THE CHINESE APPROACH TO THE CONCEPT OF DETERRENCE IN CYBERSPACE*

Dragan Trailović[1]

Delivered: 11.7.2025. *Language:* Serbian
Corrected: 18.9.2025. *Type of paper*: Review scientific paper
Accepted: 14.10.2025. *DOI number*: 10.5937/vojdelo2503055T

Abstract: This paper examines the Chinese approach to the concept of deterrence in cyberspace. It first discusses the evolution of the concept of deterrence—from nuclear to cross-domain—with particular attention to the notion of cyber deterrence. The paper then presents the specific features of the Chinese approach to deterrence and how this concept is shaped in the People's Republic of China in relation to its strategic culture. The aim of the paper is to illustrate how the PRC interprets cyber deterrence within the framework of its broader conception of integrated strategic deterrence, that is, how it conceptualizes deterrence in the cyber domain. The paper concludes that the PRC perceives cyberspace as an extension of its sovereign territory, where the strategy of cyber deterrence—integrated with other domains—serves to protect vital national interests.

Keywords: *deterrence, integrated strategic deterrence, cyberspace, information warfare, cyber deterrence, People's Republic of China*

Introduction

The concept of deterrence has evolved from its nuclear roots into more complex multidomain approaches, which include cyber deterrence as a key component. The concept itself is subject to different interpretations, depending on the strategic culture, geopolitical context, and technological development of the state applying it. The Chinese approach to deterrence developed from nuclear deterrence in the 1970s and 1980s, later expanding into other domains, including cyberspace. As an emerging global power, the PRC has actively developed its own approaches to cybersecurity

* The work was created within the framework of the project "Serbia and Challenges in International Relations 2025", funded by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and implemented by the Institute for International Politics and Economy during 2025.

[1] Institute of International Politics and Economics, Belgrade, Republic of Serbia, E-mail: dragan.trailovic@diplomacy.bg.ac.rs, ORCID: https://orcid.org/0000-0001-9707-9867

and deterrence. Its approach is deeply rooted in its strategic culture and is adapted to contemporary technological advancements.

Chinese strategic thought emphasizes that modern societies, which rely on interconnected information infrastructures for essential services such as energy, finance, healthcare, and military operations, are inherently vulnerable to systemic disruptions. A major cyberattack could paralyze national computer networks, destabilize the economy, and trigger social unrest, thereby directly threatening the stability and sovereignty of the state. This vulnerability positions deterrence in cyberspace as one of the imperatives of national defense and security—but also as an offensive instrument, wherein the mere threat of destructive cyberattacks can deter adversaries from hostile actions.

The increasing complexity of the concept of deterrence in the PRC has been significantly influenced by overall technological advancement—both in conventional weaponry and in cyber capabilities. Consequently, the PRC reexamines its strategic deterrence through the argument that maintaining strategic stability in an era of rapid technological change requires an integrated, multidomain approach that substantially surpasses the traditional model of nuclear deterrence.

Conceptualization of Deterrence: From Nuclear to Cyber Deterrence

As with many other concepts across various disciplines within the social sciences, it is evident that there is no universally accepted or unambiguous definition of the concept of deterrence. Numerous authors—both from theoretical perspectives and among practitioners, including political and military strategists—define the concept of deterrence, its types and variants, methods of application, means, and objectives differently, based on varying criteria. All of this is conditioned by the specific historical period in which the concept emerged and evolved, the particular context in which it was applied, the distinct strategic cultures of the states employing it, as well as the broader regional and global geopolitical circumstances and the level of technical and technological development, particularly in the field of armaments. Regardless, the underlying logic of the concept itself largely remains the same.

Put simply, the concept rests on the logic that one actor possesses a credible capability (ability or capacity) to dissuade another actor (the opponent) from undertaking a specific hostile action by persuading them that the expected costs of such actions outweigh the anticipated benefits (George & Smoke, 1974, p. 11; Freedman, 2021, p. 2). Essentially, deterrence is based on influencing the decision-making process of potential adversaries by shaping their perception of the cost–benefit balance of their actions (Mearsheimer, 1983, p. 14; Nye, 2017, p. 53; Mazarr, 2021, pp. 21–23; Kopanja, 2022, p. 83).

The emergence of nuclear weapons after the Second World War required a more profound theoretical examination of deterrence, resulting in the introduction of this concept as a formal subject of academic inquiry within the field of strategic studies and international relations. It is important to note that deterrence as a practice (deterrence

as techne) existed long before the Second World War; however, it was only then that the term acquired its linguistic expression—deterrence—as a defined concept (Kopanja & Aizenhamer, 2022, pp. 20–21).

Nuclear deterrence, understood as strategic deterrence, has over time been distinguished as the "pure" form of deterrence (George & Smoke, 1974, pp. 39, 46; Mueller, 2021, p. 49). The classic example is the concept of mutual assured destruction (MAD) during the Cold War, when both the United States and the Soviet Union maintained what was known as a second-strike capability to ensure retaliation in the event of a nuclear attack (Ajzenhamer, 2024, pp. 43–67; Kostić Šulejić, 2024, pp. 19–21).

In the literature that emerged after the Second World War—throughout the Cold War and continuing into the present—several phases in the development of the concept have been identified, forming a periodization often described in terms of five waves. Unlike the first three waves, which were primarily focused on nuclear and conventional deterrence in the context of great power conflict, the fourth wave concentrated on asymmetric deterrence involving non-state actors such as "rogue states," terrorists, insurgents, and ethnic conflict (Lupovici, 2010; Osinga & Sweijs, 2021, pp. ix–x; Sweijs & Zilincik, 2021, p. 130; Michaels, 2024, pp. 1058–1059). The fourth wave was subsequently complemented by a fifth, in which the relationships among great powers and the Cold War concepts of deterrence once again became central—but in a new and distinct context, particularly in relation to emerging technological trends such as artificial intelligence (AI) and cyberspace (Michaels, 2024, pp. 1059, 1062–1064).

During the Cold War, nuclear deterrence represented the dominant form of deterrence, whereas contemporary conceptions increasingly emphasize hybrid approaches that combine military, political, economic, and informational elements (Vuletić, 2017). With the rise of multidomain conflicts—those encompassing new threats across land, maritime, air, space, and cyber domains—cross-domain deterrence has gained growing importance. This form of deterrence includes, as previously noted, threats in the conventional, nuclear, cyber, and space spheres (Vuletić, 2017; Vuletić, Milenković, & Đukić, 2021, pp. 3–4).

According to Tim Sweijs and Samuel Zilincik, the focus on cross-domain deterrence arises from the challenges of integrating and synchronizing military operations across different domains (land, air, sea, cyber, and space) and at various levels of warfare (strategic, operational, and tactical). In addition, this shift reflects the increasing prevalence of hybrid operations conducted within the "gray zone," which employ a combination of military and non-military means below the threshold of conventional armed conflict and often without clear attribution (Sweijs & Zilincik, 2021, p. 131). A key feature of this type of deterrence is that it involves the use of threats in one domain to counter adversary activities in another (Lindsay & Gartzke, 2019, p. 4; Sweijs & Zilincik, 2021, p. 133). A particular variant of this form of deterrence is further defined as integrated deterrence (Gartzke & Lindsay, 2024, pp. 2–4).

According to the most recent approaches to the analysis of cross-domain and, more specifically, integrated deterrence, the domain of cyberspace constitutes the central—or nodal—domain, given its characteristic interconnection with all other domains. For example, according to these perspectives, cyberspace—more precisely, digital networks—serves as the connective tissue linking various types of military capabilities across land, sea, undersea, air, atmospheric, and space environments

(Gartzke & Lindsay, 2024, pp. 2–4). The importance of cyberspace also lies in the fact that activities conducted within this domain can generate, or manifest, consequences in physical form and in the real world—that is, across other domains (Schneider, 2019, p. 98).

The perception of cyberspace as a distinct domain—the "fifth domain"—implies that cyber operations can be treated both as an instrument of deterrence capable of exerting influence across other conventional domains, on the one hand, and as a domain from which such operations must themselves be deterred, on the other (Schneider, 2019, pp. 98, 100). As Joseph S. Nye explains, cyber deterrence should not be viewed in isolation from the broader spectrum of deterrence measures. Essentially, just as a response to a land-based attack does not necessarily have to come exclusively from land forces, a response to a cyberattack need not rely solely on cyber means; in other words, it need not be confined to the cyber domain (Nye, 2017, p. 46). For these reasons, cyber deterrence is predominantly understood through the lens of multidomain deterrence.

Despite the lack of consensus in the literature regarding whether deterrence in cyberspace is even achievable, it nevertheless appears as a potential means of responding to malicious activities within the cyber domain, often drawing upon the traditional approaches, mechanisms, and logic of the deterrence concept.

In essence, cyber deterrence primarily relies on two fundamental deterrence mechanisms: the mechanism of denial (strengthening defenses so that attacks become ineffective) and the mechanism of punishment (threats of retaliatory measures). In addition, the development of international norms and agreements contributes to shaping expectations of acceptable behavior in cyberspace (Nye, 2017, pp. 54–62). According to Nye, an additional mechanism applies in cases where actors are closely connected and interdependent—economically, politically, or in other ways—so that an attack on one could also impose significant costs on the attacker. Even if an adversary believes it can successfully carry out an attack without facing direct retaliation, the potential loss of mutually beneficial relationships may itself serve as a powerful means of deterrence (Nye, 2017, p. 58).

As previously noted, cyber deterrence possesses its own specific characteristics that distinguish it from other forms of deterrence. One of the most frequently emphasized among these is the problem of attribution—that is, the challenge of clearly identifying the attacker, primarily due to technical complexity. Anonymity in cyberspace poses significant challenges to identifying the origin of cyberattacks. Attackers can conceal their identities or falsely claim to act on behalf of others, thereby complicating precise attribution. Furthermore, the process of gathering evidence to trace such attacks often takes considerable time, delaying responses and weakening efforts to deter future attacks. Non-state actors and proxy groups further complicate the effectiveness of deterrence in this domain, as they can operate outside the traditional frameworks of state-based deterrence. Additionally, the rapid evolution of technology creates an asymmetric battlespace, where offensive capabilities often surpass defensive measures (Libicki, 2009, pp. xvi, 41–52; Nye, 2017, pp. 49–52; Sweijs & Zilincik, 2021, p. 134).

The Specificity of the Concept of Deterrence in the People's Republic of China

The concept of deterrence is interpreted in different ways depending on the strategic culture and local specificities of individual countries. Although it often draws upon Western theories, within the PRC the concept acquires distinctive characteristics, adapting to national conditions. As Jeffrey H. Michaels observes, in countries such as India and the PRC, deterrence scholars develop specific approaches that reinterpret and modify Western concepts in order to align them with local security challenges and strategic objectives (Michaels, 2024, p. 7).

Similar to the Western perspective, the Chinese understanding of the concept of deterrence was primarily grounded in the notion of nuclear deterrence and, as such, matured during the 1970s and 1980s. Since the 1990s, there has been a proliferation of both academic and practical (political and military) sources that have developed the Chinese view—above all, regarding nuclear deterrence. It is important to note that the Chinese approach to nuclear deterrence is based on a defensive nuclear strategy embodied in the policy (doctrine) according to which the PRC would employ nuclear weapons only in the event that it were attacked first—commonly known as the no-first-use policy (Leveringhaus, 2023).

The concepts of deterrence, as understood in the People's Republic of China, encompass both elements of deterrence and elements of coercion. Within the Chinese strategic framework, deterrence is a concept that transcends the mere prevention and dissuasion of adversaries from acting; beyond that, it also aims to compel them to change their behavior. According to many scholars, this differs from the Western conceptualization of deterrence, where the concept is typically viewed as discouraging adversaries from undertaking undesirable actions—that is, as a mechanism for maintaining the status quo (Chase & Chan, 2016, p. 4; Cheng, 2017, p. 151; Cheng, 2021, pp. 178–179; Kaufman & Waidelich, 2023, pp. 9–10; Beauchamp-Mustafaga, 2023, p. 100).

Essentially, the Chinese understanding of successful deterrence involves not only signaling resolve but also the actual employment of forces. The Chinese approach to deterrence is based on the notion that the credibility of deterrence increases as it approaches real outcomes—meaning that deterrence signals must closely reflect the realities of warfare. This approach is demonstrated through actions that may include real kinetic or cyber warning strikes intended to convey the utmost determination of the deterring side (Kolton, 2017, p. 133; Cheng, 2021, p. 184).

In the Chinese approach, effective deterrence rests upon three components. First, the state must possess credible capability—tangible means and technology—to carry out any threat or retaliatory action. Second, there must exist a clear and resolute commitment to undertake such actions if provoked, which reinforces the authenticity of the threat. Finally, this capability and commitment must be effectively communicated so that potential adversaries are fully aware of both the means and the readiness of the deterring side to act (China Aerospace Studies Institute, 2022, p. 127; Kaufman & Waidelich, 2023, p. 12).

Another significant feature of the Chinese approach to deterrence is that deterrence is not an end in itself but rather a means for achieving broader national interests and objectives. More precisely, within the Chinese framework, deterrence is employed not only to prevent adversary actions in specific domains but also as a strategic and tactical instrument for attaining predetermined political goals (Cheng, 2021, p. 179).

The evolution of China's concept of deterrence has been influenced primarily by the perception that the People's Republic of China is not technologically advanced enough in comparison with other major powers—meaning that the credibility of its deterrent potential is constrained by the level of its technological development. Furthermore, the PRC perceives the actions of the United States, particularly its strategic and extended deterrence, as instruments of hegemony aimed at preserving American dominance in the Asia-Pacific region. China interprets this strategy as a method of containment designed to limit its development and regional influence. In response to these factors, the PRC has revised its understanding of deterrence, turning toward the development of asymmetric capabilities (e.g., cyber weapons, space technologies), thereby strengthening the multidomain perspective of deterrence (Lindsay & Gartzke, 2019, p. 12; Morgan, 2019, p. 55). This includes the expansion and diversification of its nuclear arsenal, the enhancement of missile defense systems, and the development of advanced cyber and space capabilities as complements to traditional deterrence instruments (Kaufman & Waidelich, 2023, p. iii).

Changes in the understanding of the concept of deterrence entailed a broadening of the domains encompassed by the concept, ultimately resulting in the development of the so-called integrated strategic deterrence concept. This involved emphasizing the importance of combining multiple forms of deterrence—nuclear, conventional, space, and informational deterrence. In addition, the concept highlights the significance of synergy between military and non-military (civilian) elements of national power. Ultimately, this framework incorporates military, political, economic, diplomatic, scientific, technological, informational, and cultural instruments of national power (Chase & Chan, 2016; Chang, 2021, p. 180).

Building on these foundations, in recent years the People's Republic of China has expanded its deterrence strategy to include a range of nonconventional means—such as economic sanctions, diplomatic initiatives, and influence over the information environment—directed not only at other states but also at non-state actors, including multinational corporations, international organizations, civil society groups, and individuals (Odell, 2023, p. 45).

.

Cyber Deterrence as a Component of Integrated Strategic Deterrence in the People's Republic of China

With respect to cyberspace, cybersecurity, and cyber deterrence, some scholars argue that this domain—compared with others—is the one most frequently interpreted and practiced differently across various states and their respective strategic contexts (Gjesvik, 2018, p. 174).

The People's Republic of China perceives cyberspace as an extension of its sovereign territory—that is, as a domain in which strict state control is deemed essential for protecting vital national interests, particularly social stability, sovereignty, and security. For this reason, China actively advocates at the international level for the establishment of new norms to regulate this field, based on a state-centric approach and the application of the principle of state sovereignty within these domains as well—often referred to as "cyber sovereignty" (Kolton, 2017, pp. 126–130; Gjesvik, 2018, pp. 175–177; State Council Information Office, 2023; Creemers, 2024).

In official Chinese documents, cyberspace is explicitly defined as a domain encompassing national interests and issues of national security (State Council Information Office, 2015; State Council Information Office, 2019). Unlike the Western perspective on cybersecurity, which often emphasizes strictly technical aspects, the Chinese approach incorporates economic, cultural, political, and other dimensions. This broader perspective is grounded in the concept of comprehensive national security, wherein the protection of information and communication infrastructure is inseparable from the preservation of political and overall socioeconomic stability (Zhang & Creemers, 2023, p. 10).

Another important aspect for understanding the role of cyberspace in safeguarding vital national interests is the concept of civil–military fusion as a strategy for integrating military and civilian resources. In 2015, President Xi Jinping elevated this strategy to the national level, particularly emphasizing the importance of information technologies. He underscored that the fields of cybersecurity and informatization are key components of this fusion (Doshi et al., 2023).

The conceptualization and practical application of cyber deterrence in the People's Republic of China are inherently connected to—and can only be interpreted in relation to—China's understanding of other related concepts, such as information space, security, and warfare, or network space, security, and warfare. In fact, Chinese military doctrine situates cyberspace and cyber warfare within the broader framework of information warfare and the information domain (Schneider, 2019, p. 99). Cyberspace is regarded merely as a subset of the information space and is not treated as a separate domain from it (Giles & Hagestad, 2013). It is important to note that there is no clear distinction in the meaning of these terms, as the terms cyber and network are often used interchangeably in Chinese military terminology, whereas information serves as the overarching term. Thus, information warfare encompasses cyber operations, electronic warfare (disruption of the electromagnetic spectrum), and psychological oper-

ations (narrative control) (Vuletić & Stanojević, 2022, pp. 57–60; Zhang & Creemers, 2023, p. 45).

In official Chinese documents and analyses—predominantly from military circles—information deterrence is identified as one of several components of overall strategic deterrence, while cyber (network) deterrence is delineated as a form of military conflict within cyberspace, with the explicit indication that it can also be employed during peacetime (China Aerospace Studies Institute, 2021, pp. 243–244; China Aerospace Studies Institute, 2022, pp. 130, 152).

As one of the significant segments of China's deterrence strategy, information deterrence extends beyond the cyber realm to encompass broader information operations. This concept includes the use of cyber operations and other forms of information warfare to compel adversaries to act in ways consistent with the country's defined political objectives. Such operations involve a wide spectrum of activities, including computer network attacks, computer network defense, as well as electronic warfare, psychological operations, camouflage, concealment and deception, and kinetic strikes on information and communication networks and command-and-control facilities (Cheng, 2016; China Aerospace Studies Institute, 2022, p. 130).

Information deterrence combines deterrence and compellence, targeting adversary actions in conventional domains by means of cyber tools, rather than deterring them solely within the information domain. This approach reflects Chinese strategists' belief in the applicability of a so-called deterrence ladder used in other domains, whereby the gradation of information deterrence ranges from the lowest level—mere demonstration of cyber capability—to the highest level—actual offensive operations designed to achieve the desired deterrent effects (Zhang & Creemers, 2023, p. 17). Thus, escalation to direct military action becomes a last resort.

From the Chinese perspective, information deterrence has three primary characteristics. First is permeability: because of the very nature of information, information deterrence can transcend traditional military domains and penetrate political, economic, scientific, cultural, technological, and psychological spheres. Second is indeterminacy, arising from the problem of attribution—information attacks often originate from ambiguous sources. Third is the multiplicity of forms of information deterrence, ranging from "soft" methods such as malware, data manipulation, and electronic espionage to "hard" kinetic attacks on information infrastructure (China Aerospace Studies Institute, 2022, p. 130).

According to Chinese sources, information deterrence is classified—alongside other forms of deterrence (nuclear, conventional, and space)—as a component of overall strategic deterrence. This suggests that deterrence in cyberspace holds equal importance to nuclear deterrence due to its immense destructive potential (China Aerospace Studies Institute, 2022, p. 128).

Dean Cheng concludes that, in the case of information deterrence as well, the Chinese approach is based on the logic that deterrence is intended to enable the deterring side to achieve a specific political objective, rather than merely to prevent the opposing side from undertaking actions within the information domain (Cheng, 2021, pp. 188–189).

In addition, Chinese sources further define cyber deterrence as the prevention of large-scale cyberattacks through the demonstration of a nation's capability both to conduct and to defend against network operations, accompanied by a clear expression of readiness to retaliate. It focuses on deterring network attacks that could cause significant damage, primarily those originating from hostile states or terrorist organizations, thereby protecting national security and developmental interests. This form of deterrence is not confined to the use of cyber weapons, as it encompasses a diverse range of deterrent instruments, including traditional military forces (China Aerospace Studies Institute, 2021, p. 244; Beauchamp-Mustafaga, 2023, pp. 103–104).

While earlier approaches to cyber deterrence focused exclusively on deterring large-scale cyberattacks (strategic cyber deterrence), later perspectives within Chinese strategic thinking distinguish, in addition to the strategic level, cyber deterrence at the tactical level. Strategic cyber deterrence involves the threat and demonstration of capabilities to conduct cyber operations against an adversary's key computer networks, such as those associated with national security and critical infrastructure (e.g., military command systems, transportation networks, and communication nodes). In contrast, tactical cyber deterrence addresses smaller, more frequent cyber threats and infiltration attempts aimed at ensuring national security across various sectors during peacetime (China Aerospace Studies Institute, 2021, pp. 243–244; China Aerospace Studies Institute, 2022, p. 152; Beauchamp-Mustafaga, 2023, pp. 104–105).

The primary forms of cyber deterrence include: demonstrating and testing offensive cyber technologies; partial public disclosure of cyber weapons and equipment through the media; conducting operational exercises in cyberspace; and revealing to the public cyberattacks that have already been carried out (Beauchamp-Mustafaga, 2023, p. 107).

Initially, the People's Republic of China adopted an approach focused on the development of asymmetric offensive capabilities in cyberspace, designed to deter conventional attacks by demonstrating the potential for a massive cyber strike. However, as its digital infrastructure expanded, its exposure to cyber threats also increased, leading to the development of a defensive component. Over time, the advancement of defense and protection of digital assets became a priority—driven by the rapid growth of the information and communication technology (ICT) sector and by intense international competition in the cyber domain (Zhang & Creemers, 2023, pp. 10–21).

Ultimately, this development culminated in a new reform of the organizational structure of China's armed forces in 2024. Through this reorganization, the PRC abolished the so-called Strategic Support Force and separately established forces responsible for space, cyberspace, information support, and integrated logistical support. The Cyberspace Support Force is tasked with conducting both defensive and offensive information operations, including strengthening the nation's cyber border defense, promptly detecting and countering intrusions into computer networks, and maintaining national cyber sovereignty and information security (Ministry of National Defense, 2024).

Conclusion

China's strategy of deterrence in cyberspace reflects its broader vision of comprehensive national security, which emphasizes the protection of vital national interests—above all, territorial integrity and sovereignty, internal stability of the social and political order, and sustained economic growth and development. The Chinese strategic framework indicates that mastery of the information domain is essential for securing strategic advantage in an era where control over information is increasingly equivalent to geopolitical power.

In this context, the People's Republic of China views cyberspace as a key domain for the projection of power, underscoring the importance of information control and the development of both offensive and defensive capabilities in this realm. In contrast to Western approaches that promote an open and free internet, the PRC regards cyberspace as an extension of its sovereign territory, where state control is deemed necessary to safeguard socioeconomic and political stability. This perspective shapes its cyber deterrence strategy, which emphasizes the integration of cyber operations within the broader framework of strategic deterrence. As such, cyber deterrence is not treated in isolation but is instead embedded within wider concepts of information warfare.

References:

[1] Ajzenhamer, V. (2024). *Celuloidna apokalipsa: kako je Amerika naučila da brine i da se plaši a-bombe*. Beograd: Službeni glasnik.

[2] Beauchamp-Mustafaga, N. (2023). Exploring Chinese thinking on deterrence in the not-so-new space and cyber domains. In R. D. Kamphausen (Ed.), *Modernizing deterrence: How China coerces, compels, and deters* (pp. 99-119). Seattle, WA, & Washington, DC: The National Bureau of Asian Research.

[3] Благојевић, В., и Радановић, Т. (2022). Стратешко одвраћање – кључне надлежности државних органа Републике Србије. *Војно дело*, 74(4), 28–39. https://doi.org/10.5937/vojdelo2204028B

[4] Chase, M. S., & Chan, A. (2016). *China's evolving approach to "integrated strategic deterrence"*. Santa Monica, CA: RAND Corporation.

[5] Cheng, D. (2016). Prospects for extended deterrence in space and cyber: The case of the PRC. The Heritage Foundation. Retrieved from https://www.heritage.org/defense/report/prospects-extended-deterrence-space-and-cyber-the-case-the-prc.

[6] Cheng, D. (2017). *Cyber dragon: Inside China's information warfare and cyber operations (The changing face of war)*. Santa Barbara, CA, & Denver, CO: Praeger.

[7] Cheng, D. (2021). An overview of Chinese thinking about deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands annual review of military studies 2020: Deterrence in the 21st century - Insights from theory and practice* (pp. 178–200). The Hague: T.M.C. Asser Press.

[8] China Aerospace Studies Institute. (2021). *In their own words: Science of military strategy 2013*. Air University. Retrieved from https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2021-02-08%20Chinese%20Military%20Thoughts-%20In%20their%20own%20words%20Science%20of%20Military%20Strategy%202013.pdf

[9] China Aerospace Studies Institute. (2022). *In their own words: Science of military strategy 2020*. Air University. Retrieved from https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-01-26%202020%20Science%20of%20Military%20Strategy.pdf.

[10] Creemers, R. (2024). The Chinese conception of cybersecurity: A conceptual, institutional, and regulatory genealogy. *Journal of Contemporary China*, *33*(146), 173-188. https://doi.org/10.1080/10670564.2023.2196508.

[11] Doshi, R., de La Bruyère, E., Picarsic, N., & Ferguson, J. (2021, April 5). *China as a 'cyber great power': Beijing's two voices in telecommunications*. Brookings Institution. Retrieved from https://www.brookings.edu/articles/china-as-a-cyber-great-power-beijings-two-voices-in-telecommunications/

[12] Freedman, L. (2021). Introduction - The evolution of deterrence strategy and research. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st century - Insights from theory and practice* (pp. 1-10). The Hague: T.M.C. Asser Press.

[13] Gartzke, E. & Lindsay, R. J. (2024). *Elements of Deterrence: Strategy, Technology, and Complexity in Global Politics*. New York: Oxford Academic.

[14] George, L. A., & Smoke, R. (1974). *Deterrence in American Foreign Policy: Theory and Practice*. *New York: Columbia University* Press.

[15] Giles, K., & Hagestad, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian, and English. In K. Podins, J. Stinissen, & M. Maybaum (Eds.), *5th International Conference on Cyber Conflict* (pp. 1-17). Tallinn: IEEE.

[16] Gjesvik, L. (2018). China's notion of cybersecurity: The importance of strategic cultures for cyber deterrence. In A. Josang (Ed.), *17th European Conference on Cyber Warfare and Security* (pp. 174-180). Reading, UK: Academic Conferences and Publishing International Limited.

[17] Kadlecová, L. (2024). *Cyber sovereignty: The future of governance in cyberspace*. Stanford: Stanford University Press.

[18] Kaufman, A. A., & Waidelich, B. (2023). *PRC writings on strategic deterrence: Technological disruption and the search for strategic stability*. CNA Occasional Paper. Retrieved from https://www.cna.org/reports/2023/04/PRC-Writings-on-Strategic-Deterrence.pdf.

[19] Kolton, M. (2017). Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. *Cyber Defense Review*, *2*(1), 119-154.

[20] Kopanja, M. (2023). Efektivnost odvraćanja – kada je odvraćanje „prava" strategija za ostvarivanje nacionalnih interesa?. *Srpska politička misao*, 80(2), 75–96. https://doi.org/10.5937/spm80-44241.

[21] Kopanja, M., & Ajzenhamer, V. (2022). Odvraćanje u raljama bezbednosne dileme. In V. Blagojević (Ed.), *Neutralnost i strateško odvraćanje* (pp. 15–38). Beograd: Medija centar „Odbrana".

[22] Костић Шулејић, М. (2024). *Војна неутралност и нуклеарно оружје: између поседовања и забране.* Београд: Институт за међународну политику и привреду.

[23] Leveringhaus, N. (2023). How China's nuclear past shapes the present: Ideological and diplomatic considerations in nuclear deterrence. In R. D. Kamphausen (Ed.), *Modernizing deterrence: How China coerces, compels, and deters* (pp. 29-42). Seattle, WA, & Washington, DC: The National Bureau of Asian Research.

[24] Libicki, M. C. (2021). *Cyberspace in peace and war* (2nd ed.). Annapolis, Maryland: Naval Institute Press.

[25] Lindsay, J. R., & Gartzke, E. (2019). Introduction: Cross-domain deterrence, from practice to theory. In J. R. Lindsay & E. Gartzke (Eds.), *Cross-domain deterrence strategy in an era of complexity* (pp. 1-23). New York: Oxford University Press.

[26] Lupovici, A. (2010). The emerging fourth wave of deterrence theory - Toward a new research agenda. *International Studies Quarterly*, 54(3), 705-732. http://www.jstor.org/stable/40931133.

[27] Марјановић, З. М. (2023). *Одвраћање као стратешки концепт у постхладноратовском периоду* (докторска дисертација). Универзитет у Београду, Факултет безбедности. https://fb.bg.ac.rs/download/RepozitorijumDisertacija/2024-06-10%20Marjanovic%20Zoran/Marjanovic_Zoran_Disertacija.pdf

[28] Mazarr, M. J. (2021). Understanding deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st century - Insights from theory and practice* (pp. 14-28). The Hague: T.M.C. Asser Press.

[29] Mearsheimer, J. J. (1983). *Conventional deterrence*. Cornell University Press.

[30] Michaels, J. H. (2024). Deterrence studies: A field still in progress. *Journal of Strategic Studies*. 47(6-7), 1058-1079. https://doi.org/10.1080/01402390.2024.2417388.

[31] Ministry of National Defense of the People's Republic of China. (2024, April 19). *Ministry of National Defense: Build a Cyberspace Featuring Peace, Security, Openness and Cooperation*. Retrieved March 06, 2025, from http://eng.mod.gov.cn/xb/News_213114/NewsRelease/16302070.html

[32] Morgan, P. M. (2019). The past and future of deterrence theory. In J. R. Lindsay & E. Gartzke (Eds.), *Cross-domain deterrence: Strategy in an era of complexity* (pp. 50-65). New York, NY: Oxford University Press.

[33] Mueller, K. (2021). The continuing relevance of conventional deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st century - Insights from theory and practice* (pp. 48-63). The Hague: T.M.C. Asser Press.

[34] Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44-71. https://doi.org/10.1162/ISEC_a_00266.

[35] Odell, R. E. (2023). "Struggle" as coercion with Chinese characteristics: The PRC's approach to nonconventional deterrence. In R. D. Kamphausen (Ed.), *Modernizing*

deterrence: How China coerces, compels, and deters (pp. 45-64). Seattle, WA, & Washington, DC: The National Bureau of Asian Research.

[36] Osinga, F., & Sweijs, T. (Eds.). (2021). *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st century - Insights from theory and practice*. The Hague: T.M.C. Asser Press.

[37] Schneider, J. G. (2019). Deterrence in and through cyberspace. In J. R. Lindsay & E. Gartzke (Eds.), *Cross-domain deterrence strategy in an era of complexity* (pp. 95-120). New York: Oxford University Press.

[38] State Council Information Office of the People's Republic of China. (2023, March 16). *China's law-based cyberspace governance in the new era*. State Council Information Office. Retrieved from https://english.www.gov.cn/archive/whitepaper/202303/16/content_WS6489542ec6d0868f4e8dcd56.html

[39] State Council Information Office of the People's Republic of China. (2019, July 24). *China's national defense in the new era*. State Council Information Office. Retrieved from https://english.scio.gov.cn/whitepapers/2019-07/24/content_75026111.htm

[40] State Council Information Office of the People's Republic of China. (2015, May 27). *China's military strategy*. State Council Information Office. Retrieved from https://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

[41] Sweijs, T., & Osinga, F. (2021). Conclusion: Insights from theory and practice. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st century—Insights from theory and practice* (pp. 504-530). The Hague: T.M.C. Asser Press.

[42] Sweijs, T., & Zilincik, S. (2021). The essence of cross-domain deterrence. In F. Osinga & T. Sweijs (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st century - Insights from theory and practice* (pp. 129–158). The Hague: T.M.C. Asser Press.

[43] Vuletić, D. V. (2017). Upotreba sajber prostora u kontekstu hibridnog ratovanja. *Vojno delo*, 69(7), 308 325. https://doi.org/10.5937/vojdelo1707308V

[44] Вулетић, Д. В. (2018). Психолошка димензија хибридног ратовања. *Војно дело*, 70(6), 274–281. https://doi.org/10.5937/vojdelo1806274V

[45] Вулетић, Д. В., Миленковић, М. Р., и Ђукић, А. Р. (2021). Сајбер простор као подручје сукобљавања: Случај САД – Иран и Северна Кореја. *Војно дело*, 73(1), 1–14. https://doi.org/10.5937/vojdelo2101001V

[46] Vuletić, D. V., & Stanojević, P. (2022). Concepts of information warfare (operations) of the United States of America, China, and Russia. *The Review of International Affairs,* 73(1185), 51–71.

[47] Zhang, E. S., & Creemers, R. (2023). *The evolution of Chinese perspectives on cyber deterrence and attribution*. Leiden Asia Centre. Retrieved from https://leidenasiacentre.nl/wp-content/uploads/2023/03/Chinese-Perspectives-of-Deterrence-and-Attribution-in-Cyberspace-1.pdf

S u m m a r y

This paper analyzes the Chinese model of cyber deterrence within the framework of integrated strategic deterrence. It first examines the evolution of the concept from nuclear to cross-domain deterrence, with particular attention to cyber deterrence. It then outlines the specific features of the Chinese approach, both to the general concept of deterrence and to the specific notion of deterrence in cyberspace.

Today, deterrence increasingly relies on hybrid and cross-domain approaches that combine military, political, economic, and informational elements. Within this context, the cyber domain occupies a significant position due to its capacity to permeate and influence other domains, although challenges such as attribution—stemming from anonymity and technical complexity—continue to pose substantial obstacles to its effectiveness.

The Chinese concept of deterrence represents a distinctive approach which, while drawing upon Western theoretical foundations, is adapted to the national strategic context. This specific approach combines elements of deterrence, traditionally understood, and coercion, and it extends beyond the mere signaling of resolve to use force, encompassing the actual employment of capabilities. In addition to traditional nuclear and conventional forces, the Chinese model incorporates the development of asymmetric capabilities in the cyber and space domains, as well as the use of nontraditional instruments such as economic sanctions and diplomatic measures. These elements together contribute to the formation of an integrated strategic deterrence framework based on the concept of comprehensive national power.

In Chinese sources, information deterrence is broadly identified as one of the components of overall strategic deterrence, while in a narrower sense, cyber (network) deterrence is viewed as a form of military confrontation in cyberspace. Information deterrence encompasses the use of cyber operations alongside other forms of information warfare, such as electronic and psychological operations. Cyber deterrence, more specifically, focuses at the strategic level on preventing large-scale cyberattacks by demonstrating capabilities for conducting and defending against network operations, accompanied by a clear expression of readiness to retaliate, while at the tactical level it seeks to prevent smaller and more frequent cyber threats during peacetime conditions.

Keywords: *deterrence, integrated strategic deterrence, cyberspace, information warfare, cyber deterrence, People's Republic of China*