Mirosław Banasik

Jan Kochanowski University (Poland) ORCID: 0000-0002-9358-1240 e-mail: miroslaw.banasik@interia.pl

Lech Chojnowski

Pomeranian University in Słupsk (Poland) ORCID: 0000-0003-0339-0430 e-mail: lech.chojnowski@apsl.edu.pl

Challenges and Threats as a Consequence of Strategic Competition

Abstract: The purpose of the research, the results of which are presented in this article, was to clarify the mechanisms of strategic competition and to identify the challenges and threats arising from it for international security. A systemic approach, literature analysis and criticism, non-participatory observation, and a case study were used to solve the research problems. In the research process, it was established that strategic competition is constantly intensifying, and its consequences can harm global security. The process of strategic competition should be viewed as challenges that, if not addressed, can quickly develop into new threats. The most significant threats to international security are related to the ambitions of revisionist states seeking territorial claims and expanding spheres of influence. Although the risk of global war remains relatively low, states will seek to permanently influence their competitors in the gray zone through soft instruments. Soft influence instruments will dominate it. The effectiveness of these tools will be determined by the world's interconnectedness in the economic and political spheres. States will try to achieve their strategic goals in cyberspace and narrative using traditional mass media and social media.

Keywords: Strategic competition, international security, gray zone, cybersecurity, challenges and threats

Introduction

Dynamic changes in the international security environment prove that the world is entering a new era in international relations. Today, the greatest threats to international security are posed by superpowers that are permanently engaged in strategic competition with each other

for world domination and primacy, as well as states with revisionist aspirations. Over the past few years, the intensity of the Russian Federation's strategic competition with the United States and the democratic Western world and its values has increased. It is likely to be longlasting and will significantly affect the architecture of international security, as the United Nations, for example, did not perform well in the early days of the conflict either in the face of genocide, humanitarian disaster, or the blockade and deliberate arson of Ukrainian grain. It is worth noting that any conflict with a nuclear power like Russia involves nuclear escalation. By threatening to use nuclear weapons, the Kremlin wants not only to discourage Western governments from providing more meaningful support to Ukraine but also to intimidate Western public opinion. Russia's successful strategic deterrence creates favorable conditions for continuing conventional warfare, which could have disastrous consequences for European and global security (Horovitz & Wachs, 2022, p. 1). Second, V. Putin's statements suggest that the functions of the nuclear arsenal go beyond the narrow defensive role defined in the Russian Federation's official doctrinal documents. It can be assumed that the Kremlin is using nuclear weapons (Hastings, 2022) as a tool to achieve expansive political goals. Indeed, V. Putin is shielding a conventional onslaught against Ukraine under the nuclear umbrella. At the same time, he effectively discourages NATO from interfering in a war he considers local. Thus, by using nuclear weapons, the Russian Federation achieves its goals of strategic intimidation and manages the escalation of the conflict (Horovitz & Wachs, 2022, p. 2). The United States, on the other hand, is primarily focused on providing security through strategic deterrence and preventing military conflict in the South China Sea, the Taiwan Strait, the Baltic States, and Poland. This deterrence also has a conventional dimension. According to doctrinal documents, the US military is preparing for large-scale warfare in the land, air, sea, space, and cyberspace dimensions (Headquarters, 2021, p. 9). However, it should be made clear that the consequences of such a war with the Russian Federation or China could be unimaginable. As a result, the competition seeks to achieve strategic successes in a gray area, hoping to achieve its strategic goals without engaging in serious hostilities. In this way, they want to maintain the appearance of legitimacy of their actions in the eyes of the international community and not be held accountable for them. Moreover, they are aware of the military capabilities of the United States of America and probably want to lower the risk of escalation of the conflict to the level of nuclear war. In the gray zone, a state can implement all or selectively available instruments simultaneously and use any mechanism related to the use of national power to advance its interests. The attraction of conducting competitions in the gray zone lies in allowing a weaker state to achieve foreign policy goals, such as regime change or territory acquisition, without resorting to full-scale conventional military campaigns. Therefore, weaker states often use the gray zone to challenge stronger states with significant military advantages (McCarthy et al., 2019, p. 5). At the same time, the selectivity of the influence used makes war between states possible in chosen operational domains.

Based on a literature search, it was found that the available literature on strategic competition focuses mainly on relations between states in terms of hegemony or subordination. Security studies do not focus on operationalizing mechanisms for conducting strategic rivalries, i.e., the instruments of influence used and their consequences for international security. This creates a significant cognitive gap in this area. It particularly relates to the conduct of rivalries in cyberspace, which provides the possibility of conducting rivalries in the gray zone. It follows that the issue of international security considered through the prism of strategic competition is still insufficiently explored and described, especially in terms of the challenges and threats it brings.

Based on the existing cognitive gap, the main research problem was formulated: *What challenges and threats to international security does strategic competition pose?* The main research problem was fragmented, and the following problems were identified: 1) What are the characteristic features of strategic competition, and what might be its implications for international security? 2) How is strategic competition conducted in cyberspace, and what does it bring to international security?

The purpose of the research, the results of which are presented in this article, was to clarify the mechanisms of the ongoing strategic competition and identify the challenges and threats it poses to international security. A research hypothesis was formulated to guide the research process, expressed in the supposition that there is currently a permanent strategic competition between global actors. Challenges and threats to international security are posed by powers that seek world domination and primacy and states with revisionist aspirations. Strategic competition seeks to succeed in the gray zone using all available instruments and domains of influence, hoping to achieve their goals without needing military action.

The research process assumes that strategic rivalry is carried out with the help of instruments at the disposal of the pasture, which form a strictly ordered system of influence on the opposing party. Therefore, a systemic approach was used to study the interactions, interdependencies, and relationships between the mechanisms of strategic interaction and the participants in the international security environment and to identify the consequences of this interaction. Based on this, challenges and threats to international security were studied. In solving research problems and obtaining objective qualitative data, literature analysis and criticism, non-participant observation, and case studies were mainly used. Comparative analysis and generalization were also helpful in determining the trends and mechanisms used to achieve the goals of strategic competition and their implications for international security. The conclusions presented in the article result from applying inductive and deductive reasoning.

The characteristics of strategic competition and its implications for international security

Changes in the international security environment caused by the rapid processes of strategic competition generate new challenges and threats. For example, China, a global change generator, shows great assertiveness towards other states. China is a strategic competitor that challenges the world with its rapidly developing economy and modern technologies. To achieve its strategic goals, it skillfully uses all available instruments of influence, mainly diplomacy and military force (Biden, 2021, pp. 7–8).

The Russian Federation is focused on the imperialism of a bygone era and the disruption of the Western world. It claims control over the historic lands of Russian and Slavic nations in its so-called near abroad, referred to as the Duginist Eurasian construct (Zwack & Pierre, 2018, p. 6). At the same time, it seeks to negate U.S. principles, norms, and international law and claims dominance over its neighbors. Moreover, it seeks to create a multilateral world, asserting regional power and authority and economic and military advantages (Bryc, 2023). The state's leader, Vladimir Putin, wants the Russian Federation to be treated as a global power with the right to veto and decide on the most critical problems of the modern world (Bugajski & Assenova, 2016, p. 6). The Kremlin seeks to deter international institutions hostile to the Russian Federation, such as NATO and the European Union, and weaken their cohesion (Rumer, 2019, p. 4). Since the war with Ukraine began, it has pushed hard to strengthen relations with China, the China-led Shanghai Cooperation Organization, and the BRICS international group (Kugiel, 2022), which in the opinion, Moscow can counterbalance the West relatively quickly. The Kremlin's regional priorities focus on consolidating influence in the post-Soviet states, the Middle East, and the Arctic (Charap et al., 2021, p. 131). The competition for global influence between the United States and the Russian Federation seems somewhat exaggerated and fueled mainly by the Russian establishment. The Russian Federation has global military capabilities, especially in the areas of nuclear weapons, space capabilities, and precision-guided weapons, including hypersonic weapons (Banasik, 2021). However, the negative experience in Ukraine and the fiasco of the crewless moon landing (Bojanovich, 2023) contradict the claim of dominance in these areas. Most of the capabilities are disruptive, as exemplified by the non-kinetic influence in cyberspace. In the narrative sphere, Russia effectively undermines the Western political message through disinformation and propaganda (Moore, 2019, p. 5). The Russian Federation does not have a viable vision of the global world order or the potential necessary to create it, and divergent interests have no chance of any strategic alliance with the US (Rumer & Sokolsky, 2019, p. 4).

As with the Russian Federation, the United States has conflicting interests with China in the Indo-Pacific region. The importance of these interests to both states has made the region a significant site of competition between these powers. The U.S. vision of a free and open Indo-Pacific is incompatible with Chinese aspirations for greater control in the bodies of water bounded by the so-called First Island Chain, delineated by the Japanese Islands, Taiwan, and the western shore of Borneo, and broader Chinese regional goals (Defense, 2021, p. 33). Conflicts are escalating so rapidly that without smoothly functioning diplomacy, they can quickly escalate into confrontation or direct military clash (Engstrom, 2018). China has economic regional dominance and a steadily diminishing military advantage over the US. A military confrontation near China's shores would be particularly beneficial to China, but it seems too early for that. This is supported by the fact that the United States has an overall advantage in military technology and power projection capabilities throughout the Indo-Pacific region. In addition, they are the beneficiaries of regional political and military alliances, allowing them to dominate China (Lynch, 2020, p. 313). Nevertheless, China, by conducting large-scale military exercises, is demonstrating its readiness to invade and forcibly subjugate Taiwan (Rowles, 2022).

China has an ambitious global development strategy uses infrastructure investment to expand the country's political, economic, and military power (Schuman et al., 2013). China is using economic aid to pressure foreign governments to adopt favorable policies on issues such as Taiwan, Hong Kong, and Chinese control of islands in the South China Sea. Jinping Xi aims to create a vast network of railroads, highways, energy pipelines, maritime trade routes, and ports connecting China to the rest of Asia, Europe, the Middle East, and Africa. The sea routes connect Chinese seaports with states in the South China Sea, Indian Ocean, South Pacific, and Mediterranean (Jones, 2021, p. 3).

The United States dominates in the military sphere, although not as much as it did ten or twenty years ago. However, the U.S.'s global military advantage could be nullified if China or the Russian Federation can pick favorable physical and political ground for a short and decisive military conflict. Neither Russia nor China has sufficient national strength to prevail in a prolonged military clash with the United States today or in the foreseeable future (Brands & Beckley, 2021). U.S. global military dominance is a serious argument in the coming era of great power competition. However, improved capabilities for using non-military instruments of international influence are necessary for effective competition (Repnikova, 2022). China can already severely constrain U.S. (or Russian) military activity in East Asia, the Western Pacific (Sullivan & Brands, 2020), and especially in cyberspace (Demchak, 2019) and increasingly in space (Broad, 2021). The United States should revise its strategy in these regions and consider its ideological advantage, soft power use, and the Chinese economy's competitive limitations (Lynch, 2020, p. 99).

The Russian Federation currently has a clear military, economic, and information advantage in the areas of the so-called "near abroad" and limited but not inconsiderable capabilities to project power and maintain influence in the Middle East (Banasik, 2021) in the Arctic and the ability to conduct operations in cyberspace (Pijović, 2021). However, Russia's economic, ideological, and political conditions and the possible loss of its war with Ukraine could cause it to lose this influence.

It should not be assumed a priori that all powers want to engage in military disputes. However, some incredibly aggressive ones with hard instruments of international influence are inclined to subjugate their neighbors through military force. Such states, called revisionist states, threaten global security stability. Revisionist states are usually understood as those that seek, as the classical realists put it, to demand a change in the status quo (Dobriansky, 2020). They are not driven by the need to provide international security but by ideology and domination, which means they seek more power (Brands, 2020). In this sense, the Russian Federation is determined to be recognized as one of the leading powers in the multipolar world in order to gain a higher degree of control over its periphery and regain its authority as the undisputed hegemon there (Mcclintock et al., 2021, p. 2). It is likely that these assumptions, along with the goal of regime survival, were the reasons for the February 2022 invasion of Ukraine. It appears that the Russian Federation, despite widespread offensive aggression, seeks to defend the space of Russian interests and dismantle and undermine American hegemony (Mazarr, 2022, p. 30). This approach to competition creates global and regional instabilities. However, offering concessions to a revisionist state may lead it to believe its influence puts it in a better position to realize further aggressive ambitions. The war in Ukraine also confirms that the most significant risk of conflict in the international system comes from a failure of strategic deterrence, not from a misperception of threats (Ashford, 2021, p. 6).

Nowhere in Russian strategic documents is there a formal record of imperialist ambitions or doctrinal directives to use military force to achieve domination over neighbors (Charap et al., 2021, p. 29). Even so, it does not appear that the Russian Federation, apart from precisely its neighbors, has vital interests and resources to control large areas of foreign territory. The North Atlantic Alliance and the provisions of Article 5 effectively hinder this. However, it should be remembered that the high nuclear potential of the Russian Federation makes it a very aggressive and provocative revisionist. After the invasion of Ukraine, it should be believed that the Russian Federation is ready to use force on a larger scale than previously assumed, which means real threats to the states that appeared on the political map of the world after the collapse of the Soviet Union. This does not mean a confrontation with the United States can be completely ruled out. The support given to Ukraine significantly increases the risk of a collision course militarily with the US and NATO (Mazarr, 2022, p. 13). It should be clearly stated that the current nature of the Russian Federation's competition with the West and its revisionist inclinations creates the danger of the current war expanding to other states.

Competition in cyberspace

Hostilities can also be conducted below the threshold of war. The Russian Federation, China, as well as Iran practice gray zone warfare, in the literature referred to as hybrid, new generation, unconventional or political warfare, and sometimes as unprincipled war. The intensity of this form of competition will increase significantly soon (Connable et al., 2018, pp. 17–27). In the gray zone, influence is carried out in all possible domains using available instruments

and tools, as well as forms, methods, and ways of exerting influence (Morris et al., 2019). Adequate to the intended goals, capabilities are selectively chosen and applied following a pre-developed strategy. Due to the rapid development of new technologies and the ability to exert cognitive effects, Russian and Chinese disinformation and propaganda have become a permanent part of the international information space. They use proxy actors to stoke social tensions beyond national borders. They combine cyberattacks with psychological operations and opportunities provided by social media platforms and hitherto unknown forms of information broadcasting (Chekinov & Bogdanov, 2015, pp. 44-45). A glaring example of this type of activity was reported in January 2017 to discredit anti-Kremlin US presidential candidate Hillary Clinton. The U.S. intelligence community noted that the Russian goal in the U.S. presidential election was to undermine public faith in the democratic process, which it sought to achieve through a strategy that combined covert intelligence operations conducted in cyberspace with overt actions by Russian government agencies (U.S. Office, 2017). Russia and China view the information sphere as part of a holistic space in which competition is conducted and, therefore, use all available media to manipulate hostile societies and achieve communicative strategic advantage (Mazarr et al., 2019, p. 225). Gray zone operations can also precede, create conditions for, and support conventional military actions (Radin, 2017, p. 31). For example, using paramilitary forces and unmarked units is possible against a weaker adversary, but repeating the scenario from the annexation of Crimea would require more finesse and carry a greater risk of escalating the conflict.

From the arguments presented, it is clear that the aspirations of great powers such as China and Russia for confrontational supremacy and dominance go far beyond the arena of conventional war. Operations conducted in cyberspace are perhaps the most prominent tool for the modern conquest of other states. Cyberspace is a domain where states, using high-risk strategies, destabilize the international security environment (Nye, 2017, p. 15). Cyberspace has evolved into what military strategists consider a new space for conducting combat. The emerging sphere of strategic competition could become the starting point for the next global arms race. Although strategic thinking on cyber warfare is still in its early stages, various states have established command structures and set up separate military units with the technical competence to conduct offensive operations in cyberspace. Over the past decade, states have increasingly used cyberspace to conduct espionage, sabotage, and subversion activities (Domingo, 2016, p. 1). Theft of industrial secrets has also been carried out, and elections and democratic processes in Western states have been influenced. Major powers are also looking for ways to conduct destructive forms of large-scale conflict directly threatening economic and political security through virtual means (Schneider, 2020, pp. 160–164).

The new domain of warfare, cyberspace (Dziwisz & Sajduk, 2023), has motivated the United States, Russia, and China to develop their offensive and defensive capabilities. China, seeking to offset the United States' military superiority, is developing cyber warfare capabilities. They are taking advantage of the Internet's dependence on the functioning of

U.S. critical infrastructure, relatively weak cyber defenses, and especially the vulnerabilities of U.S. military systems using cyberspace (Sánchez & Akyesilmen, 2021, p. 53). China conducts extensive cyber espionage campaigns against the U.S. government and the private sector (Goodman, 2010, p. 103). The activities of China's specialized cyber units also target political and military intelligence. In the long term, this campaign aims to manipulate information and then use it to gain political, military, or economic advantage (Sánchez & Akyesilmen, 2021, p. 55). The current U.S. Cyberspace Defense Strategy aims to prevent U.S. interests from being harmed by preventing the possibility of aggressive Russian and Chinese cyber operations that could lead to strategic advantage (Sharpening, 2018, p. 1). The Russian Federation conducts intelligence operations with the help of its own military hackers and proxy actors. Russian cyberspace operations are increasingly aggressive and are designed to lay the groundwork for future significant disruptions of the attacked state's critical infrastructure, including, but not limited to, the energy sector, water supply, civil aviation operations, commercial and industrial facilities, and prevent the use of military capabilities. For example, the Russian consulate in San Francisco, which was closed by the US in 2017, was considered an intelligence hub for physically mapping fiber-optic networks and many other activities considered extremely aggressive and highly innovative means of intelligence gathering (Dorfman, 2017).

The Russian Federation is increasingly and effectively conducting cyber operations against European states. However, the leaders of these states are reluctant to admit this publicly. Perhaps because it is difficult to find evidence of these operations, or the states do not want to disclose the negative consequences of such actions. Russian cyber operations were particularly intense before and after the start of the war with Ukraine. One might even be tempted to theorize that because it supports Ukraine, the West is at war in cyberspace with the Russian Federation (Deni, 2018). Most European states are against conducting offensive operations in response to Russian attacks. The exceptions are Poland and the United Kingdom, which are inclined to do such operations. Perhaps because of the damage the Russian Federation will cause to other states in cyberspace, 2023 may prove to be a turning point and lead to a change in their decisions regarding offensive operations against the aggressor.

There are growing claims that strategic deterrence should be conducted in cyberspace along the lines of conventional deterrence anchored in the strategic space of armed conflict. Operational practice confirms that deterrence in cyberspace does not work and that significant powers strike and take unlawful blows. Understanding the interaction dynamics triggered by this active competition strategy is crucial, especially given the concerns of some policymakers that a proactive U.S. posture in cyberspace could lead to an uncontrolled escalation of conflicts. Statements by some U.S. experts suggest that cyberspace may be home to the most spiraling and uncontrollable types of conflicts we have ever faced (Committee, 2017, p. 7). It is also worth considering how strategic competition will seek opportunities for strategic advantage in this space and how to effectively deter them from such intentions, especially when there is no armed conflict in the real world. Behavior in cyberspace unrelated to armed conflict is not necessarily focused on the search for military advantage but may involve selected domains of strategic competition (Fischerkeller & Harknett, 2019). Due to the interconnectedness that is a fundamental structural feature of cyberspace, strategic objectives can be achieved in and through cyberspace through cyber operations or campaigns, which need not be related to armed conflict at all. The essential condition implied by interconnectedness is constant contact with a rival, which, combined with the nature of information technology and networked computer systems, imposes a structural security imperative, assuming that adversaries can constantly engage in conducting such operations. Thus, the prospect of achieving the strategic advantage of acquiring new sources of national power through the occurrence of cumulative effects made possible by well-organized campaigns conducted in cyberspace emerges (Fischerkeller & Harknett, 2019).

Outer space is the primary operational medium for conducting critical military operations in cyberspace. For this reason, significant powers are eagerly engaging in space competition. The lack of established rules and norms for the joint use of space means that competition in space is constantly intensifying, raising the risk of serious conflict. As in cyberspace, we may soon witness more dynamic competition in space. It is expected that more malicious and confrontational actions will take place in this medium of interaction between powers (Lynch, 2020, p. 65). State and non-state actors can also use cyberspace to attack civilian and military satellites and ground facilities (Rajagopalan, 2019, p. 1). Cyber operations against competing states are conducted using space. Resources placed in space collect and process intelligence information. This means that space is now militarized and rearmed with cyber means. Military activities and capabilities using space are used to conduct strategic competition and are aimed at achieving specific strategic objectives. They are used to conduct strategic deterrence, achieve dominance over the adversary, conduct armed combat, or maintain security stability. However, it should be made clear that military operations are not conducted in isolation from political or economic influence (Austin et al., 2022, p. 6).

Conclusions

Research has established that strategic competition is steadily increasing, and its consequences can harm global security. The process of strategic competition should be regarded as a challenge that, if not addressed, can quickly turn into new types of threats. Based on research, it has been determined that in the next decade, the strategic competition between the United States and China will be the most intense. The biggest threats to the existing international order will be the ambitions of revisionist states related to territorial claims and the expansion of spheres of influence. These states will use mainly non-military instruments of influence to gain an advantage over competing societies. The leader in this regard is China, which has a strong economy, ambitious global plans, and aggressive regional intentions. The weak economy of the Russian Federation is unlikely to change the global security system without aggressive use of military force, so future security will be closely dependent on the forms and extent of the competition between China and the United States. It may be a direct clash for regional influence, a struggle for economic and ideological superiority, or another, more benign form of pursuing one's political goals. The most dangerous thing for the world may soon be forming a coalition of China and the Russian Federation against the West. The most dangerous thing for the world shortly may be the formation of a coalition of China and the Russian Federation against the West.

Although the risk of global war remains relatively low, states will continue to try to influence their strategic competitors in various ways. At present, wars are fought in a gray zone, with the arsenal dominated by tools of soft influence, mainly unconventional and irregular. The effectiveness of these tools is determined by the world's interconnectedness in the economic and political spheres.

States will seek to achieve their strategic goals primarily through civilian influence capabilities with varying intensity in diverse domains. Competition will occur mainly in cyberspace and the narrative sphere using traditional mass media and social media. The prospects for direct military combat between the great powers in space remain rather unlikely. However, it cannot be ruled out in cyberspace, where there will likely be numerous tensions and escalation of conflicts. Nor can severe disputes over the military and civilian use of the common good that is space be ruled out.

References:

Ashford, E. (2021). Revisionist States are the Cause of Great-Power Competition. Atlantic Council.

- Austin, G., Rajagopalan, R.P., & Wright, T. (2022). Military Ambitions and Competition in Space: The Role of Alliances. The International Institute for Strategic Studies.
- Bryc, A. (2023). Russia's Challenge to Central and Eastern Europe. In R. Zięba (Ed.), Politics and Security of Central and Eastern Europe (pp.159–175).
- U.S. Office of the Director of National Intelligence. (2017). Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.
- Banasik, M. (2021). Rywalizacja, presja i agresja Federacji Rosyjskiej. Konsekwencje dla bezpieczeństwa międzynarodowego. Warszawa.
- Biden, J. (2021). Renewing America's Advantages. Interim National Security Strategic Guidance. Washington.
- Biden, J. (2022). National Security Strategy. Washington.
- Bojanowicz, R. (2023). Fiasko rosyjskiej misji księżycowej. Sonda Łuna-25 rozbiła się w trakcie lądowania. Forsal.pl.
- Brands, H. (2020). Do not let Great Powers Carve Up the World. Foreign Affairs.
- Brands, H., & Beckley, M. (2021). China is a Declining Power and That is the Problem. Foreign Policy.

- Broad, J. (2021). How Space Became the Next 'Great Power' Contest Between the U.S. and China. *The New York Times*.
- Bugajski, J., & Assenova, M. (2016). Eurasian Disunion. Russia's Vulnerable Flanks. Washington.
- Charap, S., Massicot, D., Priebe, M., Demus, A., Reach, C., Stalczynski, M., Han, E., & Davis, L. E. (2021). *Russian Grand Strategy*. Santa Monica.
- Committee on Armed Services House of Representatives. (2017). *Cyber Warfare in The 21st Century: Threats, Challenges, and Opportunities.* Washington.
- Connable, B., Campbell, J. H., & Madden, D. (2018). Stretching and Exploiting Thresholds for High-Order War. How Russia, China, and Iran are Eroding American Influence Using Time-Tested Measures Short of War. Santa Monica.

Czekinow, S. G., & Bogdanow, S. A. (2015). Prognozirowanije charaktiera i sodierżanija wojn buduszczego: problemy i sużdienija. *Voyennaya Mysl, 10.*

- Demchak, C. C. (2019). China: Determined to Dominate Cyberspace and AI. Bulletin of the Atomic Scientists, 75(3).
- Deni, J. R. (2018). The West's Confusion over Russia's Cyberwars. Carnegie Europe.
- Dobriansky, P. (2020). Ask the Experts: Should US Foreign Policy Focus on Great-Power Competition? *Foreign Affairs.*
- Domingo, F. C. (2016). Conquering a new domain: Explaining excellent power competition in cyberspace. *Comparative Strategy*, 35(2).
- Dorfman, Z. (2017). The Secret History of the Russian Consulate in San Francisco. Foreign Policy.
- Dziwisz, D., & Sajduk, B. (2023). Rosyjska inwazja na Ukrainę a przyszłość cyberwojny –wnioski w rocznicę "specjalnej operacji wojskowej". In A. Gruszczak (Ed.), The War Must Go On: Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski.
- Engstrom, J. (2018). Systems Confrontation and System Destruction Warfare. How the Chinese People's Liberation Army Seeks to Wage Modern Warfare. Santa Monica.
- Fischerkeller, M. P., & Harknett, R. J. (2019). What Is Agreed Competition in Cyberspace? Lawfare.
- Goodman, W. (2010). Cyber Deterrence. Tougher in Theory than in Practice? *Strategic Studies Quarterly*, Fall.
- Hastings, M. (2022). With Nuclear Threat, Putin Makes the Unthinkable a Possibility. *The Washington Post*.
- Headquarters, Department of the Army. (2021). Army Multi-Domain Transformation Ready to Win in Competition and Conflict. Washington.
- Horovitz, L., & Wachs, L. (2022). Russia's Nuclear Threats in the War Against Ukraine. Consequences for the International Order, NATO and Germany. SWP Comment, 29, 1–7. DOI:10.18449/2022C29.
- Jones, S. G. (2021). Hiding and Finding the Challenge of Security Competition. CSIS Brief.
- Kugiel, P. (2022). Znaczenie grupy BRICS po rosyjskiej inwazji na Ukrainę. Polski Instytut Spraw Międzynarodowych.
- Lynch III, T. F. (2020). Strategic Assessment 2020 Into a New Era of Great Power Competition. Washington.
- Mazarr, M. J. (2022). Understanding Competition. Great Power Rivalry in a Changing International Order – Concepts and Theories. Santa Monica.
- Mazarr, M. J., Casey, A., Demus, S.W., Luke, H., Matthews, J., Beauchamp-Mustafaga, N., & Sladden, J. (2019). Hostile Social Manipulation. Present Realities and Emerging Trends. Santa Monica.
- McCarthy, M.C., Moyer, M.A., & Venable, B. H. (2019). Deterring Russia in The Gray Zone. Carlisle.

- Mcclintock, B., Hornung, J. W., & Costello K. (2021). Russia's Global Interests and Actions. Growing Reach to Match Rejuvenated Capabilities. Santa Monica.
- Military and Security Developments Involving the People's Republic of China. (2021). A Report to Congress U.S.
- Moore, C. (2019). Russia and Disinformation: Maskirovka. The Centre for Research and Evidence on Security Threats.
- Morris, L. J., Mazarr, M. J., Hornung, J. W., Pezard, S., Binnendijk, A., & Kepe, M. (2019). Gaining Competitive Advantage in the Gray Zone. Response Options for Coercive Aggression Below the Threshold of Major War. Santa Monica.
- Nye, J. S. (2017). Normative Restraints on Cyber Conflict. Belfer Center for Science and International Affairs.
- Pijović, N. (2021). The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms. Tallinn.
- Pollpeter, K. (2022). Testimony before the U.S.-China Economic and Security Review Commission Hearing on 'China in Space: Strategic Competition.' CAN.
- Radin, A. (2017). Hybrid Warfare in the Baltics. Threats and Potential Responses. Santa Monica.
- Rajagopalan, R. P. (2019). Electronic and Cyber Warfare in Outer Space. The United Nations Institute for Disarmament Research.
- Repnikova, M. (2022). The Balance of Soft Power. Foreign Affairs.
- Rowles, J. (2022). New Chinese White Paper Points to Military Conquest of Taiwan. Trenchant Observations.
- Rumer, E. (2019). The Primakov (Not Gerasimov) Doctrine in Action. Washington.
- Rumer, E., & Sokolsky, R. (2019). Thirty Years of U.S. Policy Toward Russia: Can the Vicious Circle Be Broken? Washington.
- Russia Military Power. Building a Military to Support Great Power Aspirations. (2017). Defense Intelligence Agency.
- Sánchez, Val K.V., & Akyesilmen, N. (2021). Competition for High Politics in Cyberspace: Technological Conflicts Between China and the USA. *Polish Political Science Yearbook*, 50(1).
- Schneider, J. (2020). A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem. Washington Quarterly, 43(2).
- Schuman, M., Fulton, J., & Gering T. (2023). How Beijing's Newest Global Initiatives Seek to Remake the World Order. Atlantic Council.
- Science of Military Strategy (2013). China Aerospace Studies Institute.
- Sharpening our Competitive Edge in Cyberspace (2018). *DoD Cyber Strategy and Cyber Posture Review*. Sullivan, J., & Brands, H. (2020). *China Has Two Paths to Global Domination*. Washington.
- The State Council Information Office of the People's Republic of China. (2015). *China's Military Strategy*. Beijing.
- Zwack P. B., & Pierre, M. C. (2018). Russian Challenges from Now into the Next Generation: A Geostrategic Primer. Washington.