Article

| 2026 | Vol. 10 | No. 1 | e50620 |

SOCIETY REGISTER

U.S.-China digital rivalry and the struggle to shape the world's next order

Toghrul Seyidbayli[1] ✉

[1] Nakhchivan State University, Azerbaijan (ORCID: 0009-0008-9015-6928)

ABSTRACT: The emerging digital order, shaped primarily by the strategic rivalry between the United States (U.S.) and China, is transforming global power dynamics and producing significant implications for democracy and multilateral governance. This paper explores how competing digital ecosystems, including social media platforms, cloud services, AI pipelines, and critical infrastructures such as 5G networks and semiconductors, generate asymmetric dependencies, confer strategic leverage, and introduce new vulnerabilities for states and societies. It further analyzes the role of nondemocratic actors in advancing alternative norms, particularly in the domain of cyber governance, that challenge democratic principles and weaken multilateral institutions. Through comparative analysis and the introduction of conceptual tools such as operational depth, the governance AI stack, the computing concentration index, and the allocation-intensification gap, the study demonstrates how technological infrastructures are intertwined with political influence, strategic risk, and the erosion of democratic resilience. The findings underscore that safeguarding democracy in the digital era requires not only reinforcing domestic democratic capacities but also establishing multilateral frameworks to mitigate the coercive dimensions of authoritarian digital power.

KEYWORDS: digital geopolitics | democracy | digital governance | AI | multilateralism

INTRODUCTION

In recent years, the growing competition between the United States (U.S.) and China has expanded beyond traditional military and economic rivalry into the realms of digital technologies, cyberspace, and artificial intelligence, reflecting what Slawotsky (2021) terms a new conceptualization of national security as a fusion of ideological, technological, and economic power. Historically, economic capacity has always underpinned military strength. As Kennedy (1987) demonstrates, great powers rise and fall on the basis of their productive and financial foundations. What is new today is that digital infrastructures, platforms, and governance norms have themselves become direct centerpieces of the distribution of power and legitimacy in international relations, rather than merely supporting military capability. The rapid development of generative AI has intensified this competition, with U.S.-based systems such as ChatGPT and Gemini on the one hand, and Chinese alternatives such as DeepSeek on the other, demonstrating not only different technological capabilities but also fundamentally different approaches to government regulation, transparency, and surveillance (Sheehan, 2023;

✉ tseyidbayli@gmail.com

https://doi.org/10.14746/sr.50620

Dohmen, 2024).

The ideological dimension of the U.S.-China rivalry is perhaps nowhere more visible than in competing visions over who will shape the technological future. As President Biden stated, "The future lies in who can, in fact, own the future as it relates to technology, quantum computing, a whole range of things, including the medical fields," adding that "China is out-investing us by a long shot because their plan is to own that future" (CNN, 2021). Also, by referring to the national security documents of prominent international actors, one can also observe their apprehension regarding the rise of China and the erosion of the established Western-oriented international order. For instance, the German strategic security document acknowledges China as a significant player but critiques Beijing's approach, stating: "China is trying in various ways to remould the existing rules-based international order, is asserting a regionally dominant position with ever more vigour, acting time and again counter to our interests and values" (The Federal Government, 2023). Similarly, the Swedish national security document echoes this concern, noting: "China's ambition to become a world leader in new technology and its use of cyber capabilities also have consequences for our security and competitiveness" (Government Offices of Sweden, 2024). This ideological dimension, in which competing visions of digital order reflect deeper clashes between liberal and state-controlled governance models, supports the argument that ideology has become an integral pillar of hegemonic rivalry alongside technology and economics.

The U.S. has generally positioned itself as a champion of an open and interconnected internet, often aligning itself with its democratic allies through initiatives such as the "technocracies" framework and the promotion of regulatory standards that support transparency and competition (Blinken, 2022; Malkin & He, 2024). The global spread of GenAI systems such as ChatGPT demonstrates Washington's soft power in shaping the discourse on innovation, ethics, and digital norms, even as domestic debates reveal contradictions about privacy, surveillance, and corporate centralization. In contrast, China is advancing a model rooted in cyber sovereignty, expanding its Digital Silk Road and exporting surveillance-based governance technologies, including facial recognition systems and Safe City infrastructure to authoritarian governments (Carter & Carter, 2025), and DeepSeek and other state-backed platforms are emblematic of Beijing's ambition to create a parallel digital ecosystem that is low-cost but competitive with high-end brands (West & Allen, 2018; Au & Chen, 2025).

The implications of this competition go beyond bilateral tensions, as multilateral institutions face increasing challenges in adapting to geopolitical issues from the Middle East to East Asia, particularly in the digital arena (Alibabalu, 2025). Cyber governance, AI, and transnational digital corporations expose significant institutional gaps and create space for the dominance of power-driven policies and unilateral actions. Furthermore, the lack of coherent global frameworks for regulating AI deepens the legitimacy crisis in democratic systems, as disinformation, algorithmic manipulation, and digital surveillance continue to erode trust in institutions and polarize societies (Anthony et al., 2024; Radanliyev, 2024). This dynamic suggests that the competition between the U.S. and China is not just about who will dominate digital infrastructure, but also about which normative model, liberal-democratic openness or state-driven digital authoritarianism, will shape the future of multilateralism and democratic governance.

This paper argues that the U.S.-China competition in digital geopolitics represents a continuation of geopolitical competition, reminiscent of the great power competition for access to space in the 1950s and 1960s. By examining the strategic dimensions of this competition, particularly through the lens of AI competition exemplified by ChatGPT and DeepSeek, this study seeks to contribute to ongoing debates about the capacity of multilateral frameworks to address 21st century challenges and the broader implications of digital geopolitics for global governance.

METHODLOGY

This study uses a qualitative, multi-level approach to analyze the digital competition between the U.S. and China and its implications for democracy and global governance. The study combines comparative analysis of digital ecosystems such as social media platforms, AI pipelines, cloud services, and 5G infrastructure; normative and institutional assessments, such as standard-setting, cyber governance, and multilateral engagement; and studies of the Global South to assess alignment, dependency, and democratic impacts. For the accuracy and integrity of the data in this study, works published in reputable reference centers such as the Carnegie Endowment for International Development, GIS, and the International Journal of Political Science were cross-checked and cross-referenced. In addition, the research introduces innovative analytical tools, including operational depth, governance AI stack, computing concentration index, and allocation-escalation gap to measure strategic vulnerabilities, technological dependencies, and escalation risks, linking technical dynamics to political consequences and democratic resilience.

HEGEMONIC STABILITY THEORY

Hegemonic Stability Theory (HST), as articulated by Kindleberger (1973) and others, offers a powerful framework for understanding the U.S.-China rivalry through the lens of international political economy. HST posits that a stable international economic order requires a single hegemon to provide public goods such as open trade regimes and technical standards. After the Second World War, the U.S. provided these goods for the digital domain such as open internet architecture, Western-controlled semiconductor supply chains, and relatively free data flows. China's rise as a technological challenger has created a hegemonic stability gap. The U.S. remains willing but increasingly unable to sustain its digital hegemony alone, while China is able but unwilling to accept the existing U.S.-led order. This gap produces systemic instability, visible in export controls, technology denial, and competing AI governance frameworks.

Kindleberger (1973) emphasized that hegemonic stability requires control over critical "chokepoints." Today, those chokepoints advanced AI chips and cloud infrastructure. For instance, the U.S. has weaponized these chokepoints through export controls, such as semiconductor restrictions (Federal Register, 2022) and the AI Diffusion Framework (Federal Register, 2025). In response, China has banned imports of some sensitive products (The Guardian, 2026). From an HST perspective, this is a declining hegemon attempting to slow the challenger while preserving its role as the indispensable provider of digital order. The U.S. also created an allied bloc, Pax Silica, in late 2025, offering exclusive digital public goods. This institution-building

will is HST's distinctive contribution that hegemony is not just about power but about legitimate leadership and rule-making (Gilpin, 1981).

China's strategy follows Gilpin's (1981) hegemonic transition logic applied to political economy in which rising powers seek to change the monetary rules when those rules no longer serve their interests. Beijing has accelerated the digital Yuan's development, testing it across major cities and integrating it into Belt and Road projects to incentivize partner nations to adopt Chinese payment infrastructure. Crucially, the digital Yuan appeals not only to U.S. adversaries but also to allies resentful of dollar sanctions (Slawotsky, 2022). China has also created alternative geopolitical institutions such as BRICS and Belt and Road Initiative and technical standards for digital sovereignty. HST thus captures that China is not simply accumulating economic power; it is actively constructing a rival hegemonic monetary order with its own public goods, rules, and spheres of influence (Malkin, 2022). The critical question from HST is whether the international system can accommodate two full-stack digital sovereigns, or whether prolonged instability and a cyber-hegemonic war are inevitable.

CONCEPTUALIZING DIGITAL GEOPOLITICS

Throughout history, especially after the Peace of Westphalia in 1648, competition for control over global resources and key infrastructure has been a cornerstone of geopolitical rivalry among great powers. This has intensified especially after the collapse of the Soviet Union in 1991, when a systemic shock has gripped international relations (Alibabalu et al., 2018). During the Cold War, U.S. dominance over global telecommunications and digital infrastructure was solidified through military technological innovations such as ARPANET, the establishment of influential corporations and consortia such as RCA (a pioneer in satellite communication) and Intelsat (a U.S.-led consortium controlling international satellite traffic under U.S. governance), and a neoliberal regulatory framework that reinforced U.S. leadership in setting standards and fostering the rise of its technology giants (Slotten, 2022). Unlike this U.S. model, which relied on public-private partnerships, China's approach remains state-centric, with the Communist Party directing firms such as Huawei and ZTE as instruments of national industrial policy (Atkinson, 2020). However, while American dominance in digital technologies was facilitated by the Cold War and neoliberal globalization, the end of that era did not mean the final triumph of capitalism. More recently, the emergence of China as a powerful technological and economic alternative has significantly reshaped digital geopolitics, creating a strategic environment in a volatile, uncertain, complex, and ambiguous (VUCA) world (Liu & Miao, 2024, pp. 71-72; Alfian et al., 2025).

With the gradual repetition of the historical events of the Cold War and the repolarization of the world, it seems that globalization is not as unstoppable as it was thought, and some even believe that traditional globalization is doomed to destruction (Millon, 2024; Bagir, 2024). In this line, the concept of digital geopolitics has emerged as a central analytical framework for understanding how the distribution of power in international relations is increasingly shaped by technological innovations, particularly in AI, data governance, digital infrastructure, and the regulation of global cyberspace. In contrast to classical geopolitics, which emphasizes territorial control, including competition for resources, and military dominance, digital geopoli-

tics reflects a new frontier of competition in which states compete over the architecture, standards, and infrastructure of the digital environment that underpins global economic systems and national security strategies (Liu & Miao, 2024, p. 69). Therefore, digital geopolitics reveals how economic competition has become increasingly mediated by digital infrastructures.

Because the HST emphasizes rule-making as the hegemon's primary prerogative, it offers a relevant framework for understanding digital geopolitics. Kindleberger (1973) argued that stability requires not just a dominant power but one willing to bear the costs of providing public goods. In the digital domain, the U.S. has historically provided goods such as open internet standards and neutral data flows, but China's rise has created a dilemma of hegemonic transition. Meanwhile, the U.S. can no longer provide unilaterally, and the challenger offers a rival set of digital public goods rooted in cyber sovereignty and state-controlled platforms. Unlike previous transitions (for example, from British to American hegemony after the First World War), which unfolded over decades, the digital transition is compressed because control over data, algorithms, and computing infrastructure confers immediate structural power. Hegemonic stability theory thus explains why the U.S. has shifted from promoting open markets to building exclusionary blocs such as Pax Silica. This is a defensive move by a declining hegemon to preserve rule-making authority in a domain where losing standard-setting power means losing geopolitical influence.

Moreover, digital technologies have become tools for projecting power, shaping alliances, dependencies, and spheres of influence. States no longer compete simply for military bases or natural resources, but increasingly for the adoption of their digital platforms, standards, and infrastructures by third countries (Liu & Miao, 2024, p. 69). In this sense, control over digital ecosystems, from AI models like ChatGPT and virtual networking platforms like Facebook, Instagram, and YouTube to Chinese competitors like DeepSeek and TikTok, demonstrates not only technological superiority but also geopolitical leverage. The ability to determine the rules, norms, and infrastructures of the digital realm thus means determining who will lead and who will follow in the future structure of international power.

The emerging digital order, while witnessing a growing number of important actors, is increasingly shaped around the rivalry between the U.S. and China, which, with massive investments in digital infrastructure in line with geopolitical rivalries over technological standards, infrastructure, and digital governance models, are fiercely competing, transforming their competition not only into a struggle for economic and technological supremacy, but also for the normative and institutional direction of the digital future.

TECHNOLOGICAL INFRASTRUCTURES AND COMPETING ECOSYSTEMS

The strategic competition between the U.S. and China in the digital domain is not limited to advances in AI, quantum computing, or semiconductors; it extends to broader areas of technological infrastructure that increasingly serve as essential pillars of economic modernization, national security, and international influence. Over time, the U.S.' dominance has stemmed from its unparalleled innovation ecosystem in Silicon Valley, where public research funding and private venture capital have converged to create global dominant companies in cloud computing, semiconductors, and digital platforms. Companies such as Microsoft, Amazon, Goo-

gle, and Nvidia not only shape civilian markets but also support U.S. defense modernization strategies through dual-use technologies, thereby reinforcing the entanglement of commercial innovation and geopolitical power. The U.S.' enduring dominance of chip manufacturing and design ensures it controls bottlenecks in the global digital economy, and thus uses this as leverage against allies and competitors (Scharre, 2023; Edelman et al., 2025; Villasenor, 2025).

In contrast, China has sought to create independent, parallel infrastructure that can both wrest digital power centers from American control and extend its influence outward. The Digital Silk Road, an extension of the Belt and Road Initiative, is a symbol of this strategy, which includes investments in undersea cables, 5G networks, satellite constellations, and data centers across Africa, Southeast Asia, and the Middle East. Huawei's central role in building global 5G architectures has made telecommunications infrastructure a key arena of geopolitical competition, while Beijing's support for state-backed companies like Alibaba Cloud, Tencent, and Baidu demonstrates its strong resolve to challenge U.S. dominance of cloud and platform ecosystems. The emergence of DeepSeek, as a state-backed AI initiative, demonstrates Beijing's determination to cultivate large, autonomous models that can compete with systems developed by the U.S., proving that AI is not simply an industrial competition, but an area in which control over the production and dissemination of new knowledge is a matter of geopolitical competition (He, 2022).

The geopolitics of this competition is best captured in the concept of infrastructure dependency and the dependency of other actors. For infrastructure is not simply a neutral conduit for international communication; it embeds power relations, shapes technological standards, and thus creates conditions for long-term dependence or independence from foreign powers. Actors that rely on U.S.-led infrastructure are vulnerable to Washington's capacity to regulate, sanction, or restrict access. The U.S. ban on the export of advanced chips to China and its pressure on allies such as the Netherlands and Japan to restrict technology transfers illustrate how infrastructure dominance can be used as a coercive geopolitical tool (Bridges, 2024, pp. 1640-42; Zúñiga et al., 2024). Needless to say, this vulnerability would also apply to China's allies and partners if China were to succeed as the hegemon in the long run. However, while states that integrate into China's Digital Silk Road may secure access to relatively affordable technologies and infrastructure financing, such benefits are often accompanied by exposure to Beijing's political conditionalities, regulatory frameworks, and cybersecurity protocols, which, over the long term, may constrain democratic practices and erode political freedoms (Cheney, 2019).

A more comprehensive link between security, technology, and ideology is necessary to understand the full scope of U.S.-China digital rivalry. This requires moving beyond general digital infrastructures to examine specific technological factors such as Central Bank Digital Currencies (CBDCs). The digital Yuan, as the first major economy's CBDC, exemplifies how economic, technological, and ideological power levers converge. On security, a successful cross-border digital Yuan could erode U.S. financial sanctions, what former U.S. Treasury Secretary Mnuchin called a "replacement for war" by enabling peer-to-peer wallet transactions that bypass the U.S.-dominated SWIFT system and dollar-based financial networks. This directly undermines a core instrument of U.S. national security statecraft. Economically, a successful cross-border digital Yuan could erode U.S. dollar hegemony and the effectiveness of U.S. financial sanctions in the long term. Technologically, China's early mover advantage positions it

to set global CBDC standards and harvest unprecedented amounts of real-time data to fuel AI development. Ideologically, the digital Yuan embeds a vision of state-controlled, programmable money compatible with social credit systems which directly challenges the Western liberal model of privacy and market autonomy. Thus, CBDCs are not merely a financial innovation but a strategic instrument through which China seeks to restructure global governance networks in its favor, building its supremacy over the market (Slawotsky, 2022).

The GENIUS Act represents the U.S. response to China's digital Yuan, but it adopts a fundamentally different approach, using private-sector stablecoins rather than a state-issued CBDC (U.S. Department of the Treasury, 2026). The prohibition on paying interest on stablecoins creates a competitive disadvantage compared to China's interest-bearing digital Yuan. This situation could undermine the dollar's digital extension, as global users may prefer a state-backed, interest-bearing currency over a non-interest-bearing private alternative. Thus, it seems that the GENIUS Act does not neutralize China's challenge; it may inadvertently reinforce it.

In late 2025, an initiative called Pax Silica emerged as a U.S.-led economic security coalition to secure trusted supply chains for AI and advanced computing. The initiative brings together allied and partner nations to cooperate across the full technology stack with the goal of reducing coercive dependencies and building a durable economic order for the AI age (Ray, 2026). From a hegemonic stability perspective, Pax Silica represents the U.S. as a declining yet still dominant hegemon, attempting to provide exclusive digital public goods to its allies while slowing China's technological ascent.

What is emerging, then, is a multipolar yet bifurcated global digital order, in which infrastructures function not merely as enabling technologies but also as markers of aligned or opposing geopolitical forces. The struggle is less over technological innovations in isolation and more over the capacity to define the system architectures upon which others depend. The U.S. seeks to maintain an open, market-driven order rooted in its technological superiority, while China aspires to institutionalize a state-driven, sovereignty-driven model in which infrastructure functions as an instrument of political control and China-centric geopolitical planning (Bradford, 2023b). Consequently, the rivalry over technological ecosystems is not only a contest for economic and strategic primacy but also a struggle over the political values and institutional logics that will govern digital societies in the decades ahead.

SOCIAL MEDIA PLATFORMS AND THE CONTEST FOR INFLUENCE

The competition between the U.S. and China in the realm of digital geopolitics is most visible in the competition between American social media platforms such as Instagram, YouTube, and WhatsApp and their Chinese counterparts, notably TikTok, WeChat, and Weibo. While the former emerged from a largely market- and innovation-driven environment in Silicon Valley, the latter were nurtured within a state framework designed to serve China's commercial and broader strategic goals. This divergence at its roots has translated into fundamentally different approaches to data management, content moderation, and platform accountability, thereby embedding geopolitical logics into the everyday digital practices of billions of users worldwide (Finkelstein et al., 2024).

American platforms, due to their first-mover advantage and global reach, have played a signif-

icant role in disseminating the U.S. cultural ideas, consumption practices, and political values. YouTube has served not only as a hub for entertainment and education, but also as a platform for political mobilization and transnational activism, exemplified in events such as the Arab Spring, where digital platforms served as vital tools for popular organizing. Similarly, WhatsApp has become a hub for interpersonal communication and information dissemination across the global South, cementing the U.S. dominance in digital connectivity. Instagram, through its emphasis on visual culture, has reinforced Western consumerism and lifestyle trends while providing a vehicle for social activism. Collectively, these platforms have expanded access to U.S. and Western soft power and maintained a normative order that emphasizes freedom of expression, although this freedom is also contested in the West.

In contrast, Chinese platforms have attracted attention by leveraging Beijing's government-backed industrial policy and exploiting domestic protectionism and international expansion strategies. TikTok, in particular, has disrupted the global social media ecosystem by introducing new algorithmic architectures that emphasize viral content and user engagement in unprecedented ways. This innovation has not only challenged the dominance of the U.S. platforms but has also raised concerns in Washington and European capitals about data security, user surveillance, and potential manipulation of political discourse (Kokas, 2023).

TikTok was identified by the U.S. government as a national security threat, prompting legal challenges in both state and federal courts. Ultimately, a compromise was reached that required a change in the ownership structure to transfer partial control to U.S.-based entities. WeChat, while less globalized than TikTok, represents the integration of social media with financial services, e-commerce, and governance tools, thereby offering a model of digital governance that contrasts sharply with the fragmented, corporate-driven nature of the U.S. ecosystem (Ying, 2020). In this sense, Chinese platforms embody a different vision of digital modernity in which the boundaries between social interaction, state authority, and market activity are intentionally blurred.

The geopolitical implications of this competition extend beyond cultural influence to questions of systemic governance. While American platforms are often criticized for amplifying misinformation and fostering political polarization, Chinese platforms raise specific concerns about the lack of regulatory norms and the restriction of digital freedoms (Backer, 2018). The rapid rise of TikTok has shown that China can successfully compete with Silicon Valley in shaping global cultural flows, challenging long-held assumptions about U.S. technological hegemony. Looking ahead, the competition between these ecosystems is likely to create a bifurcated digital order in which states and societies increasingly align with one model or the other. For liberal democracies, the consolidation of Chinese platforms could undermine the resilience of open information environments, while for authoritarian regimes they may provide ready-made tools for social control and political legitimacy (Bradford, 2023a).

From this perspective, the competition between American and Chinese social media is not simply a commercial one, but a central dimension of digital geopolitics. It reflects a struggle over who sets the rules of digital interaction, whose values underpin the architecture of global communications, and ultimately, which vision of social and political order will prevail in the 21st century.

NORMS, STANDARDS, AND THE GLOBAL DIGITAL ORDER

The digital struggle between the U.S. and China is not limited to the realm of technological infrastructure or platform competition, but has also extended to the normative and institutional arenas, where global standards for the governance of cyberspace, data flows, and AI are being negotiated. The U.S. has long promoted open, interoperable, and market-driven standards, and has supported institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and multi-stakeholder forums such as the Internet Governance Forum (IGF) as tools to maintain its position in a decentralized digital order. In contrast, China has increasingly pursued an alternative approach through platforms such as the International Telecommunication Union (ITU), where it has sought to institutionalize the concept of "cyber sovereignty" and normalize the idea that each country should exercise independent control over its own digital sphere, including data storage, network security, and algorithmic regulation (Qiao-Franco, 2024; Negro, 2019).

What makes this competition particularly important is the way in which norms and standards will simultaneously shape the future trajectories of innovation and political control. Behind the curtain of technical standards lie geopolitical objectives as they encode assumptions about authority, accountability, and access, thereby embedding particular governance models in the architecture of global networks. The U.S. and its allies aim to establish a liberal digital economy by insisting on open data flows and market competition, while China's state-centric design demonstrates its interest in consolidating control-centricity, enabling censorship, and exporting a controlled model of technology-based governance. Thus, the competition is not just about who builds the network, but also about which values are transmitted through it, and, as a result, this interplay makes the digital sphere a key site for ideological and geopolitical confrontation (Chen & Gao, 2024; Bradford, 2023a).

Looking back over the past two decades, and consistent with hegemonic stability theory, the global rivalry over norms and standards in the digital area is likely to have enduring consequences for international politics, as it will embed competing conceptions of sovereignty, authority, and governance within the infrastructures of everyday life (Gilpin, 1981). Should U.S. norms prevail, the global order may evolve toward an open and liberal model of digital globalization; if Chinese norms dominate, the outcome could be a hierarchical environment of nationalized cyberspaces under more extensive state control (Kwet, 2019). Yet the more plausible trajectory points toward a multipolar digital order, in which the U.S., China, East Asian countries like South Korea and Singapore, and Europe each assert their own standards. A totalitarian model, however, would endanger human-centered and democratic values, particularly within targeted societies, thereby necessitating more rigorous international rule-making.

GEOPOLITICAL IMPLICATIONS FOR THIRD COUNTRIES

The growing competition between the U.S. and China in the technological and digital spheres has placed third countries in a precarious and strategically important position. For many of these countries, especially small and medium-sized powers, this competition manifests itself not as an abstract competition between two great powers but as a practical dilemma that directly affects their economic strategies, security postures, and domestic governance models.

The provision of digital infrastructure, whether through U.S.-backed private-sector companies or Chinese state initiatives such as the Digital Silk Road, while offering opportunities for connectivity and modernization, also imposes long-term dependencies that have jeopardized the trajectory of national sovereignty. Thus, choosing between U.S. or Chinese systems often means importing not only technology but also the underlying normative frameworks governing public surveillance, data protection, and free or unfree flows of information (Dohmen, 2024; China in 5, 2025).

In regions such as Africa, Southeast Asia, and Latin America, the impact of this competition is particularly pronounced. State-invested or state-influenced technology companies, with China's model characterized by direct state control (e.g., Huawei, ZTE) and the U.S. increasingly using strategic equity stakes (e.g., the government's 10% ownership of Intel) to secure national security supply chains (Benzinga, 2025). While these investments address critical gaps, they also entrench technological standards and generate asymmetric dependencies that extend beyond the digital sphere into broader political alignments. Integration into foreign digital ecosystems further binds states to external regulatory and security frameworks and fosters what has been described as digital imperialism (Kwet, 2019).

One important but less studied consequence of this competition is the fragmentation of global governance among third countries. Some of them adopt a protectionist strategy, simultaneously engaging with the U.S. and Chinese technologies to diversify dependencies and maximize benefits. This creates a multi-layered digital ecosystem within their borders, where Chinese-made hardware coexists with Western software and governance frameworks, creating hybrid forms of digital governance that demonstrate pragmatic compatibility. However, such hybridity carries risks, including interoperability challenges, increased vulnerability to cyber conflict, and the possibility of being caught in punitive measures, such as sanctions or technology bans, imposed by one side against the other. In this sense, competition reduces the strategic autonomy of smaller countries and exposes their domestic policies to increasing external pressures (Rolf & Schindler, 2023).

Looking ahead, geopolitical implications for third countries are likely to crystallize around issues of alignment and agency, where the growing influence of nondemocratic actors, driven by the spread of surveillance-based digital infrastructures and restrictive regulatory models, further complicates their strategic calculations. For some, Chinese-backed platforms and technologies may serve as a building block for rapid modernization, even if such adoption comes at the cost of increased state surveillance, reduced transparency, and deeper engagement with authoritarian practices that can erode democratic resilience. For others, integration into Western-led systems may strengthen liberal institutional frameworks but simultaneously limit policy flexibility in areas such as data localization, platform governance, or cybersecurity regulation. However, the broader trend points to a world in which third countries play a significant role in shaping the balance of power, as their collective choices determine which standards and norms gain global legitimacy. In this sense, their strategic agency, although often limited, emerges as a determining factor in the competition over the future digital order, making them both objects and subjects of great power competition and exposing them to the structural consequences of undemocratic influence in global politics (Anderson & Raine, 2020; Mantelassi, 2024; Dohmen, 2024; Bradford, 2023a).

SECURITY DIMENSIONS OF DIGITAL RIVALRY

The security risks of U.S.-China competition are now a complex issue for statecraft, as digital systems constitute both the stage and the ammunition of contemporary geopolitical affairs. Control of networks, data, and computations brings not only economic advantage but also leverage and asymmetric military advantage. The literature on arms interdependence shows how control over sensitive equipment such as spy satellites and secure ground control networks, communication infrastructure networks, and the continuity of their supply chains in times of crisis can translate into political coercion and even major defeat. The same logic applies in the digital realm, where access to cloud infrastructure, platform APIs, and semiconductors can be used as strategic tools of state policy. At the same time, the rapid spread of powerful AI and automation tools has expanded the attack surface and transformed the computation of espionage and disruption, as machine learning techniques can enhance both surveillance capabilities and the effectiveness of infiltration operations. Thus, infrastructure hotspots and the enhancement of AI by great powers have created a security environment in which technological advantage has been directly translated into diplomatic and military options (Allen, 2023, pp. 5-8; Zhang, 2020).

Cybersecurity and state espionage have evolved from occasional intrusions to ongoing tools of strategic competition. High-value supply chain intrusions and breaches complement national security in two ways. The first is the collection of strategic information that has long-term political and operational value and can effectively change adversary behavior when necessary. The second is the destructive operations that can undermine and disrupt the adversary's decision-making in times of crisis and war. The operational logic of these campaigns is to target data in depth, not just to destroy or disrupt temporarily. This shift forces third-party infrastructure to be beholden to vendor ecosystem security commitments (GSIS, 2025). To be safe, an adversary does not need to own the target data centers if it can compromise a trusted supplier or a global software package. These features have exacerbated the problem of cybersecurity governance.

AI is increasingly woven into military strategy, not just by powering drones or autonomous weapons, but also by shaping how governments gather intelligence, plan operations, and manage logistics. Unlike traditional weapons, AI systems process vast amounts of data to predict, make decisions, and act faster than humans, giving countries that control them a strategic advantage in warfare and deterrence. However, this advantage comes with political risks when the technology is not local, as reliance on foreign AI technologies or cloud services can leave militaries vulnerable to external pressure, while the inability to clearly attribute cyberattacks or AI-based intelligence creates new areas of uncertainty where they may escalate without an outright declaration of war. In this sense, AI in the military does not simply add new tools to the battlefield; Rather, it is changing the speed, secrecy, and unpredictability of global power competition (Harrel, 2025).

Data has become the 21st century's equivalent of oil because it fuels economies, enables innovation, and supports national security, but it also creates new forms of dependency and vulnerability. Countries that control the flow of data through platforms, cloud infrastructure, or digital standards can thus turn that dominance into political leverage, shaping how others

communicate, trade, and even plan their military. At the same time, the concentration of sensitive data in foreign-owned systems exposes societies to surveillance, manipulation, and coercion, making the struggle over data sovereignty as important as the geopolitics of oil, which was once strategically significant (Zuboff, 2018; Gao, 2023; Chaisse, 2023).

The security implications of digital competition extend beyond military AI to the intelligence-gathering capacities of civilian technologies such as electric vehicles (EVs) and smartphones. Both EV fleets and personal devices generate granular, real-time data on infrastructure, supply chains, and individual behavior, information that can be harvested by state actors through corporate partnerships or legal mandates (Battista & Cervi, 2025). As Baranowski (2022) argues, data-driven technologies have introduced new forms of information asymmetry that privilege those who control access to these flows. This asymmetry is deepened by what Baranowski (2025) terms the "database construction of reality," where social life becomes increasingly mediated by unevenly controlled digital infrastructures. Thus, every connected device functions as a potential sensor in a broader intelligence architecture, making the digital geopolitical rivalry far broader than military AI alone.

DEMOCRACY UNDER DIGITALISM AND AUTHORITARIANISM

The rise of digital geopolitics has significantly expanded the reach of nondemocratic actors in the international system, not only by exploiting their material capacities in cyber operations, surveillance technologies, and AI, but also by articulating normative and institutional alternatives that are gradually eroding the liberal foundations on which post-Cold War multilateralism was built. Authoritarian powers have increasingly recognized that the infrastructural backbone of the digital order, including standards-setting, cloud architecture, undersea cables, and supply chain interdependencies, can be used as a means to extend political authority beyond national borders, thereby transforming interdependence from a source of cooperation into a mechanism of coercion. This reshaping of digital infrastructures into tools for geopolitical leverage undermines democratic states' ability to globalize the principles of transparency, accountability, and open access, while simultaneously strengthening the international presence of regimes that have historically operated on the margins of global norm-setting (Mantelassi, 2024).

In this context, the influence of non-democratic actors cannot be reduced to isolated cyber intrusions or espionage incidents, but must be understood as part of a sustained strategy to redefine governance in digital terms, prioritizing models of centralized control, state surveillance, and normative separation from liberal institutional frameworks. The doctrine of "cyber sovereignty," prominently promoted by China but increasingly echoed in the practices of Russia, Iran, and allied states, seeks to redefine digital governance as an extension of territorial authority, thereby legitimizing censorship, surveillance, and selective connectivity while simultaneously challenging the universality of the open internet model. By promoting these frameworks in international fora such as the International Telecommunication Union (ITU) and through initiatives such as China's Digital Silk Road, authoritarian actors embed alternative governance logics within multilateral structures, creating a dual process in which they both challenge existing rules and actively shape new institutional arrangements that reflect

their political interests (Farrand et al., 2024).

The challenges to multilateralism in this context are both structural and normative. Structurally, existing multilateral institutions lack the judicial transparency, technical capacity, and political coherence to regulate the increasing militarization and politicization of digital infrastructure. Normatively, the assumed universality of liberal digital values such as openness, interoperability, and cross-border data flows is increasingly rejected by states that frame norms such as Western impositions, thereby legitimizing divergent approaches to governance that divide the digital realm into competing spheres of influence. This division not only hinders collective responses to common threats such as cybercrime, disinformation, and attacks on critical infrastructure, but also accelerates the erosion of trust between states as digital competition exacerbates security dilemmas and encourages technological disintegration (Garcia, 2022; Mantelassi, 2024).

In this sense, digital competition has become not only a contest for technological supremacy, but also a profound challenge to the survival of multilateralism as a mode of global governance. The proliferation of technological blocs, the emergence of bilateral agreements between authoritarian and hybrid regimes on issues such as the deployment of 5G and the ethics of AI, and the inability of existing institutions to enforce accountability in cases of cyber aggression underscore the extent to which digital geopolitics destabilizes the assumption of inclusive, rule-based cooperation. Consequently, the study of digital security competition directly responds to the call for papers by showing how the dominance of nondemocratic actors in the digital sphere reshapes the asymmetry of power in global politics and how this in turn poses unprecedented obstacles to multilateralism, which now faces not only the classic problems of governance and collective action, but also the latent politicization of the technological infrastructures on which the 21st century order increasingly depends.

Dimension	the U.S.	China	Geopolitical/Democratic Implications
Social Media Platforms	Instagram, YouTube, WhatsApp	TikTok, WeChat, DeepSeek	Platforms influence global communication norms and can shape public opinion, information flows, and political discourse in other countries.
AI & Strategic Technologies	AI research, cloud AI services, semiconductor leadership	DeepSeek, state-backed AI, military-civil fusion	Control and deployment of AI technologies affect strategic capabilities, digital dependencies, and national policy flexibility.
Infrastructure & Networks	5G, cloud services, semiconductor supply chains	Digital Silk Road, Huawei 5G, domestic chips	Deployment of digital infrastructure creates interdependence, influencing political alignment, security, and economic strategy in third countries.
Norms & Governance Models	Open Internet frameworks, standards-setting, privacy protocols	Cyber sovereignty, centralized regulation, state-guided digital governance	Competing governance models shape multilateral negotiations, regulatory frameworks, and the global digital order.
Third-Country Influence	Participation in global digital markets and standards	Export of digital infrastructure and platforms	Third countries' choices in aligning with digital ecosystems affect domestic policy, international partnerships, and exposure to external influence.

Tab. 1. Comparative overview of U.S. and Chinese digital ecosystems and their geopolitical implications
Source: Author's own elaboration

In the age of digital geopolitics, democracy has become both a target and a stress test, as non-democratic actors increasingly exploit cyber tools, AI, and data flow control to undermine democratic institutions abroad through electoral interference, disinformation campaigns, and manipulation of public trust, while simultaneously shielding themselves from counter-pressure at home. This asymmetric vulnerability not only exposes the fragility of democratic systems but also complicates multilateral regulation, as democracies tend to support open and pluralistic digital spaces while authoritarian regimes pursue sovereign and security approaches, thereby creating a structural conflict that erodes prospects for inclusive governance and underscores the growing democratic deficit in global digital politics (Shahbaz, 2018).

SUGGESTIONS

To provide fresh thinking on the digital competition debate, four concepts can be proposed that shed more light on the security risks for politics and international relations in the second cold war. First, operational depth refers to the extent to which a country depends on foreign-made digital systems for its most sensitive tasks, such as national security, energy supply, or banking. The deeper this dependence, the greater the political pressure a foreign power can exert. A country's critical functions, such as defense and industrial capacities, health and food sectors, and data centers that rely heavily on foreign digital systems, create significant vulnerability to foreign pressure or disruption. This dependence can escalate into a severe national security threat during international crises. Second, the idea of an autonomous AI stack, such as chips, data, or real-world deployment methods, emphasizes that control over AI does not just mean owning the smart software, but also owning the entire chain, from computer chips and data to the methods of deploying algorithms in society. Losing control at any stage gives foreign actors disproportionate influence (Schindler et al., 2024; Egan, 2025).

Third, the Computing Concentration Index (CCI) measures the extent to which a country's digital power, such as cloud services or large data centers, depends on a handful of foreign suppliers. A high CCI means more exposure and less room for political autonomy. This encourages states to test limits. For example, a nation might launch a ransomware-like strike on a rival's port logistics, watch the economic chaos unfold, and deny involvement while offering help to restore systems. Finally, the allocation-intensification gap encompasses a dangerous gray area where cyberattacks such as power outages, data breaches, or financial paralysis are visible, but it is not clear who is behind them, encouraging states to engage in covert pressure and escalation without overt engagement. These concepts are not abstract and can be tracked, scored, and compared across countries, helping us to see how technological dependence can easily translate into political vulnerability. In this sense, they illustrate how today's digital tools are transforming interdependence into a new form of power politics (Farrell & Newman, 2019; Allen, 2023).

The policy implications flow directly from this recognition of security. First, alliances must move beyond declarative statements and invest in substantial diversification. Third countries, in particular, must coordinate in digital domains. Second, export controls must be accompanied by resilience investments such as subsidizing alternative supply chains, strengthening domestic capacities, and open, reliable models to avoid the creation of permanent technology

deserts in third countries. Third, a new diplomacy of attribution and restraint is needed, and to this end, international norms and rapid multilateral attribution mechanisms must be developed to reduce gaps and make coercive cyber operations more costly and less ambiguous. Finally, as AI accelerates both offense and defense, arms control thinking must be updated to include computation, datasets, and model-sharing regimes as elements of strategic stability, not just sensors or weapons. Similar examples include export control regimes retooled to consider model architectures and training datasets as dual-use goods. Implementing these steps would require public-private partnerships, specific measurement tools, and targeted assistance to third countries to manage their operational depth.

CONCLUSION

Analysis of digital competition has shown that the rise of cybersecurity threats, the militarization of AI, and data-driven strategic competition are not just technological shifts but a profound political transformation with direct implications for democracy and the future of multilateral governance. Nondemocratic actors are increasingly using digital tools for influence and coercion, enabling them to intervene in democratic processes abroad while consolidating control domestically, creating a double asymmetry in which democratic states are more vulnerable to digital interference due to their openness, while authoritarian regimes thrive in digital ecosystems with tight surveillance and security. This dynamic is fueling the erosion of trust in democratic institutions, exacerbating polarization, and challenging democracies' capacity to maintain legitimacy in an age when information is weaponized.

From the perspective of Hegemonic Stability Theory, the digital rivalry between the U.S. and China represents a classic transition dilemma as the declining hegemon can no longer unilaterally provide global digital public goods, while the challenger offers a rival set of rules rooted in cyber sovereignty. Unlike previous transitions, the digital domain is compressed in time because control over data and algorithms confers immediate structural power. This gives rise to a democratic asymmetry dilemma: democratic hegemons face domestic constraints on surveillance and industrial policy that authoritarian challengers do not, making it harder for democracies to compete without undermining their own values.

At the same time, the contestation over digital governance highlights a deeper divide in the global order. Democracies tend to champion open networks, transparency, and rights-based frameworks for data and AI, whereas authoritarian states advance sovereignty-based models that privilege control, censorship, and state primacy. The inability to reconcile these competing paradigms risks producing fragmented digital spheres in which multilateralism is increasingly constrained by ideological divides. Moreover, the technical chokepoints of digital power, compute capacity, supply chains, and platform governance are weaponized in ways that privilege nondemocratic actors who can pursue coercive strategies without domestic accountability, thereby intensifying the democratic deficit in international digital politics.

Ultimately, the struggle over digital power is also a struggle over the future of democracy itself. If democratic states fail to develop collective mechanisms to protect electoral integrity, regulate AI, and ensure the security of critical data infrastructure, they risk ceding both technological

and normative leadership to nondemocratic actors. Multilateralism, in this context, requires rethinking not only institutional cooperation but also how to embed democratic resilience into digital governance frameworks. Thus, safeguarding democracy in the digital age demands a dual strategy: reinforcing internal democratic robustness against digital interference, and simultaneously advancing multilateral initiatives that prevent authoritarian states from setting the rules of global digital order. Only by bridging the gap between technological competition and democratic values can the international system hope to navigate the new security dilemmas of digital geopolitics.

FUNDING: This research received no external funding.
CONFLICT OF INTEREST: The authors declare no conflict of interest.

REFERENCES

Alfian, M. F., Hudaya, M., Anggraheni, P., & Zuliyan, M. A. (2025). Technology As An Instrument in Great Power Politics: An Overview of the US-China Tech War. Dinamika Global: Jurnal Ilmu Hubungan Internasional, 10(1), 73-99.

Alibabalu, S. S. (2025). India–Middle East—Europe Economic Corridor. In Ismail Ermağan (Ed.), Geopolitical Perspective on South Asia (29-38). Istanbul: South Asia Strategic Research Center (GASAM).

Alibabalu, S. S., Terkulova, R., & Sadri, B. (2018). The Middle East Security from Lockean System to Hobbesian Conflicts. 5. International Student Congress, 79-83.

Allen, G. C. (2023). China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes. CSIS. Retrieved from https://www.csis.org/analysis/chinas-pursuit-defense-technologies-implications-us-and-multilateral-export-control-and

Anderson, J. & Raine, L. (2020). Many Tech Experts Say Digital Disruption Will Hurt Democracy. Pew Research Center. Retrieved from https://www.pewresearch.org/internet/2020/02/21/many-tech-experts-say-digital-disruption-will-hurt-democracy/

Anthony, A., Sharma, L., & Noor, E. (2024). Advancing a more global agenda for trustworthy artificial intelligence. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/research/2024/04/advancing-a-more-global-agenda-for-trustworthy-artificial-intelligence?lang=en

Atkinson, R. D. (2020). How China's mercantilist policies have undermined global innovation in the telecom equipment industry. Information Technology and Innovation Foundation, June. 1-37. Retrieved from https://itif.org/publications/2020/06/22/how-chinas-mercantilist-policies-have-undermined-global-innovation-telecom/

Au, A. & Chen, F. F. (2025). China expands AI globally through the Digital Silk Road. East Asia Forum. Retrieved from https://eastasiaforum.org/2025/04/11/china-expands-ai-globally-through-the-digital-silk-road/

Backer, L. C. (2018). Next generation law: Data-driven governance and accountability-based regulatory systems in the West, and social credit regimes in China. Southern California Interdisciplinary Law Journal, 28, 123-172.

Bagir, M. (2024). Globalization's Challenge to Nation-State Sovereignty and Conflicts in the Middle East. Nous Academy Journal, 3, 66-80.

Baranowski, M. (2022). Radicalising Cultures of Uneven Data-Driven Political Communication. Knowledge Cultures, 10(2), 145-155.

Baranowski, M. (2025). The database construction of reality in the age of AI: the coming revolution in sociology? AI & Society, 40, 1125-1127.

Battista, D. & Cervi, L. (2025). Digital politics in transition and the new logics of fluid visibility on social media: The Ocasio-Cortez case. Society Register, 9(4), 25-42.

Benzinga. (2025, October 8). Trump administration now holds stakes in 5 public companies: Here's a list—INTC, MP, LAC and more. Retrieved from https://www.benzinga.com/markets/equities/25/10/48061018/trump-administration-now-holds-stakes-in-5-public-companies-heres-a-list-intc-mp-lac-and-more

Blinken, A. J. (2022). The Administration's approach to the People's Republic of China. U.S. Department of State. Retrieved from https://2021-2025.state.gov/the-administrations-approach-to-the-peoples-republic-of-china

Bradford, A. (2023a). Digital Empires: The Global Battle to Regulate Technology. Oxford University Press.

Bradford, A. (2023b). The battle for the soul of the digital economy – An interview with Anu Bradford on digital empires. Retrieved from https://geopolitique.eu/en/2023/12/17/the-battle-for-the-soul-of-the-digital-economy-an-interview-with-anu-bradford-on-digital-empires/

Bridges, M. (2024). Infrastructure Is Remaking Geopolitics: How Power Flows from the Systems That Connect the World. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/united-states/infrastructure-remaking-geopolitics

Carter, B. & Carter, P. (2025). Exporting the tools of dictatorship: The politics of China's technology transfers. Perspectives on Politics, 23(3), 1089-1108.

Chaisse J. (2023). 'The Black Pit:' Power and Pitfalls of Digital FDI and Cross-Border Data Flows. World Trade Review, 22(1), 73-89.

Chen, X. & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? International Affairs, 100(6), 2419-2440.

Cheney, C. (2019). China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. Council on Foreign Relations. Retrieved from https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political-illiberalism

China in 5. (2025). Understanding China, five minutes at a time. Retrieved from https://chinain5.com/2025/08/12/the-ai-race-china-vs-us

CNN. (2021). Biden says US faces battle to 'prove democracy works.' Retrieved from https://www.cnn.com/2021/03/25/politics/biden-autocracies-versus-democracies

Dohmen, H. (2024). Assessing US-China tech competition in the Global South. Atlantic Council. Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/assessing-us-china-tech-competition-in-the-global-south/

Edelman, R.D., Fu, D., Hass, R., Kim, P.M., Lin, Y., Ma, Y., O'Hanlon, M.E., Sisson, M.W., Tabassi, E., & Turner Lee, N. (2025). How will AI influence US-China relations in the next 5 years? Brookings Institution. Retrieved from https://www.brookings.edu/articles/how-will-ai-influence-us-china-relations-in-the-next-5-years/

Egan, J. (2025). Global Compute and National Security. Retrieved from https://www.cnas.org/publications/reports/global-compute-and-national-security

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: security, economy and sovereignty. International Affairs, 100(6), 2379-2397.

Farrell, H. & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. International Security, 44(1): 42-79.

Federal Register. (2025). Framework for artificial intelligence diffusion. Retrieved from https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion

Federal Register. (2022). Implementation of additional export controls: Certain advanced computing and semiconductor manufacturing items; supercomputer and semiconductor end use; entity list modification. Retrieved from https://www.federalregister.gov/documents/2022/10/13/2022-21658/implementation-of-additional-export-controls-certain-advanced-computing-and-semiconductor

Finkelstein, J., Jussim, L., Farmer, K., Goldenberg, A., Zucker, J., Finkelstein, D., & Yanovsky, S. (2024). The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States. Intelligence Report. Network Contagion Research Institute.

Gao, R. Y. (2023). A battle of the Big Three?—Competing conceptualizations of personal data shaping transnational data flows. Chinese Journal of International Law, 22(4), 707-787.

Garcia, E. V. (2022). Multilateralism and Artificial Intelligence: What Role for the United Nations? In M. Tinnirello (Ed.), The Global Politics of Artificial Intelligence (pp. 57-84). Chapman and Hall/CRC.

Gilpin, R. (1981). War and change in world politics. Cambridge University Press.

Government Offices of Sweden. (2024). National security strategy. Retrieved from https://www.government.se/globalassets/government/national-security-strategy.pdf

GSIS. (2025). Significant Cyber Incidents. Retrieved from https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Harrel, P. (2025). Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology. Carnegie Endowment for International Peace. Retrieved

from https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en

He, A. (2022). The Digital Silk Road and China's influence on standard setting, CIGI Paper No. 264, Centre for International Governance Innovation.

Kennedy, P. (1987). The rise and fall of the great powers: Economic change and military conflict from 1500 to 2000. Random House.

Kindleberger, C. P. (1973). The world in depression, 1929-1939. University of California Press.

Kokas, A. (2023). Trafficking Data: How China Is Winning the Battle for Digital Sovereignty. Oxford University Press.

Kwet, M. (2019). Digital colonialism: US Empire and the new imperialism in the Global South. Race & Class, 60(4), 3-26.

Liu, H. & Miao, C. (2024). Digital geopolitics in a VUCA world: China encounters a new global order. Global Policy, 15(S6), 67-83.

Malkin, A. (2022). The made in China challenge to US structural power: Industrial policy, intellectual property and multinational corporations. Review of International Political Economy, 27(3), 538-561.

Malkin, A. & He, T. (2024). The geoeconomics of global semiconductor value chains: Extraterritoriality and the US-China technology rivalry. Review of International Political Economy, 31(2), 674-699.

Mantelassi, F. (2024). Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy. Retrieved from https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and

Millon, C. (2024). Digital geopolitics and the rise of cyberwarfare. Retrieved from https://www.gisreportsonline.com/r/digital-geopolitics-cyberwarfare/

Negro, G. (2019). A history of Chinese global Internet governance and its relations with ITU and ICANN. Chinese Journal of Communication, 13(1), 104-121.

Qiao-Franco, G. (2024). An Emergent Community of Cyber Sovereignty: The Reproduction of Boundaries? Global Studies Quarterly, 4(1), 1-11.

Qin, M. & Han, W. (2024). China piles $47.5 billion into 'Big Fund III' to boost chip development. Retrieved from https://www.caixinglobal.com/2024-05-28/china-piles-475-billion-into-big-fund-iii-to-boost-chip-development-102200633.html

Radanliyev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 9(1), 28-78.

Ray, T. (2026). Three elements Trump's 'Pax Silica' needs to succeed. Atlantic Council. Retrieved from https://www.atlanticcouncil.org/dispatches/three-elements-trumps-pax-silica-needs-to-succeed/

Rolf, S. & Schindler, S. (2023). The US–China rivalry and the emergence of state platform capitalism. Environment and Planning A: Economy and Space, 55(5), 1255-1280.

Scharre, P. (2023). Four Battlegrounds: Power in the Age of Artificial Intelligence. W.W. Norton & Company.

Schindler, S., Alami, I., DiCarlo, J., Jepson, N., Rolf, S., Bayırbağ, M. K., … & Zhao, Y. (2024). The Second Cold War: US-China Competition for Centrality in Infrastructure, Digital, Production, and Finance Networks. Geopolitics, 29(4), 1083-1120.

Shahbaz, A. (2018). The Rise of Digital Authoritarianism. Freedom House. Retrieved from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism

Sheehan, M. (2023). China's AI regulations and how they get made. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117

Slawotsky, J. (2021). The fusion of ideology, technology and economic power: Implications of the emerging new United States national security conceptualization. Chinese Journal of International Law, 20(1), 3-62.

Slawotsky, J. (2022). Digital currencies and great power rivalry: China as a disseminator in the digital age. Asia Pacific Law Review, 30(2), 242-264.

Slotten, H. R. (2022). Beyond Sputnik and the space race: The origins of global satellite communications. Johns Hopkins University Press.

The Federal Government. (2023). Robust. Resilient. Sustainable. Integrated Security for Germany: National Security Strategy. Retrieved from https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf

The Guardian. (2026). China blocks Nvidia H200 AI chips that US government cleared for export – report. Retrieved from https://www.theguardian.com/technology/2026/jan/17/china-blocks-nvidia-h200-ai-chips-that-us-government-cleared-for-export-report

U.S. Department of the Treasury. (2026). Treasury proposes rule to implement the GENIUS Act's requirements to counter illicit finance. Retrieved from https://home.treasury.gov/news/press-releases/sb0435

Villasenor, J. (2025). How Overly Aggressive Bans on AI Chip Exports to China Can Backfire. Brookings Institution. Retrieved from https://www.brookings.edu/articles/how-overly-aggressive-bans-on-ai-chip-exports-to-china-can-backfire/

West, D. M. & Allen, J. R. (2018). How artificial intelligence is transforming the world. Brookings Institution. Retrieved from https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/

Ying, R. (2020). The Digitalization of Lifestyle in a Digital Era: A Case Study of WeChat in China. International Journal of Literature and Arts, 8(3), 119-126.

Zhang, J. (2020). China's Military Employment of Artificial Intelligence and Its Security Implications. International Affairs Review, August 16. Retrieved from https://www.iar-gwu.org/print-archive/blog-post-title-four-xgtap

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Zúñiga, N., Burton, S. D., Blancato, F., & Carr, M. (2024). The Geopolitics of Technology Standards: Historical Context for US, EU and Chinese Approaches. International Affairs, 100(4), 1635-52.

ARTICLE HISTORY: Received 2025-11-20 / Accepted 2026-01-19