For citation:
URTMELIDZE, T. (2025). The role of intellectual property in addressing state security challenges. *Uluslararası Sosyal Bilimler ve Eğitim Dergisi – USBED 7*(12), 215–230. https://doi.org/10.5281/zenodo.15023899, https://dergipark.org.tr/tr/pub/usbed

The role of intellectual property in addressing state security challenges

Tamazi URTMELIDZE

Associate Professor; Georgian Technical University, Law and International relations, 0171, Tbilisi, Georgia
E-mail: t.urtmelidze@gtu.ge *ORCID: 0009-0002-3916-0979*

Article Type:	Research Article
Submission Date:	20/01/2025
Revision Dates:	23/01/2025 (Editor r.), 05/03/2025 (Minor r.)
Acceptance Date:	14/03/2025

Ethical Statement

✓ Ethical approval was not received for the article. The author declares that his work is not subject to ethics committee approval.

Researchers' contribution to the study

Author's contribution: Wrote the article, collected data and analyzed/reported results.

Conflict of interest

The authors declare that there is no possible conflict of interest in this study.

Similarity

This study was scanned in the iThenticate program. The final similarity rate is 6 %.

The role of intellectual property in addressing state security challenges

Abstract

This study explores the critical role of intellectual property (IP) in addressing national security challenges, focusing on the strategic integration of IP into state policies. The analysis highlights how technological advancements, supported by robust IP frameworks, strengthen economic security and enhance national defense capabilities. Key examples from global powers such as the United States, China, Russia, and Georgia demonstrate how IP protection fosters innovation, technological sovereignty, and strategic advantages. The study emphasizes that hybrid threats, including cyberattacks and disinformation campaigns, have reshaped global security dynamics. Case studies illustrate how countries leverage IP to advance critical technologies such as artificial intelligence and hypersonic weapons, ensuring competitive advantages in defense and international influence. The findings underscore the need for adaptive policies that balance technological innovation with national security priorities. By investing in research and development, fostering innovation ecosystems, and strengthening IP protection, nations can navigate the evolving landscape of geopolitical competition and hybrid warfare. This research concludes that IP is not only an economic asset but also a vital component of state security strategies, requiring continuous adaptation to address emerging global challenges effectively.

Keywords: Intellectual property, State security, Hybrid warfare, Technological sovereignty, Cybersecurity

EXTENDED ABSTRACT

Intellectual Property (IP) plays a vital role in strengthening national security by fostering innovation, technological advancement, and economic stability. As global powers compete for technological dominance, IP protection has become a strategic tool to secure critical assets and maintain geopolitical influence. This study examines how nations such as the United States, China, Russia, and Georgia integrate IP into their security frameworks, ensuring technological sovereignty while addressing hybrid threats such as cyberattacks and disinformation campaigns.

This research is grounded in techno-nationalism and hybrid warfare. Techno-nationalism underscores the importance of a country's ability to innovate independently, linking technological capabilities to economic and security outcomes. Hybrid warfare highlights the increasing use of non-conventional threats—such as cyberattacks, artificial intelligence-driven disinformation, and economic coercion—to achieve strategic goals. These frameworks demonstrate how intellectual property serves as both a defensive and offensive asset in modern geopolitical competition.

Several key concepts define the relationship between IP and state security:

- Technological Sovereignty: The ability of a nation to develop and control its own technological resources, reducing dependency on foreign innovation.
- Economic Security: The role of innovation-driven industries in maintaining stable economic growth and resilience against global disruptions.
- Hybrid Threats: The use of cyber warfare, misinformation, and economic leverage to undermine national stability and global order.
- Strategic IP Management: The implementation of policies that safeguard critical technologies from espionage, theft, or foreign control.

Existing literature highlights the intersection of IP and security in various geopolitical contexts. Franke & Torreblanca (2021) emphasize how global competition is shifting towards technological dominance, making IP a key factor in national security. Kistauri et al. (2018) analyze how innovation-driven economies gain competitive advantages, reinforcing their security infrastructure. Reports from the U.S. National Security Strategy (2022) and China's State Council Program on Artificial Intelligence (2017) further illustrate how global superpowers integrate IP into their defense and economic policies. Russia's security strategy highlights cyber threats and information control, while

Georgia's national security approach underscores cybersecurity resilience. These studies demonstrate the growing importance of IP as a strategic asset in global security frameworks.

This study adopts a qualitative research approach, using case studies, policy analysis, and comparative methods. Primary sources include national security strategies, government reports, and academic research on IP and state security. The study evaluates how major global powers structure their IP policies and assesses their impact on security dynamics. A comparative analysis identifies similarities and differences in national strategies, focusing on innovation ecosystems, economic security, and hybrid threats.

Findings indicate that strong IP protection supports national security by fostering innovation, encouraging investment in research and development, and securing critical technologies. The United States prioritizes technological leadership through a combination of public-private partnerships, ensuring that emerging technologies such as AI, microelectronics, and quantum computing remain under secure development. China's state-driven approach aims to dominate global innovation, with policies promoting domestic artificial intelligence, automation, and cyber capabilities. The Russian Federation emphasizes cybersecurity and information control, integrating IP into strategies that counter Western technological influence. Georgia, as a smaller but strategically significant actor, focuses on cybersecurity resilience, particularly in response to Russian cyberattacks during the 2008 war.

Hybrid warfare has blurred the lines between conventional and unconventional security threats. The Russia-Ukraine war serves as a prime example of how cyberattacks, disinformation campaigns, and technological disruptions are deployed alongside traditional military operations. China's approach to cognitive warfare—using artificial intelligence to manipulate social media narratives—further exemplifies how states weaponize IP-driven technologies to influence public perception and political outcomes.

Key challenges in integrating IP into national security include the trade-off between economic openness and security control. While nations must engage in global markets to foster innovation, overreliance on foreign technology can create vulnerabilities. Countries must develop adaptive IP policies that balance innovation with risk mitigation, ensuring that their critical technological assets remain secure yet competitive in international markets.

This study underscores that intellectual property is no longer solely an economic tool but a fundamental pillar of national security. As technological competition intensifies, countries must adopt dynamic IP policies that secure innovation while mitigating security risks. The following recommendations emerge from the analysis:

1. Investment in Research and Development (R&D): Governments should allocate significant resources to innovation-driven sectors, ensuring technological leadership in critical areas such as AI, cybersecurity, and advanced computing.
2. Strengthening Public-Private Partnerships: Close collaboration between governments, academic institutions, and private enterprises is crucial for safeguarding IP and maintaining technological leadership.
3. Enhancing IP Protection Mechanisms: Countries must enforce stricter IP protection laws, prevent espionage, and counter technology theft through strategic security policies.
4. Building Cybersecurity Resilience: Given the rising threat of hybrid warfare, nations must develop stronger cyber defenses to protect critical infrastructure and sensitive information.
5. Balancing Economic Openness with Security: Governments must carefully navigate global trade and investment policies, ensuring that foreign influence does not compromise national security interests.

In conclusion, IP is a strategic asset that shapes global power dynamics. Nations that successfully integrate IP into their security strategies will maintain technological sovereignty, economic resilience, and geopolitical influence in an increasingly contested international order. Future research should explore the role of international cooperation in IP security, as well as the impact of emerging technologies on global security frameworks.

INTRODUCTION

The role of intellectual property (IP) in state security has become increasingly important in today's complex geopolitical landscape. With rapid advancements in technology and innovation, nations are heavily investing in IP protection to maintain economic stability and ensure national defense. Intellectual property, including patents, trademarks, and trade secrets, plays a critical role in fostering technological advancements and addressing global security challenges. This study aims to explore the intersection of intellectual property and national security by analyzing the strategies and policies of key global players, including the United States, China, Russia, and Georgia. The importance of IP lies not only in its ability to promote economic growth but also in its capacity to strengthen a nation's defense mechanisms. By fostering innovation and securing technological sovereignty, countries can achieve competitive advantages in global markets and enhance their security frameworks. Technological sovereignty, in particular, has emerged as a vital issue, as countries seek to reduce reliance on external technologies and develop homegrown solutions. This focus underscores the relationship between economic strength and national security, emphasizing the need for robust IP frameworks. The conceptual framework of this study draws on the principles of techno-nationalism and hybrid warfare. Techno-nationalism highlights the linkage between technological innovation and a nation's security, economic prosperity, and global influence. On the other hand, hybrid warfare demonstrates how emerging technologies, such as artificial intelligence and cyber capabilities, are utilized in conflicts to achieve strategic goals without direct confrontation. Both concepts are integral to understanding how nations leverage IP to address evolving security threats. From a methodological perspective, this study analyzes policy documents, case studies, and global practices to provide a comprehensive understanding of the role of IP in state security. Examples from the U.S. National Security Strategy, China's innovation-driven defense policies, and Russia's emphasis on technological superiority illustrate the strategic importance of IP in addressing both traditional and non-traditional security threats. In conclusion, this study highlights the necessity of aligning intellectual property strategies with national security goals. As countries face challenges such as hybrid threats, cyberattacks, and global competition, the integration of IP into state policies becomes indispensable. By examining the approaches of leading nations, this research contributes to a deeper understanding of how IP can serve as a cornerstone of both economic development and national security.

Method

This study adopts a qualitative approach to examine the role of intellectual property (IP) in state security. Data sources include national security strategies, government reports, and academic literature focusing on IP and national security. Case studies from the United States, China, Russia, and Georgia provide insights into how IP supports economic growth, technological sovereignty, and hybrid warfare resilience. A comparative analysis identifies patterns in leveraging IP for innovation and security, emphasizing themes like economic stability, technological advancements, and hybrid threats such as cyberattacks. Theoretical frameworks, including techno-nationalism and

hybrid warfare, are applied to contextualize the findings. This structured methodology enables a comprehensive understanding of IP's strategic role in addressing global security challenges.

IP AND STATE SECURITY DYNAMICS

Security systems of the countries, as one of the most important fields, require daily updating. Technologies, and intellectual property objects such as patents, know-how, software, etc., have an increasing impact on the security of the country. Economic security is closely related to the innovative economic capabilities of the country.

As of today, the countries achieve a competitive advantage by introducing innovative technologies. They establish new strategies, master efficient production methods, invest in updating knowledge, etc. Therefore, the core of structural transformations in the XXI century is the development of an innovative economy. Today, the basis for the effective functioning of the economy is an uninterrupted process of replacing outdated technologies with new ones, and the development of resource-saving technologies. Information technologies (IT) deserve special attention. Their development is a strategic direction of economic security. This process has a significant impact not only on the quality of material resources but also on intellectual capital and leads to Bringing the phenomenon of knowledge to the fore. Strong protection of intellectual property encourages foreign and domestic investment and promotes an innovative environment, which is crucial for economic stability and growth. Economically strong countries are better equipped to defend their security and position in the international arena. Technological sovereignty becomes an existential issue as the state actors dominate the global market, multipolarity and unilateralism replace multilateralism, and great states subjugate technologically interdependent countries as they seek to create spheres of influence (Franke & Torreblanca, 2021). Global practice shows that the quality of economic security largely depends on the adoption of technological solutions based on innovations in the economy and increased competitiveness. As innovation and competitiveness should be considered together and not separately, as an important resource for modernization and strengthening of economic security, it is precisely the innovation that provides new opportunities for optimal formation of economic security at the level of international standards (Kistauri et al., 2018).

We will focus on the approaches of the USA, China, the Russian Federation, and Georgia to the issues of intellectual property, innovation, and new technologies from the perspective of national policy, in order to clearly demonstrate the great importance that modern countries attach to intellectual property in terms of global and individual security.

National strategic approaches are based on the essential advantages of nations, such as creativity, resilience, and strength; technological leadership, and economic dynamism. Special attention is paid to the protection of intellectual property, acquisition of technological advantages, use of state-of-the-art technologies and development of markets with new innovative products, creation of jobs.

The U.S. National Security Strategy 2022 outlines the country's vision for the global security architecture. Democracies and autocracies are competing to determine which system of governance best serves the needs of their people and the world. Competition is growing for the development and deployment of key technologies that will transform security and the economy. Global cooperation in the areas of common interest is weakening, yet the need for such cooperation earns existential significance. The U.S. National Strategy considers Russia to be a direct threat to the free and open international system, recklessly violating the basic laws of the modern international order, as demonstrated by its brutal war of aggression against Ukraine. China, by contrast, is the only competitor with both the intent to change the international order and the growing economic, diplomatic, military, and technological power to achieve this goal.

The U.S. National Security Strategy refers to the challenges of adversary technology and cybersecurity. We must complement the innovative power of the private sector with a modern industrial strategy that includes strategic public investments in the American workforce, as well as in strategic industries and supply chains, especially in critical and emerging technologies such as microelectronics, advanced computing, biotechnology, clean energy, and advanced telecommunications (The White House, 2022).

According to the U.S. National Security Strategy, technology is central to contemporary geopolitical competition and in the future of U.S. national security, economy, and democracy. The leadership of the United States and its allies in technology and innovation has long been the foundation of our economic prosperity and military strength. Over the next decade, critical and emerging technologies will reshape the economy, transform the military forces, and reshape the world, according to the U.S. National Security Strategy (The White House, 2022).

The State Safety (Security) Policy of the People's Republic of China states that in order to strengthen China's national defense and armed forces in the new era, it is necessary to carefully implement Xi Jinping's ideas about the military strategy, to continue the growth of the political loyalty of the armed forces, strengthen them through reforms and technology, manage them following the law, and focus on the ability to fight and win. Efforts will be directed towards the comprehensive development of mechanization and informatization, accelerating the intellectual development of the armed forces, creating a modernized structure of the armed forces with Chinese characteristics, improving and developing the socialist military institutions with Chinese characteristics, and constantly enhancing the capabilities to fulfill the missions and tasks of the new era (Ministry of National Defense of the People's Republic of China, n.d.).

In 2017, the Chinese Government launched the State Council Program to develop a new generation of artificial intelligence, which aims to create China's advantage as a pioneer by fully mobilizing and utilizing national research and development resources in both the public and private sectors. The economic state approach to the promotion of artificial intelligence allows Beijing to achieve faster effects in the economic, social, and security areas. Beijing has made the use of artificial

intelligence in the military training of the People's Liberation Army a state policy to compete on equal terms with Washington in the development of new technologies.

There are three key components for the creation of a new comprehensive state system of China: (1) adoption of the state economic measures to stimulate domestically developing strategic industries; (2) reforming the institutional mechanisms of science and technology; and (3) mobilizing and involving the private sector in state technological development.

In 2018, the trade war between the USA and China and US sanctions against Chinese technology companies forced the government to realize that in order to introduce innovations into the country's economy, it is necessary to create a state-integrated system.

Since the onsets of the millennium, China has overtaken Germany and Japan to become the world's second-largest Research and Development (R&D) transactor after the USA, and the gap in Research and Development (R&D) spending between the USA and China is rapidly closing, despite modest increases in U.S. spending since 2000. The drive for innovative development requires significant increases in Research and Development (R&D) investment across all sectors of the economy. From 2016 to 2023, China's R&D spending is expected to grow at a double-digit rate. In 2019, total R&D spending exceeded 2 trillion Chinese yuan (CNY). By 2022, this figure will reach 3.087 trillion CNY, an increase of 10.4% compared to the previous year.

Since then, institutional reforms have been implemented in the high-tech sector of China, laying the foundation for the creation of a national innovation system and promoting the integration of technological research and development with its market commercialization.

The foreign policy of the Russian Federation is focused on the development of intellectual property, especially new technologies. It outlines priority areas: to ensure international information security, its threats and strengthen Russia's sovereignty in global cyberspace, the Russian Federation intends to pay priority attention to: taking political, diplomatic, and other measures aimed at countering the weaponization of global cyberspace, the policy of states hostile to use of information and communication technologies, interference in the internal affairs of states for military purposes, as well as limiting access to advanced information and communication technologies by other states and strengthening their technological dependence (Ministry of Foreign Affairs of the Russian Federation, 2023).

The priorities of the foreign policy of the Russian Federation include the structural transformation of the world economy, its transition to a new technological base (including the introduction of artificial intelligence technologies, the latest information and communication, energy, biological technologies, and nanotechnologies), growth of national self-awareness, cultural and civilizational diversity, and other objective factors that accelerate the process of movement of the development potential to new centers of economic growth and geopolitical influence, and contribute to the democratization of the international relations.

In the Russian narratives, the liberal-democratic values, along with the Western technological superiority and mechanisms of "global interdependence", such as standardization and unification, are presented as tools that the West uses to exert control over the rest of the world. The Russian leadership is convinced that the countries of the Global South share the goals of Russia, which include: advocating for limited access to technologies; creating alternative mechanisms for international transactions, and accepting the national currencies in international settlements. Russia identifies the BRICS (Brazil, Russia, India China, and South Africa) countries as its primary partners within the Global South.

The National Security Strategy of Georgia lists the goals that the country has set, as well as the challenges in the context of national security. Improvement of the high rate of economic growth is a priority for Georgia's security. An inadequate pace of economic development, a sharp decrease in state revenues, and an extreme increase in unemployment may contribute to social tension and threaten the development, stability, and national security of the country. Maintaining and increasing the competitiveness of the country's economy and its citizens is a priority for the long-term economic security of Georgia. Along with the critical infrastructure reliance of the state on information technologies, the challenges related to the protection of Georgia's information space are increasing. During the Russian-Georgian war of 2008, the Russian Federation launched targeted and massive cyberattacks against Georgia, in parallel with land, air, and marine attacks. These cyberattacks demonstrated that the protection of cyberspace is as important to national security as the protection of land, air, and sea areas (Ministry of Foreign Affairs of Georgia, n.d.).

National security depends significantly on the economic situation of the country. Moreover, economic capabilities directly affect the country's military strength, social and demographic situation, etc. From the point of view of national security, the mutual influence of economics and politics is of particular and perhaps essential significance (Gakhokidze, 2007).

The countries need to invest in technology and research and development, as this is what gives them priority. National security policy, also known as national security doctrine, is the framework that describes how a country will ensure national security, a high level of citizen protection, and law and order. National security policy is a formal description by a country of its guiding principles, values, interests, goals, strategic environment, threats, risks, and challenges for protection and promotion of national security. As a rule, national security policy is based on the country's constitution, other fundamental documents, and legislation. The policy explains the behavior and responsibilities of state institutions in terms of ensuring security and protecting the rule of law (Geneva Center for Security Sector Governance, n.d.).

GLOBAL PERSPECTIVES ON HYBRID THREATS

The concept of hybrid threats has long been established in global security policy. When discussing the role of hybrid warfare in politics, it is important to understand what hybrid warfare is in general. Hybrid warfare is a military strategy that uses political warfare and combines conventional, irregular, and cyber warfare with other methods of influence, such as fake news (disinformation), diplomatic disruption, and foreign interference in elections.

Hybrid warfare could be a new form of global competition. It is also known as the "blue zone" of conflict and is a feature of the news almost every day. "Hybrid warfare uses non-military means to achieve military goals, primarily through tactical methods such as cyberattacks, fake news campaigns, and espionage."

The Russian concept of "non-linear warfare defines hybrid warfare as "deployment of conventional and irregular armed forces combined with psychological, economic, political, and cyber-attacks" (Chitadze, 2019).

The multifaceted nature of hybrid threats requires a rapid and qualified response to them, which is incredible without implementation of the innovative policies. In recent years, digital technologies have become important for governments and organizations. Rapid development and implementation of digital technologies have changed the way governments and organizations work, communicate, and provide services.

In the context of hybrid warfare, digital technologies can be both a tool and a target in conflict. Their impact on digital ecosystems can be significant in terms of humanitarian, social, and economic consequences. Digital technologies are among the most vulnerable during armed conflicts.

Within the framework of hybrid warfare research, it is noteworthy to analyze the nature of hybrid operations during the Russian-Ukrainian war. The studies confirm that this confrontation has somewhat changed the nature and tactics of the hybrid threat - cyber threat.

In the armed conflict between Ukraine and Russia (a definition adopted by the Geneva Academy of International Humanitarian Law and Human Rights), digital technology plays an essential, if not critical, role.

The armed conflict between Russia and Ukraine has drastically changed cybercrime. The data analysis shows that the limit between cybercrime and government-sponsored cyber activities is increasingly blurred. It is confirmed that cybercrime on both sides is initiated with close ties to the government in order to protect the national interests (Gabrian, 2022).

Unlike traditional warfare, where the Geneva Conventions and other agreements define the boundaries of permissible behavior, cyberspace remains a blurred zone. This uncertainty creates fertile ground for the states to use cybercriminal organizations as marionettes, allowing them to credibly deny their goals.

Since the beginning of the conflict in Ukraine, cyberattacks have focused on three main categories: broad-spectrum cyber disinformation; medium-spectrum cyber threats, mainly through overloading the target server or its surrounding infrastructure, causing it to fail (DDoS); and the use of cyberattacks to destroy specific targets.

During the first year of the conflict, the digital infrastructure of Ukraine was severely damaged in more than ten of the country's twenty-four regions, and restoring it to pre-conflict levels will cost 1.55 billion USD. This was partly accomplished through the destruction and breakdown of the equipment (Himmelfarb, 2023).

The conflict in Crimea and eastern Donbas in 2014 and the sophistication of the Russian cyberattacks forced Ukraine to strengthen the security of its IT systems with the assistance of the United States and Europe. Ukraine has developed a comprehensive cyber defense strategy for the period from 2014 to 2022 (Nehrey et al., 2022).

The Ukrainian IT Army was created in February 2022 by the order of the Deputy Prime Minister and Minister of Digital Transformation to counter the Russian cyberattacks. The declaration was a call for the volunteers whose actions on the cyber front were coordinated by a Telegram channel with approximately 300,000 subscribers (European Union Agency for Cybersecurity, 2022).

Several large technology corporations supporting Ukraine in cyberwarfare appeared for the first time during the current conflict (Kaminska et al., 2022). For example, Microsoft supported Ukrainian cybersecurity officials in combating malware, as well as providing awareness and intelligence on Russian cyber operations. China's approach to hybrid operations must also be taken into account. This refers to the increasing introduction of artificial intelligence in the dissemination of mass information, especially on social media. The People's Liberation Army of China is exploring the impact of more automated methods supported by algorithms through so-called cognitive domain operations (US Department of Defense, 2022). Some Chinese authors believe that this is the next evolution of warfare, moving away from focusing on the physical realms - land, sea, air - and moving into the electromagnetic field - attacking or maneuvering against the human mind (Yamaguchi et al., 2023). China is increasingly trying to manipulate social media to support its online disinformation campaign (Harold et al., 2021).

Thanks to artificial intelligence, it is becoming increasingly difficult to distinguish between real and fabricated informational videos and products. In late 2022, a Chinese channel published a video featuring computer-generated press secretaries created entirely with the help of artificial intelligence. Deep fakes will continue to develop and are expected to become a more convincing media product that will be increasingly difficult to detect and verify. The states such as the Russian Federation and China are already using these technologies, and as generative AI technologies advance, democracies will increasingly need to prevent and counter cognitive attacks that are algorithmically enhanced and adapted.

According to Russian press information, in December 2019, Russian President Vladimir Putin deployed no less than thirty hypersonic missiles in the Orenburg region. According to Moscow, this intent dates back to the 1980s. As Russia claims, its missile "Avangard" reaches such incredible speeds that it can defend itself against modern missile defense systems (Halbert, 2016).

The emergence of such hypersonic weapons forces potential adversaries to also take care of development of the similar technology, which, along with billions of dollars in costs, requires time and scientific potential. Such information (disinformation) is a tool for influencing the adversary. One of the main tools in hybrid threats is disinformation. When analyzing such information, experts take into account the complexity of the creation of the new technological weapons and note that (if this information turns out to be false), if the US reaction is not equal to the real threat that hypersonic systems pose, Washington risks wasting money and political capital, or worse, stepping up to the stage of escalation and making strategic mistakes. A similar kind of competition existed between the US and the USSR when the US launched a program to put nuclear weapons into interstellar orbit. This and similar disinformation encouraged the USSR to spend billions of dollars on the development of similar technologies, which ultimately turned out to be completely unproductive. The financial costs spent due to such disinformation eventually became one of the reasons for the economic crisis. The diversity of hybrid threats confirms that the states will increasingly have to enhance communication with their populations in ways that Clausewitz could never have imagined, and they may be paralyzed by such deliberate disinformation (Singer et al., 2018). The examples above demonstrate that hybrid challenges evolve and exhibit different characteristics.

The struggle for technological superiority is driven by the ability of the technology owner to capture new markets, defeat competitors with new, cheaper, and more reliable products, and generate billions of dollars in revenue. The struggle for technological superiority forces the states to counter the technological advances of a potential adversary, including through unconventional methods. The US-China competition is noteworthy in this regard, including on the technological front. Many Chinese high-tech companies, which in the recent past were low-cost technology vendors, are evolving into technology leaders and top competitors. Huawei is playing a leading role in the development of the equipment for 5G mobile networks and is a prime example of this evolution. However, as Chinese high-tech companies have become increasingly innovative rather than simply relying on imported technology, Western governments and companies have come to view them as a threat to national or corporate security. In 2012, the US banned the use of Huawei and ZTE network equipment in the US market; in 2020, this was expanded to include a broader "blacklist," restricting market access and banning exports. Although the conflict has centered on the technology companies, it has also spilled over into broader geopolitical tensions between China and the United States and their Western allies, called the "technological cold war." Business activity is increasingly influenced by the nationalist and geopolitical policies of the state (Yiu et al., 2021).

Although the "technological cold war" can be interpreted as a turning point in decades of increasing globalization, it is not a new phenomenon. It represents the latest explosion of so-called "Techno-nationalism", which began after World War II and manifested itself in the US's efforts to prevent Japan from absorbing and using American technological innovations.

Techno-nationalism in this traditional sense encompasses "the power of the state or the government with a mercantilist mindset that directly links technological innovation and capabilities to the country's national security, economic prosperity, and social stability" (Yadong, 2022).

While techno-nationalist policies typically aim to support domestic technological innovation and protect domestic industries from foreign competition, they are also typically pragmatic and serve national interests alongside openness. Recently, a "new techno-nationalism" has emerged in the context of the decline of the US as a global hegemon and the rise of new global powers with radically different economic and political models (Manning, 2019).

The task of coordination of innovative development is to promote structural reforms, select the most effective mechanisms for the concentration of the resources on priority innovative directions, create a system for monitoring the effectiveness of the use of innovative infrastructure facilities, create conditions for the development of competition, coordinate the activities of the development institutions, implement the foreign policy direction of innovations, and regulate the behavior of companies with state participation and natural monopolies, including through the innovative development program.

The fate of competition between the global powers may be determined by a country's ability to more quickly and effectively implement the innovations that are now the basis of a state's military, economic, and cultural superiority. The government must overcome its bureaucratic tendencies, create an environment conducive to innovation, and invest in the tools and skills needed for the activation of the cycle of technological progress. They must commit to innovation for the benefit of the nation and the democratic process.

The work focuses on the role of intellectual property in the context of the national security of the countries. The examples provided confirm that the development of the technologies is associated with the development of security systems by the countries and significant investments in the technologies. The inherent desire to gain technological advantage forces the states to be attentive to the results achieved by their competitors and to strengthen intellectual property management policies. The turbulent environment available in the world requires daily improvement of security systems. Readiness to ensure military, economic, technological, and other types of security.

CONCLUSION

This study highlights the critical relationship between intellectual property (IP) and state security, emphasizing how nations leverage IP to foster innovation, economic growth, and national defense capabilities. Through comparative analysis, key findings demonstrate the significant role of IP in addressing challenges posed by hybrid threats, geopolitical competition, and technological sovereignty. The results reveal that nations like the United States, China, Russia, and Georgia incorporate IP strategies into their national security policies. The United States prioritizes technological innovation and supply chain resilience, emphasizing critical areas like microelectronics and artificial intelligence. China focuses on state-driven technological advancements and integrating AI into defense, showcasing rapid growth in research and development. Russia underscores technological self-reliance and cybersecurity, reflecting its efforts to counter external influences. Georgia's approach highlights the importance of economic stability and resilience against cyber threats, particularly in the context of its geopolitical challenges. Challenges remain in harmonizing IP policies with the demands of national security. Hybrid threats, such as cyberattacks and disinformation campaigns, continue to blur the boundaries between traditional and unconventional security domains. The struggle for technological superiority among global powers underscores the urgency of developing adaptive IP frameworks that support innovation while mitigating security risks. To address these challenges, nations must prioritize investment in research and development, foster innovation ecosystems, and enhance public-private partnerships. Strengthening IP management policies and promoting international collaboration are crucial for creating a secure, innovation-driven environment. Additionally, balancing economic openness with strategic security objectives will be key to navigating the complexities of modern geopolitical competition. In conclusion, the integration of IP into national security frameworks is no longer optional but essential. As nations face an increasingly interconnected and competitive world, robust IP policies serve as a foundation for achieving technological leadership, economic stability, and strategic security objectives. This study underscores the need for continuous adaptation of IP strategies to address evolving global challenges effectively.

REFERENCES

Chitadze, N. (2019). Has the new Cold War started? Possible military confrontation between the USA and Russia, based on the examples of comparing the military potentials of the two powers and the withdrawal from the Intermediate-Range Nuclear Forces Treaty by both countries. *Journal in Humanities, 8*(1), 39. Retrieved from https://jh.ibsu.edu.ge/jms/index.php/SJH/article/view/388/405

Daphne, W. Y., William, P. W., Kelly, X. C., Xiaocong, T. (2022). Public sentiment is everything: Host-country public sentiment toward home country and acquisition ownership during

institutional transition. Journal of International Business Studies, Palgrave Macmillan; Academy of International Business, *53*(6), 1202-1227

European Union Agency for Cybersecurity (ENISA). (2022). ENISA Threat Landscape 2022. Retrieved from https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202022.pdf

Franke, U., & Torreblanca, J. I. (2021). Geo-tech politics: Why technology shapes European power. Retrieved from https://ecfr.eu/publication/geo-tech-politics-why-technology-shapes-european-power/

Gabrian, C. A. (2022). How the Russia-Ukraine war may change the cybercrime ecosystem. *Bulletin of "Carol I" National Defence University*, December, 43. Retrieved from https://revista.unap.ro/index.php/bulletin/article/view/1614/1562

Gakhokidze, J. (2007). *Main Problems of National Security.* Georgian Technical University.

Geneva Center for Security Sector Governance. (n.d.). National security policy. Retrieved from https://securitysectorintegrity.com/defence-management/policy/

Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society, 32*(4), 256-268.

Harold, S. W., Beauchamp-Mustafaga, N., & Hornung, J. W. (n.d.). Chinese disinformation efforts on social media. Retrieved from https://apps.dtic.mil/sti/trecms/pdf/AD1142311.pdf

Himmelfarb, A. (2023). Ukraine Rapid Damage and Needs Assessment February 2022 – February 2023. World Bank, United Nations. Retrieved from https://ukraine.un.org/sites/default/files/2023-3/P1801740d1177f03c0ab180057556615497.pdf

Kaminska, M., Shires, J., Smeets, M. (2022). Tallinn workshop report: Cyber operations during the 2022 Russian invasion of Ukraine: Lessons learned (so far). Retrieved from https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/560503/1/ECCRI_WorkshopReport_Version-Online.pdf

Kistauri, N., Melashvili, M., Kveladze, K. (n.d.). Economic security and factors affecting it. Retrieved from https://www.researchgate.net/publication/330637847

Luo Y. (2022). Illusions of techno-nationalism. *Journal of International Business Studies*, *53*(3), 550–567. https://doi.org/10.1057/s41267-021-00468-5

Manning, R. A. (2019). Techno-nationalism vs. the Fourth Industrial Revolution. *Global Asia*, *14*(1), 14–21.

Ministry of National Defense of the People's Republic of China. (n.d.). China's defensive national defense policy in the new era. Retrieved from http://eng.mod.gov.cn/xb/DefensePolicy/index.html

Ministry of Foreign Affairs of the Russian Federation. (2023). The concept of the foreign policy of the Russian Federation (Approved by Decree of the President of the Russian Federation No. 229, March 31, 2023). Retrieved from https://www.mid.ru/ru/detail-material-page/1860586/?lang=en

Ministry of Foreign Affairs of Georgia. (n.d.). National security concept of Georgia. https://mfa.gov.ge/national-security-concept

Nehrey, M., Voronenko, I., & M. Salem, A. B. M. (2022). Cybersecurity assessment: World and Ukrainian Experience. 335-340. https://doi.org/10.1109/ACIT54803.2022.9913081.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media.* Eamon Dolan Books.

The White House. (2022). National security strategy. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

US Department of Defense. (2022). Military and security developments involving the People's Republic of China. Washington, DC. Retrieved from https://navyleaguehonolulu.org/maritime-security/ewExternalFiles/2022-military-and-security-developments-involving-the-peoples-republic-of-china.pdf

Yamaguchi, S., Yatsuzuka, M., & Momma, R. (2023). China security report 2023: China's quest for control of the cognitive domain and gray zone situations. National Institute for Defense Studies. Retrieved from https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01.pdf