongoing conflict, particularly through advanced military intelligence data analysis capabilities. Several of the company's software help improve situational awareness for Ukraine's military and government officials in the theater of operations of the war. As Franke and Söderström (2023) indicate, "Palantir's tools provide real-time data integration and analysis, critical for making informed decisions in the rapid pace of war" (2023, p. 4). Although these tools are not foolproof, they allow the Ukrainian military to better predict enemy movements and optimize resource allocation, thus increasing operational effectiveness on the battlefield.

All the information reviewed leaves no doubt that Palantir's work with the Ukrainian government extends beyond military applications to critical areas such as humanitarian aid and the reconstruction of technological infrastructure in

hardware and software, among others. A specialized national security report emphasized that: “The strategic partnership includes the use of Palantir technology in demining operations, which are essential to restore security and normalcy in war-torn areas” (Dessai, 2024, p. 12). Using artificial intelligence and data analytics, Palantir helps identify and prioritize demining sites, accelerate territorial recovery efforts, and improve overall civilian security. The combination of artificial intelligence with strategic thinking emphasizes the importance of integrating technology into national security strategies, particularly in the context of protracted conflicts.

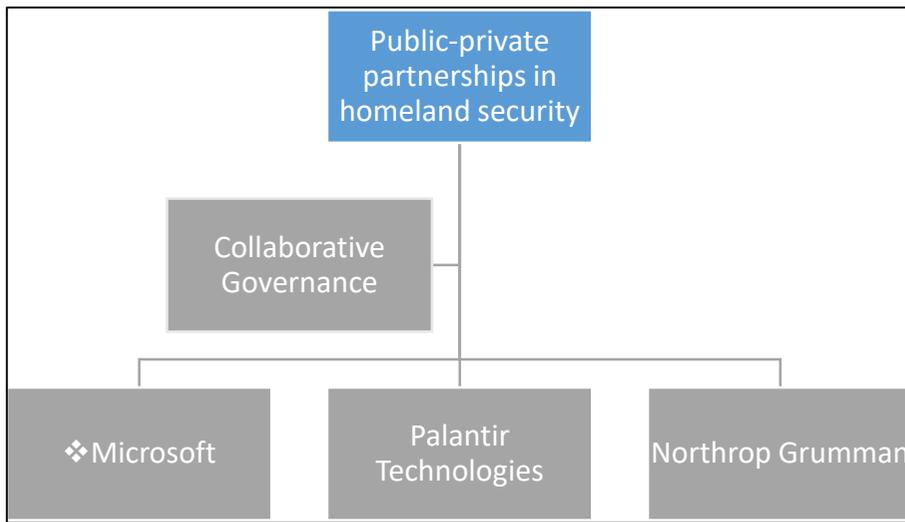
However, Palantir's involvement in Ukraine raises ethical considerations about data privacy and the implications of using advanced surveillance technologies in warfare. Critics rightly argue that: "The deployment of these technologies may lead to surveillance practices that are invasive of society, which could undermine civil liberties" (Franke & Söderström, 2023, p. 4). While the benefits of increased security and operational efficiency are clear, it is crucial that stakeholders address these ethical concerns and always ensure that the use of technology in national security respects human rights and democratic principles. It is therefore essential to balance national security needs with ethical considerations as Ukraine continues to navigate the complexities of war and the recovery of its capabilities.

3.3. Northrop Grumman Case

Finally, during the ongoing conflict with Russia, Northrop Grumman has made significant contributions to Ukraine's national security strategy, particularly through initiatives to strengthen local defense capabilities (Advisor, 2024). The company recently announced plans to build ammunition production facilities in

Ukraine, with the aim of increasing the country's self-sufficiency in the production of defense inputs. According to Price (2024), Northrop Grumman's partnership with the government of Ukraine will focus on the co-production of medium-caliber munitions, which are essential to sustain military operations on the battlefield. This cooperation aims to meet current military needs and seeks to develop Ukraine's long-term defense industrial base, thereby increasing its ability to protect itself against external threats (Advisor, 2024).

Table 4. APP that participates in Ukraine's national security strategy in the war



Source: prepared by the authors (2024)

However, Northrop Grumman's involvement in Ukraine raises an important consideration about the influence of foreign defense contractors in conflict zones. Critically, while such partnerships can provide the necessary support, they can also lead to extreme reliance on foreign technology and knowledge, which, under certain adverse geopolitical conditions, could undermine Ukraine's defense

strategy. For these reasons, Advisor (2024) is of the opinion that co-production agreements should be carefully managed to ensure that they do not limit Ukraine's strategic autonomy or create excessive dependence on external entities. In this context, Ukraine's national security policy must find a way to balance the immediate interests of increased military capability with the need for a long-term sustainable and independent defense strategy.

In short, the balance of costs and benefits of PPPs is in Ukraine's favour. Microsoft, Palantir Technologies, and Northrop Grumman have made significant contributions to national security during the war. Microsoft has provided more than \$400 million in aid, including technical support and cybersecurity, to help Ukraine strengthen its digital infrastructure and defend against Russian cyberattacks (Gills, 2023). Palantir Technologies provides data analytics tools that enable the Ukrainian military to immediately improve decision-making to optimize military and intelligence operations. For its part, Northrop Grumman announced plans to build an ammunition plant in Ukraine, which will eventually improve the country's defense capabilities, while promoting relative self-sufficiency in weapons production. Therefore, this joint effort strengthens national technology, data analytics, and industrial manufacturing capabilities to strengthen Ukraine's strategy to defend against hybrid threats.

4. Analysis and discussion of results

As stated in the introduction of this work, the general objective of the research: to analyze the political implications of public-private partnerships on Ukraine's national security, is expressed or broken down into three questions that were answered dialogically by a high-level national security advisor, who was

kind enough to respond to the interview of the authors of the article, held in July 2024. The central excerpts of the interview are presented below, together with the reflective response of the authors of the article.

1. In response to the first question posed: How have public-private PPP partnerships influenced the formulation and implementation of national security policies in Ukraine during the war with Russia?

PPPs have been crucial in accelerating the development and deployment of advanced defense technologies in Ukraine. Private companies, often more agile than government agencies, have been instrumental in integrating cutting-edge technologies, such as drone surveillance and cybersecurity measures, into national defense strategy. The involvement of private partners has allowed the Ukrainian government to leverage additional resources, such as funding, expertise, and technology, that it would not have otherwise had access to. This has been essential in a time of war when national resources are severely limited. PPPs have undoubtedly enabled Ukraine to adapt more quickly to the changing dynamics of war and threats. Private sector participation has facilitated faster decision-making processes and the implementation of strategic initiatives, which is critical in a high-risk conflict environment (Advisor, 2024).

It is not clear from the response of Advisor (2024), whether PPPs, beyond their battlefield support in terms of cybersecurity, management and provision of combat technologies or continuous advice to troops, actively participate, together with the corresponding instances of the government of Ukraine, in the formulation of national security policies and strategies that have been implemented in the course of the war, in the period 2022-2024. What I do know is that their support has been crucial in dealing with the material and virtual threats posed by the

invading army to bring Ukraine to its knees, so there is reason to assume that soon the determined action of the PPPs will gradually increase in other dimensions of the defense and national security sector.

2. As for the second question: What political challenges have public-private partnerships in Ukraine faced in addressing national security needs in a context of armed conflict? Advisor (2024) literally replied that:

One of the main challenges has been ensuring that private sector objectives align with national security priorities. In some cases, private entities may prioritize profits or specific business interests, which do not always align perfectly with the country's national security objectives. The legal framework governing PPPs in Ukraine, in a context of war, can be complex and fraught with challenges for international private companies. (2024, p. 02)

Issues such as corporate social responsibility, control of patented technologies, and the degree of private sector involvement in direct combat or intelligence operations pose significant challenges and must be always decided by the sovereign government of Ukraine, in accordance with the general will of the country. In this context, there is often a delicate balance between maintaining operational security and ensuring transparency in PPPs. The Ukrainian public demands accountability, especially with regard to how resources are used, and decisions are made during the war, which may conflict with the need to maintain the confidentiality of certain strategic details, typical of national security policy.

3. The third and final question: How has the involvement of private actors in national security affected the balance of power and accountability between the Ukrainian government and companies in the defense and security sector? By its very nature, this question was aimed at revealing the tensions that commonly occur

between private enterprise, the national government and an informed public opinion that insists on valuing transparency and honesty in the management of public goods, much more so in a context of war where every hryvnia⁶ counts and, Definitely, the efficient use of the few available resources can make the difference between national victory or defeat.

As explained in detail by Advisor (2024), the critical role of private companies in defense and security has potentially increased their influence over national security policies and, to some extent, defines defense priorities. This can lead to power shifts in which certain private entities gain significant influence over government decisions and public policymaking.

The government of Ukraine is fully aware of the fact that the participation of private actors requires solid legal and institutional mechanisms to ensure accountability, particularly in the management of public funds, compliance with legal and ethical standards and the execution of operations. At this difficult time in the war, the challenge is to create oversight structures that effectively monitor and regulate private sector participation, without hindering its ability to contribute effectively to national security. Either way, there is a risk that governments will rely on private entities, which could compromise the state's autonomy in matters of national security. Ensuring that the government retains ultimate control and decision-making power is critical to maintaining sovereignty and democracy while ensuring that national security interests are not subordinated to private interests (Advisor, 2024).

⁶ The hryvnia is legal tender in Ukraine.

In general terms, many conclusions (theoretical and practical) emerge from the hermeneutical reading of the authoritative opinions of Advisor (2024). On a practical level, everything seems to indicate that the Ukrainian national security policy developed in the heat of the war responds to a neoliberal approach that tends to privatize many strategic areas of security and defense, even more so in terms of military technologies. This situation is neither good nor bad, everything will depend, teleologically speaking, on whether the efforts of the PPPs give rise to the national victory of Ukraine in the face of the onslaught of Russian imperialism in the 21st century.

In theoretical terms, the information obtained in the research allows us to affirm that the national security strategy developed by Ukraine, in the period 2022-2024, is congruent with the theoretical developments handled in this research to interpret the role of PPPs in security and defense policy in general. In short, it is a public policy that until now has been justified in the search for collaborative governance, in the theory of the interdependence of the public sector and private enterprise and, fundamentally, in shared risks.

Conclusions and recommendations

Public-private partnerships (PPPs) have proven to be an important part of Ukraine's national security, especially in the face of the war that erupted in 2022. Through the gradual implementation of public-private PPP partnerships, the Kiev government was able to improve military infrastructure, develop new defense technologies, and optimize military training (Advisor, 2024). This strategic approach not only strengthens the state's capacity to respond to external aggression, but also fosters a sense of solidarity and cooperation between the

public and private sectors (domestic and international) in times that alter the course of Ukraine's history as a free and sovereign nation (Center for Preventive Action, 2024).

In critical perspective, the effectiveness of public-private partnerships in Ukraine is not without its problems. The war created an unstable environment that made it difficult to implement and maintain several PPP cooperation projects. In this context of increasing entropy, factors such as legal uncertainty, administrative corruption and the risk of total war limit the participation of the private sector in certain key areas. Likewise, the lack of a clear legal framework, in some areas of strategic cooperation, has generated mistrust among investors, hindering the development of PPP projects that could have made a significant contribution to national security. Addressing these issues, at least academically, is critical to maximizing the future potential of PPPs.

Despite these challenges, PPPs show great potential for innovation in the management of national security in Ukraine and in the world. In fact, as Advisor's expert opinion (2024) ratifies, cooperation between the government and technology companies allows Ukraine to strengthen its cybersecurity, a key aspect of the current conflict. In this dynamic landscape, corporate engagement in protecting critical infrastructure and sharing cyber threat intelligence is critical to maintaining national resilience. This cooperation model, which is also fully in line with NATO policies, can serve as a reference for other neighboring countries facing similar situations and, at the same time, highlights the importance of integrating private sector resources into national security strategies (Soroka *et al.*, 2023).

The qualitative results obtained in this research allow the authors of the article to affirm that research on PPPs in the context of the war in Ukraine reveals important opportunities and challenges. The future ability of these partnerships to enhance national security depends largely on being able to overcome the structural barriers that exist in political, legal, and institutional terms, and to create an enabling regulatory environment. As Ukraine continues to face aggression against its national sovereignty, strengthening the strategy of effective public-private partnerships is critical for the country's defense and for its long-term recovery and development. Ukraine's experience can provide valuable lessons on how to strategically use public-private partnerships in crisis situations to enhance the national security of countries near or far.

To encourage debate and academic reflection, the authors of this article recommend to national security policymakers, political advisors, experts, and scientists in charge of the study of these or similar issues, the following three ideas:

First, it is very important to create a clear legal framework to promote cooperation between the public and private sectors. This includes developing regulations that define roles, responsibilities, and accountability mechanisms while fostering private sector trust and participation in national security programs. A well-structured framework will allow public-private partnerships to function more effectively and ensure the proper integration of private sector resources and capabilities into the national defense strategy.

Secondly, continuous training must be promoted for the actors responsible for defining national security policy, within the framework of the development of strategic capacities, both in the public and private sectors. This includes implementing training programs that meet specific national security needs, as well

as a space for dialogue and collaboration to share knowledge and experiences. By permanently strengthening skills and abilities in both PPP sectors, it will be possible to improve the response to recurring threats and optimize resource management in crisis situations.

Third, it is essential to foster innovation in national security through collaboration with technology companies and *startups*. The war in Ukraine has shown the importance of having advanced technologies for comprehensive defense and cybersecurity. With a policy of encouraging scientific research and joint development between the government and the private sector, innovative solutions can be created that respond to emerging challenges in the field of national security. This will not only improve the ability to respond to threats, but will also contribute to Ukraine's long-term resilience, in the most difficult times in its history.

References

- Advisor, N. S. (15 de July de 2024). Public-private partnerships in homeland security. A case study in the context of the war in Ukraine: 2022-2024. (R. team, Entrevistador)
- Arias, F. G. (2009). *El proyecto de investigación*. Caracas: Editorial Episteme.
- Barandiarán, X., Canel, M.-J., & Bouckaert, G. (2022). ¿Qué mueve a confiar en la gobernanza colaborativa? Análisis de un programa gubernamental en el País Vasco. *Revista Española de Ciencia Política*, (60), 251-275.
- BBC News Mundo. (26 de febrero de 2022). *Rusia y Ucrania: qué pasó en Crimea en 2014 (y por qué importa ahora)*. Obtenido de <https://www.bbc.com/mundo/noticias-internacional-60500020>
- Bergengruen, V. (08 de February de 2024). *How Tech Giants Turned Ukraine Into an AI War Lab*. Obtenido de Time: <https://time.com/6691662/ai-ukraine-war-palantir/>

- Burt, T. (27 de abril de 2022). *The hybrid war in Ukraine*. Obtenido de Microsoft blogs: <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>
- Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92 (01), 43-62. DOI:10.1111/1468-2346.12504.
- Center for Preventive Action. (20 de mayo de 2024). *War in Ukraine*. Obtenido de Global Conflict Tracker: <https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine>
- Dessai, T. (15 de May de 2024). *Four Defense Technology Companies Transforming National Security*. Obtenido de Global X: <https://www.globalxetfs.com/four-defense-technology-companies-transforming-national-security/>
- Dodds, K., Taylor, Z., Akbari, A., Castán, V., Detterbeck, K., Inverardi-Ferri, C., & Ok Lee, K. (2023). The Russian invasion of Ukraine: implications for politics, territory and governance. *Territory, Politics, Governance*, 11 (08), 1519–1536. <https://doi.org/10.1080/21622671.2023.2256119>.
- Franke, U., & Söderström, J. (5 de september de 2023). *Star tech enterprise: Emerging technologies in Russia's war on Ukraine*. Obtenido de European Council on Foreign Relations: <https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/>
- Ganguli, I., & Waldinger, F. (12 de agosto de 2023). *The impact of the war in Ukraine on science and universities*. Obtenido de VOX EU: <https://cepr.org/voxeu/columns/impact-war-ukraine-science-and-universities>
- Gills, S. (20 de november de 2023). *Accelerating AUKUS: Securing Multilateral and Multiagency Collaboration*. Obtenido de Microsoft: <https://devblogs.microsoft.com/azuregov/accelerating-aukus/>
- Gobierno de España. (2016). *Estrategia de Seguridad Nacional Un proyecto compartido*. Madrid: Presidencia del Gobierno.
- Jiménez, V. (2012). El estudio de caso y su implementación en la investigación. *Revista Internacional de Investigación en Ciencias Sociales*, 08 (01), 141-150. <http://scielo.iics.una.py/pdf/riics/v8n1/v8n1a09.pdf>.

Norman, J. (21 de February de 2024). *Humanitarian principles are under fire in Ukraine*. Obtenido de Danish Institute for International Studies: <https://www.diiis.dk/en/research/humanitarian-principles-are-fire-in-ukraine#:~:text=A%20lack%20of%20clarity,neutrality%20as%20a%20relevant%20principle>

Novytskyi, H. V., Shcherbyna, L., Pyvovarov, V., Kartamysheva, O., & Lysodyed, O. (2022). Ukraine's constitutional doctrine of national security Miles Doctus. *Revista Científica General José María Córdova*, 20 (38), 387-406. <https://doi.org/10.21830/19006586.902>.

Oficina Internacional del Trabajo. (2008). *Comisión de Cooperación Técnica*. Ginebra: Organización Internacional del Trabajo.

Polski Instytut Spraw Międzynarodowych. (15 de april de 2024). *Regional Cooperation in Central Europe after Russia's Aggression against Ukraine*. Obtenido de <https://pism.pl/webroot/upload/files/Raport/Report%20Regional%20Cooperation.pdf>

Price, P. (22 de July de 2024). *Key Investments to Ensure Mission Readiness*. Obtenido de Northrop Grumman: <https://www.northropgrumman.com/what-we-do/advanced-weapons/key-investments-to-ensure-mission-readiness>

Rincón, L. (2012). *Introducción a la teoría de riesgo*. México DF: Facultad de Ciencias UNAM. <http://lya.fciencias.unam.mx/lars/libros/riesgo.pdf>.

Ruppert, K. (21 de February de 2024). *In Search of a Formula for Lasting Peace in Ukraine. Investing in a security structure and institutions that will disincentivize further Russian aggression is key*. Obtenido de United States Institute of Peace: <https://www.usip.org/publications/2024/02/search-formula-lasting-peace-ukraine>

Soroka, L., Danylenko, A., Sokiran, M., Levchenko, D., & Zubko, O. (2023). Public-private collaboration for national security: challenges and opportunities. *Amazonia Investiga*, 12 (70), 43-50. <https://doi.org/10.34069/AI/2023.70.10.4>.

Tokatlian, J., & Pardo, R. (1990). La teoría de la interdependencia: ¿Un paradigma alternativo al realismo? *Estudios Internacionales*, 23 (91), p. 339-382. <https://doi.org/10.5354/0719-3769.1990.15518>.

Unión Internacional de Telecomunicaciones, Banco Mundial, Secretaría de la Commonwealth, Organización de Telecomunicaciones de la Commonwealth y Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN. (2018). *Guía para la elaboración de una estrategia nacional de ciberseguridad Participación estratégica en la ciberseguridad*. New York: UIT.

United Nations. (12 de May de 2024). *Report on the Human Rights Situation in Ukraine*. Obtenido de <https://www.ohchr.org/sites/default/files/documents/countries/ukraine/2024/24-07-02-OHCHR-39th-periodic-report-Ukraine.pdf>

Van Dijk, T. A. (1998). Prologo. En I. Vasilachis de Gialdino, *La construcción de representaciones sociales Discurso político y prensa escrita* (págs. 15-19). Buenos Aires: Gedisa editorial.

Van Dijk, T. A. (2009). *Discurso y Poder*. Barcelona: Editorial Gedisa

Note: The authors declare that they have no situations that represent a real, potential or evident conflict of interest, of an academic, financial, intellectual or intellectual property nature related to the content of the manuscript of the previously identified project, in relation to its publication. Likewise, they declare that the work is original, has not been published partially or totally in another means of dissemination, no ideas, formulations, quotes or diverse illustrations were used, extracted from different sources, without clearly and strictly mentioning their origin and without being duly referenced in the corresponding bibliography.