

The Formation and Evolution of the Concept of Strategic Competition

Tamta Kodua

PhD Candidate, Caucasus International University, Georgia

Abstract

This paper examines the concept of strategic competition, its essence, and the principal stages of its development. The study aims to demonstrate the significance and distinctive characteristics of strategic patience as an instrument for pursuing long-term policy objectives. It analyzes the prerequisites for the emergence of the concept, its evolution and the principal areas of its practical application. Particular attention is devoted to the role of strategic patience in international relations and security policy. The study demonstrates that strategic competition should not be understood as inaction or passivity, but rather as a deliberate, consistent and adaptive approach to action aimed at achieving long-term objectives.

Keywords: formation, evolution, concept of strategic competition.

Introduction

Strategic competition represents one of the most complex forms of competition for power within the international relations system. Its scope extends beyond merely increasing the quantitative volume of military armaments or comparing the defensive capabilities of States. Strategic competition constitutes a broader process through which States seek to develop military, economic, political, technological and informational capabilities that enable them to secure long-term advantages over their competitors or preserve existing advantages. In this context, the defining characteristic of strategic competition is not simply the existence of rivalry, but rather the interdependence of States' actions and strategic decision-making.

An increase in one State's capabilities affects another State's perception of threats, allocation of resources and subsequent strategic decision-making. This interdependence is particularly evident in the contemporary cyberspace, where States' strategic behavior is often shaped by conditions of incomplete information and uncertainty regarding the adversary's actual capabilities. Gomez and White argue that a key challenge in assessing the strategic significance of cyber operations lies precisely in the information deficit and that an assessment based solely on material capabilities is insufficient to explain State behavior.²

A key starting point for understanding the historical foundations of strategic competition is the military-technological rivalry of the industrial era. From the second half of the XIX century onward, the expansion of

¹ Received: 22/01/2026 ; Accepted : 25/07/2026 ; Published : 26/09/2026

© 2026 The Author. Published by AVADA-CROMA. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, adaptation, and reproduction in any medium, provided that the original author and source are properly credited.
<https://creativecommons.org/licenses/by/4.0/>

² Gomez, M. A., Whyte, C. „Unpacking Strategic Behavior in Cyberspace: A Schema Driven Approach.“ *Journal of Cybersecurity*, 2022. 1-15.

industrial production, the development of railway networks, the advancement of telegraph communications, the growth of steel production and the expansion of the military-industrial sector transformed the material foundations of States' military power. Particularly significant was the naval competition between the German Empire and the United Kingdom in the late XIX and early XX centuries. Under the leadership of Admiral Alfred von Tirpitz, Germany initiated a large-scale naval buildup based on the Naval Laws adopted in 1898 and 1900, prompting Britain to respond with policies aimed at preserving its naval superiority. The construction of the British battleship *HMS Dreadnought* in 1906 marked the emergence of a new stage in military-technological competition. This case clearly illustrates a fundamental mechanism of strategic competition: technological innovation affects not only the capabilities of the State that possesses it, but also compels competitors to reassess their perceptions of the balance of power.

However, the most important historical experience for understanding contemporary strategic competition in theoretical terms is the Cold War. Following 1945, the bipolar international system that emerged between the United States and the Soviet Union became the principal axis of strategic competition. On July 16, 1945, the United States conducted the first nuclear detonation in history as part of the *Trinity* test, while on August 29, 1949, the Soviet Union tested its first atomic device. In 1952, the United States tested a thermonuclear device and the Soviet Union soon responded with corresponding technological developments. This process demonstrated that the primary objective of strategic competition is not necessarily direct military confrontation with an adversary. An important function of such competition may instead be the development of capabilities designed to deter the adversary from initiating an attack.

Literature Review

Cybersecurity research increasingly treats cyberspace as a domain of political competition whose effects depend on strategic interpretation, institutional context and the organisation of digital infrastructure. Gomez and Whyte (2022) challenge explanations based solely on technical capabilities or incomplete information. Drawing on cross-national wargames, they show how decision-makers use strategic-cultural schemas to interpret ambiguous cyber incidents and select responses. This suggests that identical technical events can produce different policy choices when officials understand the threat through different prior experiences and assumptions. academic.oup.com

The place of cyber operations within conventional strategic studies remains contested. Žilínčik and Duyvesteyn (2023) examine how the field has conceptualised cyber warfare and caution against treating it as a self-contained form of conflict. Beckerman (2022) likewise questions whether the traditional security-dilemma model adequately explains cyber interactions. Together, these studies indicate that claims about escalation or a distinct logic of “cyber war” need to be tested against the political objectives and circumstances of particular operations. [Get Access](#)

Other scholars shift attention from war to persistent competition below its threshold. Liebetrau (2022) identifies a European strategic gap in addressing cyber conflict short of war, especially where military, intelligence and allied activities intersect. Maschmeyer (2023) conceptualises cyber operations as instruments of subversion that can affect political relationships without resembling conventional military attacks. Fedoniuk and Maghdysiuik (2022) examine this broader competition through the United States–China relationship, showing how cybersecurity is bound up with national strategy, rivalry and competing accounts of cyber influence. doi.org

Geographical and sociotechnical approaches further complicate state-centred accounts of cyber power. Ashraf (2023) argues that cyber conflict operates across several overlapping spatial arrangements and cannot be understood through territorial boundaries alone. Dwyer (2023) examines the role of computational systems themselves, proposing that their operations shape how cyber harms unfold. Czerwińska (2025) connects cybersecurity to international power dynamics, critical infrastructure and cooperation between states. Read together, these works suggest that cyber power emerges through interactions among political actors, technical systems and infrastructures that cross jurisdictions. [Springer Nature Link](#)

A useful direction for further research is to connect these levels of analysis. Strategic-culture studies explain how officials interpret incidents; research on subversion explains what states seek to accomplish; and geographical and computational approaches show where and through which systems those objectives take effect. An integrated framework could therefore examine how interpretations of a cyber incident shape a state's response, while the structure of digital infrastructure limits or amplifies the operation's political effects. This is a synthesis of the reviewed literature rather than a conclusion established by any single study.

The nuclear age placed the concepts of deterrence, second-strike capability and strategic stability at the center of strategic studies. The logic of nuclear deterrence was based on the assumption that an adversary would refrain from launching a first strike if it were confident that the other side would retain sufficient capabilities to inflict retaliatory destruction. This logic ultimately gave rise to the concept of mutually assured destruction (MAD). Paradoxically, strategic advantage became associated not with the ability to win a war, but with creating conditions in which the costs of initiating war would be unacceptable to both sides. This distinction is particularly important when drawing comparisons with cyberspace. Gjelinčič and Duyvesteyn point out that the automatic interpretation of the use of cyber power as a form of warfare has increasingly become subject to critical reassessment within strategic studies. The effects of cyber operations often do not conform to the classical model of nuclear or large-scale military force employment. Consequently, explaining cyber strategic competition requires a distinct conceptual approach.³

The experience of the Cold War revealed another important pattern: strategic competition combines technological rivalry with institutional and economic competition. The launch of the *Sputnik 1* satellite by the Soviet Union on October 4, 1957, generated a strong perception of technological inferiority in the United States. In 1958, the Advanced Research Projects Agency (ARPA) was established, with its activities focused on the development of high-risk, high-impact technological innovations in the field of defense. It was within this institutional environment that the development of networking technologies began, which later contributed to the formation of the Internet. Thus, a historical paradox lies in the fact that part of the technological foundations of contemporary cyberspace emerged within the broader context of strategic competition during the Cold War.

The end of the Cold War did not mark the end of strategic competition. Following the dissolution of the Soviet Union in December 1991, the international system came to be characterized by the pronounced predominance of the United States. At the same time, however, the rapid globalization of digital infrastructure began to transform the strategic environment. The proliferation of the Internet, the widespread adoption of personal computers, the development of mobile communications, and the digitalization of economic processes created a new security environment. Information networks, initially regarded primarily as instruments of economic efficiency, communication, and knowledge dissemination, gradually evolved into critical infrastructure essential to national security. Dwyer notes that a geopolitical understanding of cybersecurity cannot be reduced to an approach focused solely on human and state actors, as computational infrastructure, software systems and network interconnections themselves create distinctive conditions for the exercise of power.⁴

The discovery of the Stuxnet malware in 2010 marked a qualitatively new stage in the development of strategic cyber operations. The malware was specifically designed to target the industrial control systems used at Iran's Natanz nuclear facility, demonstrating the capacity of digital code to affect physical processes. This case confirmed that cyber operations are not limited to the theft of data or the temporary disruption of websites. An actor possessing the requisite capabilities can employ digital means to influence the physical functioning of industrial infrastructure. It is at this juncture that cyber power began to emerge as a distinct category of strategic power.

The growing geopolitical significance of cyber power has also transformed the spatial conceptions underlying classical geopolitics. Traditional geopolitical thought has focused on territorial location, maritime routes,

³ Žilinčik, S., Duyvesteyn, I. „Strategic Studies and Cyber Warfare.“ *Journal of Strategic Studies*, 2023. 836–857.

⁴ Dwyer, A. „Cybersecurity's Grammars: A More than Human Geopolitics of Computation.“ *Area*, 2021.

landmass, natural resources, and geographical depth. In cyberspace, however, power is increasingly shaped by network architecture, data centers, software, undersea communication cables, cloud computing infrastructure, satellite communications and technological production chains. According to Ashrafi, the spatial dimension of power in cyberwarfare demonstrates that the digital domain does not eliminate the significance of geography; rather, it reshapes and reconfigures its role.⁵ Thus, in contemporary cyber geopolitics, territory and networks do not replace one another; rather, they constitute interconnected foundations of power.

Realism and neorealism provide an important theoretical framework for explaining these processes. From a realist perspective, States operate within an international system in which there is no overarching authority ultimately responsible for ensuring their security. Consequently, States associate the provision of security with their own capabilities. This logic is particularly evident in cyberspace, where states cannot rely solely on international norms or collective mechanisms to protect their critical infrastructure. Instead, they require national cyber capabilities, intelligence resources, incident-response institutions and technological resilience. According to Chervinska, the geopolitics of cybersecurity demonstrates the interrelationship between the dynamics of international power and State Security.⁶

From a realist perspective, one of the principal mechanisms underlying strategic competition is the security dilemma. The security dilemma arises when measures adopted by one state to enhance its own security are perceived as threatening by another state. In response, the latter increases its own capabilities, which, in turn, reinforces the initial state's perception of threat. In cyberspace, this problem is further complicated by the difficulty of clearly distinguishing between defensive and offensive capabilities. The ability to penetrate networks, identify vulnerabilities, and assess an adversary's digital infrastructure may be employed both for defensive intelligence purposes and for preparing offensive operations. Beckerman's question of whether an autonomous cyber security dilemma exists reflects the broader theoretical significance of this problem.⁷

Another defining characteristic of the contemporary phase of strategic competition is the expansion of the space between the traditional conditions of war and peace. A significant proportion of cyber operations takes place below the threshold of armed conflict. States may conduct intelligence operations, collect data, disrupt political processes, or exert pressure on digital infrastructure without their actions reaching the legal or political threshold traditionally associated with an armed attack. Libetrau notes that cyber conflict conducted below the threshold of war is becoming increasingly significant in contemporary security policy, while the examples of France, the Netherlands and Norway demonstrate that European States increasingly recognize this environment as an independent strategic reality.⁸ Moreover, the insufficient clarity of strategic guidance in these states is identified by the author as a significant challenge.

This circumstance significantly changes the nature of strategic competition. During conventional arms races, primary attention was devoted to preparing for potential war; in cyberspace, however, competition can be conducted continuously. Cyber intelligence operations, covert network intrusions, information gathering, vulnerability discovery and the assessment of an adversary's capabilities are carried out even during periods of peace. Under such conditions of competition, it is difficult to identify a clear point at which peace ends and conflict begins. In analyzing the relationship between cyber operations and subversion, Mearsheimer argues that a substantial proportion of cyber conflict occurs at low intensity and below the threshold of armed conflict.⁹ Accordingly, a significant part of contemporary strategic competition takes the form of continuous, covert and incremental competition.

The power transition approach is also important for understanding contemporary strategic competition from a theoretical perspective. Within the international system, the growing capabilities of a rising power may

⁵ Ashraf, C. „A Preliminary Engagement with the Spatiality of Power in Cyberwar.“ *GeoJournal*, 2023. 5555–5573.

⁶ Czerwińska, M. „Geopolitics of Cybersecurity: International Power Dynamics and State Security in Cyberspace.“ *Humanities & Social Sciences Reviews*, 2025.

⁷ Beckerman, C. „Is There a Cyber Security Dilemma?“ *Journal of Cybersecurity*, 2022.

⁸ Liebetrau, T. „Cyber Conflict Short of War: A European Strategic Vacuum.“ *European Security*, 2022. 497–516.

⁹ Maschmeyer, L. „Subversion, Cyber Operations, and Reverse Structural Power in World Politics.“ *European Journal of International Relations*, 2022. 79–103.

constitute a long-term strategic challenge for the established leading state. In the XXI century, this issue has become particularly evident in the relationship between the United States and China. China's growing economic, technological and military capabilities have been accompanied by competition in the areas of semiconductors, artificial intelligence, fifth-generation communication networks, data, quantum technologies and cyber capabilities. Fedoniuk and Magdysiuk regard the confrontation between the United States and China in the field of cybersecurity as an important dimension of contemporary strategic competition. Accordingly, cyberspace constitutes an additional arena of competition within the potential process of power transition.¹⁰

The significance of cyber competition between the United States and China is not limited to their bilateral relationship. The technological policies of these two states influence other countries' choices regarding digital infrastructure, data security, technology partners and cybersecurity standards. Sanchez and Akiyesilmen characterize the technological conflict between China and the United States in cyberspace as part of high politics competition. In this context, the object of strategic competition is no longer limited to a specific military capability but also encompasses the ability to shape the technological order.¹¹

Russia's approach represents a distinct model of strategic cyber competition. In Russian security policy, the information space is understood as a broad strategic category in which technical cyber operations, political communication, information influence, and military objectives may be employed in an interconnected manner. In comparing the evolution of the cybersecurity strategies of the United States and Russia, Hassan and other co-authors emphasize the different ways in which the two States link cyber warfare to national security requirements.¹² This difference demonstrates that a quantitative assessment of cyber capabilities alone is insufficient. It is also necessary to take into account the political doctrine and strategic culture that shape their use.

Another significant consequence of the geopolitical transformation of strategic competition is that power is becoming increasingly associated with the resilience of digital systems. The strength of a modern State is determined not only by how effectively it can attack an adversary's systems. Equally important is its ability to maintain the continuity of its own State institutions, energy sector, financial system, defense networks, communications infrastructure and public services. Accordingly, cyber resilience is emerging as a component of strategic power. Preventing attacks is not always possible; therefore, a State's ability to rapidly restore functionality, mitigate damage and preserve its capacity for political decision-making has a direct impact on the outcome of strategic competition.

This gives rise to an important characteristic of the relationship between cybersecurity and strategic competition. On the one hand, strategic competition increases security threats; on the other, it accelerates the development of States' cybersecurity capabilities. The growing capabilities of a competitor generate increased investment in cyber defense, personnel training, intelligence systems, critical infrastructure protection and technological research. Thus, strategic competition emerges as one of the driving factors behind the development of cybersecurity. However, the same process can also produce the opposite effect, as the continuous accumulation of capabilities may deepen mistrust, increase the prevalence of covert operations and complicate the establishment of stable international rules.

The XXI century model of strategic competition therefore differs from the classical arms race in several fundamental respects. It is conducted continuously rather than only during periods of overt crisis; it involves both state and non-State actors, as well as private entities; a substantial portion of the capabilities involved remains invisible and difficult to measure; the boundary between defensive and offensive resources is often blurred; operations largely remain below the threshold of armed conflict; and the high pace of technological innovation rapidly alters the balance of power. The cyber conflict occurring below the threshold of war, as

¹⁰ Fedoniuk, S., Magdysiuk, S. „US China Confrontation in Cyber Security.“ *Історико політичні проблеми сучасного світу*, 2022. 113–127.

described by Libetrau, represents one of the most evident manifestations of this new strategic environment.¹³ This environment compels States to align strategic planning not only with preparations for potential war, but also with the continuous competition that takes place during peacetime.

Thus, the historical development of strategic competition can be understood as comprising several interconnected stages. The first stage is associated with military-technological competition during the industrial era. The second stage encompasses the nuclear and missile arms race of the Cold War, when deterrence and strategic stability became central categories of international security. The third stage, beginning in the 1990s, is associated with the rapid development of digital infrastructure and the emergence of cybersecurity as a distinct security concern. The fourth stage, beginning in the second half of the 2000s, is characterized by the establishment of cyber operations as an instrument of interstate competition. The fifth and current stage is defined by the integration of cyber power, artificial intelligence, data control, digital sovereignty and advanced technologies into a broader framework of strategic competition.

Accordingly, in the XXI century, strategic competition should be understood as a multidimensional competition among states for relative power and long-term strategic advantage, in which, alongside military power, technological capabilities, cyber power, informational superiority, economic resilience and control over digital infrastructure have become increasingly significant. Cyberspace is no longer merely an additional arena of this competition. Rather, it is itself transforming the dynamics of strategic competition by reducing the constraining significance of geographical distance, expanding the scope for covert action, complicating the assessment of adversaries' intentions and situating interstate competition in the space between the traditional boundaries of war and peace. Due to the aforementioned, a contemporary theoretical understanding of strategic competition is incomplete without considering the cybersecurity factor. This interrelationship also provides a basis for answering the first research question: strategic competition contributes to the strengthening of cybersecurity by fostering the development of capabilities, institutional resources and technological innovation, while simultaneously generating new threats, a security dilemma and an environment of continuous competition. Understanding this dual nature constitutes one of the principal theoretical prerequisites for comprehending the geopolitical essence of strategic competition in the XXI century.

References

- Ashraf, C. (2023). A preliminary engagement with the spatiality of power in cyberwar. *GeoJournal*, 88, 5555–5573. <https://doi.org/10.1007/s10708-023-10929-z> [Springer Nature Link](#)
- Beckerman, C. E. (2022). Is there a cyber security dilemma? *Journal of Cybersecurity*, 8(1), Article tyac012. <https://doi.org/10.1093/cybsec/tyac012> durham-repository.worktribe.com
- Czerwińska, M. (2025). Geopolitics of cybersecurity—International power dynamics and state security in cyberspace. *Humanities & Social Sciences Reviews*, 13(2), 337–342. <https://doi.org/10.18510/hssr.2025.13246> [Humanities & Social Sciences Reviews](https://www.humanitiesandsocialsciencesreviews.com)
- Dwyer, A. C. (2023). Cybersecurity's grammars: A more-than-human geopolitics of computation. *Area*, 55(1), 10–17. <https://doi.org/10.1111/area.12728> [Wiley Online Library](https://onlinelibrary.wiley.com)
- Fedoniuk, S., & Maghdysiuk, S. (2022). US-China confrontation in cyber security. *Історико-політичні проблеми сучасного світу*, (45), 113–127. <https://doi.org/10.31861/mhpi2022.45.113-127> [Історико-політичні проблеми сучасного світу](https://www.mhpi.org)
- Gomez, M. A., & Whyte, C. (2022). Unpacking strategic behavior in cyberspace: A schema-driven approach. *Journal of Cybersecurity*, 8(1), Article tyac005. <https://doi.org/10.1093/cybsec/tyac005> [Oxford Academic](https://academic.oup.com)
- Liebetrau, T. (2022). Cyber conflict short of war: A European strategic vacuum. *European Security*, 31(4), 497–516. <https://doi.org/10.1080/09662839.2022.2031991> doi.org

¹³ Liebetrau, T. „Cyber Conflict Short of War: A European Strategic Vacuum.“ *European Security*, 2022. 497–516.

- Maschmeyer, L. (2023). Subversion, cyber operations, and reverse structural power in world politics. *European Journal of International Relations*, 29(1), 79–103.
<https://doi.org/10.1177/13540661221117051> Lennart Maschmeyer, 2023
- Žilinčík, S., & Duyvesteyn, I. (2023). Strategic studies and cyber warfare. *Journal of Strategic Studies*, 46(4), 836–857. <https://doi.org/10.1080/01402390.2023.2174106>