Politics and Governance
2025 • Volume 13 • Article 10234
https://doi.org/10.17645/pag.10234

cogitatio

ARTICLE

Open Access Journal

Data Flows Meet Great Power Politics: The Emerging Digital Security Dilemma Between China and the US

Ziyuan Wang

Institute of International Relations, China Foreign Affairs University, China

Correspondence: Ziyuan Wang (wangziyuan@cfau.edu.cn)

Submitted: 28 February 2025 **Accepted:** 25 August 2025 **Published:** 5 November 2025

Issue: This article is part of the issue "Technology and Governance in the Age of Web 3.0" edited by Chang Zhang (Communication University of China), Zichen Hu (London School of Economics and Political Science), and Denis Galligan (University of Oxford), fully open access at https://doi.org/10.17645/pag.i443

Abstract

This article employs security dilemma theory to probe the geopolitical implications of state intervention in the digital realm. Its central argument is that with cross-border data flows being conducive to subversive actions, governments have grown wary of rival states leveraging control over data flows to advance strategic objectives. Therefore, when a government tightens its domestic regulation over data flows, its actions could trigger a spiral of suspicions and countermeasures with other states. Such a security dilemma fosters the technology rivalry between China and the United States. As Beijing became sensitive to unrestricted flows of information and data, it set out to exert tighter control over data flows within and across Chinese borders. But Beijing's move aggravated US perceptions of subversive threats, prompting Washington to try to drive Chinese entities out of the US-centric technology ecosystem. Washington's actions signaled hostile intent to China, which in turn decided to build alternative digital infrastructures. Given that state intervention in the digital realm could exacerbate great power rivalry, Web 3.0 will likely perpetuate security dilemma dynamics by shifting the battlefield from corporate platforms to protocol layers, from data ownership to infrastructure sovereignty.

Keywords

data flows; digital infrastructure; security dilemmas; subversion; US–China relations

1. Introduction

Web 3.0 technologies such as blockchain and generative artificial intelligence sharply increase the importance of data for socioeconomic life. Widely expanding the use of data in productive and commercial fields, those technologies not only boost market efficiency but also enable commercial actors to evade government scrutiny. In turn, governments are devising policies to regulate unrestricted data flows. China,

for its part, went beyond regulating market-oriented blockchain applications. It made massive state-led investments in blockchain technology as part of its broader ambition to build a sovereign digital ecosystem. This project was designed to lessen China's dependence on Western digital infrastructures and deepen its ties with the Global South (Kumar, 2025). Beijing's digital strategy has aroused Washington's concerns. The White House's *National Cybersecurity Strategy* claims the following:

> The People's Republic of China now presents the broadest, most active, and most persistent threat to both [US] government and private sector networks….Having successfully harnessed the Internet as the backbone of its surveillance state and influence capabilities, the PRC is exporting its vision of digital authoritarianism, striving to shape the global Internet in its image and imperiling human rights beyond its borders (White House, 2023).

Ostensibly, Beijing's perceived success in harnessing blockchain would be instrumental in extending its geopolitical reach and reshaping norms in the digital realm. But whether this scenario materializes depends not only on China's digital policy but also on the US approach to Chinese challenges. Notably, the Obama administration did not endeavor to limit China's access to international markets for digital technologies after it realized the expansion of China's surveillance apparatus. In contrast, officials of the Trump and Biden administrations frequently pointed to China's surveillance system as a threat to American interests. This dramatic policy shift invites the following questions: Why did the US become sensitive to the evolution of China's digital development? Is Beijing's digital strategy driven by an impulse to compete with the US for technological supremacy? And what are the implications of data flows for US–China relations?

Security dilemma theory offers an important perspective. From it, some analysts suggest that because China is deeply integrated into global networks, its domestic practice could generate considerable security externalities. As a result, even the policy measures China undertook to enhance its domestic security could pose a threat to countries embedded in global supply chains (Pearson et al., 2022). Still, China's initial motives in strengthening its regulation of data flows and the concomitant security risks to the US are underexplored. Specifically, it is unclear why Chinese leaders adopted a heavy-handed regulatory approach to their own digital economy, which risked jeopardizing market stability in China as a crucial source of regime legitimacy. On the other hand, since the US was and still is a dominant player in the global flows of data, why it became concerned over China's digital policy is worth investigating.

In response, this article focuses on the subversive threats of data flows as a crucial source of security dilemmas among states (Section 2). Sections 3–5 illustrate this argument through a case study of the rise of the US–China technology rivalry. Section 3 discusses how the Snowden revelations, cyberattacks, and Russian interference in the 2016 US election heightened awareness in Washington of the subversive potential of data flows. Section 4 explores how concerns about subversion shaped Chinese regulation of data flows. Section 5 shows how the two sides' security-enhancing measures produced a spiral of tensions by fostering mutual perceptions of hostile intent. Section 6 contrasts my account with the zero-sum competition model and underscores the former's explanatory leverage. The article concludes by considering the implications of Web 3.0 for digital security dilemmas.

2. Security Dilemmas in the Digital Realm

The security dilemma is a central dynamic in international politics. Whereas states must strive to enhance their security in the anarchic international system, measures undertaken by states to bolster their self-defense can still inspire reciprocal fears and fuel interstate rivalry accordingly (Jervis, 1978). Nevertheless, security dilemma theory posits that international conflict is not inevitable but occurs or escalates in situations wherein state actors lack confidence in the prospects for cooperation (Glaser, 1997). Offense dominance and perceptions of hostile intent may create such situations. Offense dominance means the acquisition of territory and strategic resources is relatively easy. It is, in general, characterized by large offensive opportunities or defensive vulnerabilities (Evera, 2001, pp. 160–166). In such circumstances, offensive actions can yield considerable benefits; accordingly, state actors may perceive each other as prone to aggression. Such perceptions, moreover, can be bolstered by the human cognitive tendency to see threatening behavior as intentional (D. Johnson, 2020, pp. 118–120). Once convinced of each other's hostile intent, state actors may feel compelled to adopt hardline policies and hence find themselves in a spiral of tensions.

The digital realm can foster offense dominance by lowering the barriers to subversive actions. By definition, subversion refers to "targeted, hostile action within another state to weaken it or cause it to alter its policy" (Kastner & Wohlforth, 2025, p. 1). This is a distinct form of offense. Unlike diplomatic and military activities, subversion operates inside the territory of other states. Subversion also goes beyond espionage in its intended effects—namely, reshaping the domestic political dynamics of target states. Extensive espionage, though, may arouse fears of subversion by revealing the capacity of a rival state to carry out unlawful operations abroad.

Data flows tend to facilitate subversion. Through online propaganda, co-option, and cyberattacks, foreign governments could exploit data flows to undermine or manipulate the domestic institutions of target states. Alarmingly, the same data that allow companies to tailor products to user preferences may also be weaponized to mobilize societal groups against a state's domestic order. Likewise, foreign adversaries may engage in cyber espionage to access private data and identify vulnerable individuals in the target country's government institutions. The adversaries then would manipulate financial and career incentives to co-opt those individuals to undertake activities contrary to that country's interests. Finally, data flows enable hackers to exploit systems' vulnerabilities. Hackers do not traverse land, sea, or air to mount an attack; rather, they can infiltrate target systems through technical backdoors or by altering data. Cyberattacks thereby play a crucial role in the theft of valuable data and the erosion of public trust in the domestic institutions of target countries (Maschmeyer, 2023).

The offensive opportunities in the digital realm—such as online propaganda, co-option, and cyberattacks—correspond to the defensive vulnerabilities of target systems. Because the internet is an open and virtual space, it is easy for threat actors to conceal their identities as they undertake subversive actions. Further, the layered design of digital infrastructures inevitably contains critical flaws ripe for exploitation. As digital systems become increasingly interdependent, every driver, cloud service, and Application Programming Interface used by customers is a potential vector of attack. Although the strategic implications of cyber intrusions and algorithm manipulations are debatable (Gartzke & Lindsay, 2015), the capacity of adversaries to infiltrate critical infrastructures and institutions undetected is sufficiently worrisome to national security decision-makers. Crucially, subversive actions violate sovereignty as the basis of state survival.

Inasmuch as cyber intrusions can erode public trust in domestic institutions, they are a legitimate national security concern.

Since subversive threats foster offense dominance in the digital realm, governments' exertion of direct control over data flows can aggravate fear and competition among states. For example, if state A tries to enhance administrative oversight over commercial actors operating under its jurisdiction, such measures could lead other states to worry that it will obtain valuable data. In response, state B will try to curtail its market ties with state A, but such a move may signal hostile intent and fuel A's pessimism about its international environment (Copeland, 2016). This pattern of interactions would encourage technology rivalry, as state actors harbor security concerns regarding their interconnections in the digital realm.

The rise of the technology rivalry between China and the US provides a crucial case to examine the argument laid out above. Given that the US and China are now engaged in a systemic competition for global leadership, it is tempting to see their technology rivalry as an extension of the ongoing bipolar struggle. However, if the evidence presented in the case study convincingly challenges this assumption, it will boost the plausibility of my argument derived from security dilemma theory.

3. Internet Openness, Subversive Threats, and US National Security

The internet is a public domain. Its openness enables frequent and rapid data flows across disparate systems and devices. Over decades, a few tech giants have become dominant over data resources by acting as key nodes in data flows. This structural reality enabled the US government to exploit the internet for intelligence advantages. Through the tech companies and related digital infrastructures operating under its jurisdiction, the US government could access users' data and track their activities. After 9/11, for instance, the US government demanded that the Society for Worldwide Interbank Financial Telecommunication share data to help it track terrorist financing (Farrell & Newman, 2019, p. 61).

The US's exploitation of global digital infrastructures for espionage became widely known after the Snowden files exposed the US National Security Agency's collection of vast amounts of private data of American and foreign citizens. In the shadow of the Snowden revelations, Washington was hard-pressed to reassure the public. Although the US government subsequently enacted new legislation and regulations to oversee federal data usage, public distrust made American tech companies less willing to cooperate with the government (Sanger, 2018, pp. 85–99). The growing rift between the US government and tech firms made it more challenging to defend against cyberattacks, rendering the US vulnerable to digital subversion. In 2014–2015, the US Office of Personnel Management suffered a series of cyberattacks, leading to the leak of personal data of millions of federal employees. According to the Committee on Oversight and Government Reform under the House of Representatives, this leak exposed a vast number of US government officials to foreign influence operations, including blackmail and family threats. The Committee in turn emphasized that the US "has never been more vulnerable to cyberattacks" (Committee on Oversight and Government Reform, 2016, p. v).

The 2016 election interference by Russia raised widespread anxiety in the US about the threats of subversion of its democratic institutions. During the campaign period, Russia's government agencies and related organizations spread disinformation, stole and leaked email information associated with the Hillary

campaign, and created myriad false accounts to spread anti-democracy narratives (Kastner & Wohlforth, 2025, pp. 151–167; Sanger, 2018, pp. 201–235). In the aftermath of the presidential election, the bipartisan committee led by Robert Mueller ascertained the fact that Russia's intelligence agency managed to exfiltrate a massive amount of data from the computer networks of the Democratic National Committee, an operation that enabled Moscow to disrupt the 2016 US election (Mueller, 2019, pp. 94–107). Although it is not clear whether such operations were decisive in altering the election outcome, they surely disrupted the democratic process and sowed chaos in the US.

The events described above highlight how data exfiltration has increased subversive threats. Because of its centrality to digital networks, the US fell victim to such threats even though Washington also managed to exploit internet openness for strategic and intelligence advantages. China's domestic regulatory measures were motivated by similar fears of subversion, as it has long been concerned with ideological influence from abroad.

4. China's Sensitivity to Subversive Threats

Since the end of the Cold War, fears about subversion have been deeply rooted in Beijing's preoccupation with "political security" (*zhengzhi anquan*). In the official discourse, political security means "national sovereignty, government power, political systems, political order, and ideologies are protected from threats, infringements, subversion, and destruction" (Yang, 2018). This concept is identical to regime security. Chinese concerns for regime security stemmed from anxiety over the perceived US strategy of "peaceful evolution" (Zhang, 2023). In the post-Cold War years, Beijing's security anxiety was deepened by the fact that liberal ideology served as the normative foundation for US hegemony. Hu Jintao, the General Secretary of the Communist Party of China (2002–2012), stated that "the struggle in the international ideological and cultural sphere remains profound and complex" (Hu, 2006, p. 1). In 2008–2012, a series of ideological disputes between China and the West, combined with the Jasmine Revolution in North Africa and the Middle East, led China to introduce a surveillance system known as the Great Firewall, which enabled the regime to track and filter the data flowing across its borders.

Subsequently, the Snowden revelations drove home the urgency of strengthening regulatory measures, as they confirmed that Washington had been exploiting global data flows for strategic purposes. Snowden thus aggravated Chinese perceptions of subversive threats from a weaponized internet. According to the Cyberspace Administration of China, the Snowden incident sounded the alarm around the world to the effect that "without cybersecurity, there is no national security" ("Xuezhe jiedu," 2014; also see Pearson et al., 2022, p. 146).

Consequently, Chinese leaders decided to exercise direct control over data flows across and within Chinese borders. In February 2014, China announced the establishment of the Central Leading Group for Cybersecurity and Informatization, unifying the functions of various network management departments under the State Council and the Propaganda Department of the Chinese Communist Party. Under this central authority, China undertook to curtail foreign access to Chinese data. In 2015, the State Council issued guiding suggestions and action plans regarding the use of data in the market, enhancing government oversight of enterprise data. Article 25 of the 2015 National Security Law emphasizes that "maintaining cyberspace sovereignty, security, and development interests" is a major task of national security (People's

Central Government, 2015). Article 37 of the Cybersecurity Law further clarified that operators of critical information infrastructure must store personal information and important data within the country and that domestic commercial entities must have government approval before they transfer data abroad (Cyberspace Administration of China, 2016). Didi, China's largest ride-hailing company, was punished by this law, which forced it to delist from the New York Stock Exchange in 2021. The localization of data storage thus became a central feature of Chinese governance of the digital realm.

Establishing stringent oversight over tech companies has also better positioned the Chinese government to censor societal information. Early in 2016, the Chinese government began to pursue "special management shares," which would allow government agencies to participate in major decision-making of private companies through small shareholding. Specifically, the State Administration of Press, Publication, Radio, Film, and Television suggested that state-owned special management shares account for at least 1% of a company's shares, an arrangement that would give government agencies board seats and the right to review media content (Jin, 2016). By 2021, ByteDance, TikTok's parent company, had accepted the special-management-shares arrangement (De Mott, 2023). Tencent—the parent company of WeChat (arguably the most popular messaging app in China)—appears not to have done so, but it is widely known that its headquarters in Shenzhen city "has at least one floor exclusively reserved for internet inspectors composed of state security police, national security staff, and online censors" (Walker, 2021). These regulatory measures have given China's government privileged access to data, allowing it to monitor the society, deter potential challengers, and shape the domestic information environment more effectively.

5. The Spiral of Suspicions and Decoupling Between the US and China

This article suggests that security dilemma dynamics in the digital realm contribute to the US–China technology rivalry. Thanks to internet openness, data flows become central to socioeconomic development; accordingly, data flows assume strategic importance in enabling threat actors to subvert the domestic institutions of nations connected to the internet. Policymakers in Beijing and Washington thus became concerned about subversive threats. As a result, although China's strengthening of regulation over its tech companies was driven by the defensive motives of safeguarding regime security, Washington has come to consider China's domestic policy a subversive threat and undertake assertive actions in response.

5.1. The Trump Administration's Concerns for Chinese Subversion

As Donald Trump's first administration was poised to escalate trade conflict with China, economic security became a top priority for US officials. This policy stance helped intensify Washington's scrutiny of Beijing's data regulation practice and the US's domestic vulnerabilities. The White House noted that "China gathers and exploits data on an unrivaled scale and spreads features of its authoritarian system" (Trump, 2017, p. 25). In early October 2018, Vice President Mike Pence delivered a landmark speech outlining a shift in US policy, wherein he characterized China as an "unprecedented surveillance state." Pence then suggested that China's attempted control over data flows signaled its revisionist ambition. As he put it, "a country that oppresses its own people rarely stops there. And Beijing also aims to extend its reach across the wider world" (Pence, 2018).

Pence's speech was indeed motivated by the cabinet's decision to counter China's subversive behavior. When Trump's national security team gathered to prepare that speech, they were preoccupied with Chinese attempts

to influence the 2018 Congressional elections. According to John Bolton, then National Security Advisor, Trump's officials believed that "China could bring considerably greater resources to bear on this effort [election meddling] than Russia" (Bolton, 2024, p. 262). In their view, China had both the capability and intention to subvert the US political institutions. To deprive Beijing of subversive means, Washington undertook to curtail America's commercial and societal ties with China.

5.2. US Decoupling Measures Against China

Just a month after Pence's speech, the US Department of Justice launched the China Initiative, a program designed to prosecute cases related to Chinese economic espionage and data security threats (US Department of Justice, 2021). Toward the end of the first Trump administration, this program had publicized nearly 60 significant cases (US Department of Justice, 2021), with FBI Director Christopher Wray claiming that 2,000 cases related to China had been under investigation (Lucas, 2022). While the China Initiative was primarily directed against economic espionage activities, it showed the tendency of US leaders to assume the worst about Chinese intentions in collecting data. This very perception of threat led the US to decouple its technology ecosystem from China.

The US-led sanctions against Huawei and the Clean Network program are notable examples in this regard. Both policy actions were designed to curtail the access of Chinese data service providers to the markets of the US and its allies. Initially, the US government accused Huawei of providing technical support to Iran through fraudulent means. Based on this charge, the US demanded that Canadian authorities arrest and extradite Huawei Chief Financial Officer Meng Wanzhou. Shortly thereafter, the US government imposed comprehensive sanctions on Huawei. In May 2019, the US Department of Commerce designated Huawei to the Entity List subject to specific license requirements for certain transactions, which significantly restricted Huawei's business dealings with American companies. Secretary of State Mike Pompeo justified this move by claiming that "if the Chinese Communist Party wants to obtain information through the Huawei technology, Huawei will certainly give it to them" (Segal, 2021, p. 157). Arguably, Huawei's perceived association with the Chinese government aroused concerns in Washington that Beijing could use this company as a vehicle for subversion. According to the US Department of Commerce, Huawei posed a threat to US national interests due to its perceived ties to the Chinese military, its involvement in stealing trade secrets from US companies, and its ability to covertly access mobile phone networks around the world through "back doors" (Fitzgerald, n.d.). The last charge underscored Washington's misgivings over China weaponizing data for subversive actions.

The Clean Network initiative signified a crucial move by the Trump administration toward technology decoupling. Initially, the Department of State committed to provide a "clean pathway" for all 5G traffic passing through US diplomatic facilities. Several countries, including Japan, Australia, the Czech Republic, Norway, and Israel, joined the US in the 5G Clean Path initiative. Traditional allies including the UK, France, and Canada also announced that they would exclude Huawei from their 5G suppliers. Building on this practice, the Department of State officially launched the Clean Network initiative in August 2020, a program committed to establishing international trust standards for digital infrastructure (US Department of State, n.d.). Targeting Chinese network carriers, app downloads, mobile apps, cloud storage, and undersea cables, this initiative aimed to prevent Chinese-related commercial entities from accessing US citizens' information through digital infrastructures (Pompeo, 2020). The Council on Foreign Relations compared the Clean

Network program to the Long Telegram of the 21st century (Fidler, 2020). It suggested that the US had set out to hinder China from using data flows to undermine democratic institutions—just as after WWII the US became wary of the Soviet Union's subversion against European countries.

Meanwhile, the first Trump administration issued executive orders to prohibit transactions with the parent companies of two popular Chinese apps (WeChat and TikTok). The orders highlighted the potential for the Chinese government to access personal data of American citizens, which could be used to facilitate subversive actions. As TikTok was on its way to becoming the most popular entertainment platform in American society, the Trump administration claimed that data collection via this platform "threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage" (Trump, 2020). Trump also pointed to the censorship practice of TikTok regarding information related to China's crackdowns on Hong Kong protests and extensive human rights violations in Xinjiang. Hence, his administration was concerned that TikTok might be "used for disinformation campaigns that benefit the Chinese Communist Party" (Trump, 2020).

Joseph Biden's administration inherited Trump's concerns for subversive threats in the digital realm, but modified Trump's approach to national security. Whereas Trump tried to confront China with unilateral sanctions, the Biden administration sought to build a technology ecosystem among US allies by tightening restrictions on critical technology transfers to China. In an elaboration on Biden's technology strategy, National Security Advisor Jack Sullivan vowed that the US must lead the revolution in digital technology, promote American values (notably privacy rights and intellectual property), and work with its allies and partner countries to promote competitiveness and prosperity (Sullivan, 2021). Under this policy, the Biden administration established the Critical and Emerging Technology Working Group with Japan, South Korea, Australia, and India, four regional powers with technological potentials to compete with China. With its Asian and European allies, the Biden administration also created a series of mechanisms for coordination on a series of economic security measures, such as developing common standards for emerging technologies, implementing export controls, and enhancing supply chain resilience and cybersecurity (White House, 2023, p. 30). Washington's actions aggravated Chinese perceptions of hostility. President Xi openly stated that "Western countries led by the United States have carried out all-around containment, blockade, and suppression against us, which presents unprecedentedly severe challenges to our development" (State Council of China, 2023). By that time, China's leadership had adopted new macroeconomic policies designed to reduce its reliance on the American market. Then Vice-Premier Liu He interpreted China's policy approach as a necessary response to de-globalization and the restructuring of industrial and supply chains (Liu, 2020).

5.3. China's Quest for Alternative Digital Infrastructures

As China was braced for a long-term struggle with the US, it sought to develop a technology ecosystem independent of the US-centered digital infrastructure. Blockchain technology served this end. Back in 2016, China began to incorporate blockchain technology into its grand plan for national development. The 13th Five-Year National Informatization Plan initiated an industrial policy aimed at developing "revolutionary technologies" (*dianfuxing jishu*; People's Central Government, 2016). Consequently, blockchain came to figure prominently in China's development strategy. In late 2019, against the backdrop of escalating tensions in US–China relations, Xi convened a politburo meeting to focus on blockchain as a

national strategic priority. On that occasion, he stressed the need to "accelerate the deep integration of blockchain with cutting-edge information technologies such as artificial intelligence, big data, and the Internet of Things," because blockchain could help achieve a "breakthrough in driving independent innovation of core technologies" ("Xi Jinping zai," 2019).

Notably, China unequivocally rejected the decentralization principle of blockchain technology. The Chinese authorities went out of their way to limit the use of cryptocurrencies in the domestic market, culminating in a comprehensive ban on all cryptocurrency transactions in 2021 ("China declares all crypto-currency," 2021). Consistent with its stringent regulatory policy over private digital platforms, Beijing endeavored to prevent commercial actors from accessing blockchain. Still, it wanted to harness this technology to strengthen its control over digital infrastructures. Around 2020, the Chinese government stepped up efforts to promote the digital version of its currency (known as e-CNY). While the central ledger of e-CNY is under the control of Chinese authorities, the tamper-resistance of blockchain offers a technical guarantee that Beijing cannot secretly alter the ledger. This lends credibility to e-CNY among international banks. Thus, blockchain technology enables state-led digital payment systems, which helps reduce China's reliance on Western-dominated financial infrastructures.

Building on this initiative, China elevated cooperation with Russia. The Sino-Russian digital collaboration made significant progress in the wake of China's diplomatic fallout with the Biden administration in Alaska. In March 2021, Chinese Foreign Minister Wang Yi met with his Russian counterpart Sergei Lavrov, who called for a shift "away from using international payment systems controlled by the West" (Tétrault-Farber & Osborn, 2021). In turn, Wang Yi proposed that China and Russia work together to "bolster the security of each other's regime and institution" ("Wang Yi tong," 2021). The Chinese and Russians thus found a common interest in the joint development of digital infrastructures, which served to resist Western geopolitical and ideological pressures. By the end of 2021, the two governments had agreed to "give full play to the role of infrastructure organizations and financial institutions of both countries, including the RMB clearing bank in Russia" (Ministry of Foreign Affairs of the People's Republic of China, 2021). This initiative gained traction after the outbreak of the Russia–Ukraine War. By mid-2025, major Russian banks had introduced a netting payments system dubbed the China Track, which could help Russia circumvent the sanctions imposed by the US and the European Union ("Exclusive," 2025).

In sum, with both Washington and Beijing fearing subversion through data flows, each explored paths toward digital decoupling. This process soon became self-reinforcing. In Washington, concerns over digital subversion prompted policy measures designed to curtail market ties. The US sanctions on Chinese firms spurred Beijing to build alternative digital infrastructures aimed at the creation of an autonomous technology ecosystem, as China's leaders interpreted Washington's actions as evidence of hostile intent. In this context, China has tried to harness Web 3.0 technologies such as blockchain to enhance its autonomy within global infrastructure networks. What is clear is that regime security concerns have propelled Beijing to elevate blockchain technology to a national strategic priority.

6. A Contest for Technological Supremacy? Evaluating an Alternative Argument

This article suggests that when American and Chinese leaders became sensitive to subversive threats in the digital realm, they adopted policies that fueled a spiral of mutual suspicions and led to technology decoupling

and rivalry. Grounded in security dilemma theory, this argument stands in contrast with the model of zero-sum competition espoused by several leading experts on US–China relations. In their view, China has been pursuing a grand strategy of displacing the US from its hegemonic position (Doshi, 2023; Friedberg, 2011; Mastro, 2024). As a corollary, the emerging technology rivalry is merely an extension of the broader competition for global power between a rising China and the US, the established hegemon.

The zero-sum competition model, however, falls short in two respects. First, it overlooks the defensive motives of Beijing in formulating its digital policies. Certainly, China's approach to data reflected Xi Jinping's personal vision for national development, which was premised on the idea that the Chinese practice of Marxist ideology would prove its superiority vis-à-vis Western liberalism (Shirk, 2023, p. 184). But this does not mean Xi would necessarily pursue an offensive strategy. Quite the contrary, Xi's policies were in large part defensive, as they highlighted the need to safeguard China's domestic regime. Since 2014, Xi has envisioned China becoming an "Internet strong country" (*wangluo qiangguo*), while emphasizing that "if we can't pass the test of the Internet, we can't pass the test of holding [domestic] power for a long term" (Cyberspace Administration of China, 2024). Internationally, China has sought to justify its defensive approach to data security by promoting "cyber sovereignty" (*wangluo zhuquan*). This concept was officially proposed by Xi at the 2015 World Internet Conference, where he claimed that "cyber surveillance, cyber espionage, and cyber terrorism have become global public hazards" ("Xi Jinping," 2015). Cyber sovereignty was, therefore, designed to address the "global public hazards" posed by the US's exploitation of the internet. According to Xi, the norm of cyber sovereignty meant "respecting the rights of each country to independently choose its internet development path [and] internet management model" (Xi, 2015). Because this norm upheld the state's role in the management of cybersecurity, it served to shield China from hostile ideologies from abroad.

Apparently, the norm of cyber sovereignty is contrary to the internet freedom promoted by the US. But it is worth noting here that the norm of cyber sovereignty does not prescribe any concrete path of technological development for other countries. While China has been intent on localizing data storage and limiting data flows across its borders, this practice would hinder China from shaping global norms for data flows. China expert Matthew Johnson notes that "the Party's strategy for data accumulation through multilateral trade agreements is intentionally offset by domestic laws making the vast majority of China's data a protected resource" (Johnson, 2023, p. 33). If foreign governments embrace this model of cyber sovereignty, they will have to accept asymmetric access to data flows, and it is doubtful that they are willing to do so. However, since the norm of cyber sovereignty does not specify the terms for an alternative internet order, it could legitimize the heterogeneous strategies that various authoritarian regimes may adopt to safeguard their domestic political order. Along with those regimes, China will likely use cyber sovereignty as window dressing for its continued exploitation of the open internet for access to data that could yield economic and intelligence advantages (Lindsay, 2015).

Put simply, the zero-sum competition model tends to overstate China's ambitions in the digital realm. There is no denying that China's privileged access to data would enable its technological innovation. Xi compared data to "the oil of the 21st century," asserting that "whoever masters big data technology will hold the resources and maintain the initiative for development" ("Laolao bawo," 2016). However, the use of data is non-rivalrous—one's use does not diminish others' use; rather Xi's remark may well reflect his sensitivity to regime survival. Indeed, authoritarian regimes have long grappled with the dilemma of maintaining social

control and fostering a dynamic economy. Digital technologies offer a way out. By enabling the micro-targeting of individual behaviors, digital technologies promise to lower the costs of surveillance and boost market efficiency (Wright, 2018). For that matter, Xi mobilized the country to "leverage big data to enhance the modernization of national governance" ("Xi Jinping," 2017). Furthermore, when the Central Leading Group for Cybersecurity and Informatization was elevated to the status of full commission in 2018, Xi took the occasion to provide comprehensive guidance on China's cyber sector with a focus on regime security. In his words, "it is necessary to enhance the overall governance capability of cyberspace…[and] to consolidate the ideological foundation for the unity and struggle of the entire Party and the Chinese people" (People's Central Government, 2018).

In contrast to the model of zero-sum competition, security dilemma theory underscores the defensive motives of China in promoting the norm of cyber sovereignty and developing digital infrastructures—namely, Beijing's anxiety for regime security. This raises a second issue: Why did China's domestic regulatory policy arouse security anxiety on the US part? Security dilemma theory answers this question by underscoring US fears of subversion. That is, it was not until US leaders became sensitive to subversive threats in the digital realm that they became determined to restrict the access of Chinese entities to the American market.

While differences over internet governance had emerged during the Obama years as an outstanding dispute, that did not derail US–China technology relations. In 2010 when Google declared its withdrawal from Mainland China, then Secretary of State Hillary Clinton stressed the need for dialogue and communication in promoting China's internet openness (Clinton, 2010). Even an escalation of cyber disputes did not lead to the technology rivalry between the two countries. In the aftermath of the Snowden revelations, US leaders felt compelled to reaffirm their commitment to data security. They in turn tried to distinguish between cyber espionage for commercial gain and cyber operations conducted for national security purposes (Lindsay, 2015, p. 26). To vindicate this point, the Obama administration in May 2014 indicted five Chinese officers linked to the People's Liberation Army for stealing commercial sector data. Counterintuitively, this move helped elicit Beijing's cooperation, as Chinese leaders put a premium on maintaining stable relations with Washington (Sanger, 2018, pp. 121–123). In September 2015, the US and China reached a bilateral agreement on cyber behavior during the state visit by President Xi. The agreement led to serious bilateral negotiations about cyber norms and a sharp decline of Chinese cyberattacks (Hvistendahl, 2016). This outcome is contrary to the zero-sum competition model that considers a US–China technology rivalry inevitable.

Although the dispute over cyber norms signified US–China antagonism in the digital realm, it was not sufficient to bring about technology rivalry, as neither Washington nor Beijing pursued a policy of technology decoupling during the Obama years. The turning point instead occurred in the aftermath of Russian interference in the US election of 2016. Prior to that, the US had been solely focused on China's cyber espionage. In the shadow of Russian interference, however, the Trump administration began to move beyond this focus and frame China's cyber threats in terms of subversion. It noted in particular that China was "improving its cyber attack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens" (Coats, 2019, p. 5). Linking this issue with "online influence operations" and "election interference," Trump's officials considered China a major source of subversive threats alongside Russia (Coats, 2019, p. 5). Similarly, during the Biden years, the US intelligence community stated that "Beijing's growing efforts to actively exploit perceived US societal divisions using its online personas move it

closer to Moscow's playbook for influence operations" (Office of the Director of National Intelligence, 2023, p. 10). It was in this context that Washington resolved to restrict the access of Chinese entities to the American market. Sensitivity to subversive threats thereby intensified security dilemma dynamics between China and the US.

7. Conclusion

In the digital realm, security dilemma theory suggests that the defensive measures undertaken by a state to govern its domestic digital environment could pose subversive threats to other states, which would in turn pursue technology decoupling. However, decoupling measures could signal malign intent and help escalate interstate tensions into technology rivalry. Security dilemma theory helps explain the emerging technology rivalry between the US and China. As Beijing became alert to unrestricted flows of information and data, it pursued stringent control over tech companies in charge of managing cross-border data flows. This measure was largely defensive in that it was primarily designed to fend off subversion by Western liberal ideology. Still, China's regulatory policies aggravated American perceptions of subversive threats, prompting Washington to limit the access of Chinese entities to its market. For China, Washington's actions likewise signaled hostile intent; thus, Beijing decided to undertake preventive measures to develop separate digital infrastructures. Hence, a digital security dilemma has emerged between the US and China, wherein efforts by one side to tighten regulatory control over data flows are perceived as threatening by the other.

Investigating the causal dynamics behind the US–China technology rivalry is crucial to understanding the geopolitical risk of Web 3.0. China's active use of blockchain technology could shift the arena of contestation to more foundational layers of the internet—the protocol layers that underpin decentralized systems. Unlike the earlier era dominated by corporate digital platforms, the new competition will likely be focused on infrastructure sovereignty—that is, who controls the rules, protocols, and standards that structure digital interactions on a global scale. In turn, governments would seek to protect their technology ecosystems, develop indigenous digital infrastructures, and align protocols with state interests. As demonstrated, this trend had its origins in great powers' fears of subversion via data flows. Web 3.0 technologies seem to help mitigate such fears by enhancing infrastructure resilience. However, when governments manage to develop their own digital infrastructures using Web 3.0 technologies, their direct involvement in digital governance and infrastructure-building could signal competitive intentions and exacerbate international perceptions of threat. As security dilemma theory suggests, even if state intervention in the digital realm is initially intended as a defensive regulatory act, that could still intensify the dynamics of great power rivalry.

Acknowledgments

I would like to thank Coh Chong Chen and Xue Gong for inviting me to present this article at the 2025 workshop "Economic Statecraft in U.S.–China Tech Competition" held by the S. Rajaratnam School of International Studies at Nanyang Technological University. I am especially indebted to Miles Evers and Kai He for their invaluable feedback. Thanks also go to Tianjiao Jiang, Nan Yang, and Yue Yuan for their professional advice that encouraged me to explore cybersecurity as an emerging topic in international security studies. Needless to say, I am accountable for all errors and flaws in the article.

Funding

This research was supported by the Fundamental Research Funds for the Central Universities, project "Political Infiltration and Subversion in Great Power Competition" (大国竞争中的政治渗透和颠覆; 3162023ZYKC03).

Conflict of Interests

The arguments made in this article do not represent the official position of the Ministry of Foreign Affairs or any other government authorities in China.

References

Bolton, J. (2024). *The room where it happened: A White House memoir*. Simon & Schuster.

China declares all crypto-currency transactions illegal. (2021, September 24). *BBC*. https://www.bbc.com/news/technology-58678907

Clinton, H. (2010). *Remarks on internet freedom*. U.S. Department of State. https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

Coats, D. (2019). *Worldwide threat assessment of the US intelligence community*. Office of the Director of National Intelligence.

Committee on Oversight and Government Reform. (2016). *The OPM data breach: How the government jeopardized our national security for more than a generation*.

Copeland, D. (2016). *Economic interdependence and war*. Princeton University Press.

Cyberspace Administration of China. (2016). *Zhonghua renmin gongheguo wangluo anquan fa*. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm

Cyberspace Administration of China. (2024). *Shi nian qian, Xi Jinping shou ti cong 'wangluo daguo' dao 'wangluo qiangguo'*. https://www.cac.gov.cn/2024-03/08/c_1711570533840069.htm

De Mott, F. (2023, March 29). TikTok parent ByteDance has special stock owned by China's government: Here's how 'golden shares' give Beijing influence over the social-media giant. *Markets Insider*. https://markets.businessinsider.com/news/stocks/tiktok-ban-bytedance-golden-shares-chinese-government-communist-party-board-2023-3

Doshi, R. (2023). *The long game: China's grand strategy to displace American order*. Oxford University Press.

Evera, S. (2001). *Causes of war: Power and the roots of conflict*. Cornell University Press.

Exclusive: 'China Track' bank netting system shields Russia–China trade from Western eyes. (2025, April 22). *Reuters*. https://www.reuters.com/business/finance/china-track-bank-netting-system-shields-russia-china-trade-western-eyes-2025-04-22

Farrell, H., & Newman, A. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press.

Fidler, D. P. (2020, October 5). The Clean Network program: Digital age echoes of the "long telegram"? *Council on Foreign Relations*. https://www.cfr.org/blog/clean-network-program-digital-age-echoes-long-telegram#:~:text=The%20U.S.%20State%20Department's%20Clean,%22long%20telegram%22%20in%201946

Fitzgerald, S. (n.d.). *Fact sheet—Huawei & entity list*. https://fitzgerald.house.gov/sites/evo-subsites/fitzgerald.house.gov/files/evo-media-document/FINAL%20Fact%20Sheet%20%E2%80%93%20Huawei%20%26%20Entity%20List%202.2.21.pdf

Friedberg, A. (2011). *A contest for supremacy: China, America, and the struggle for mastery in Asia*. WW Norton.

Gartzke, E., & Lindsay, J. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2), 316–348.

Glaser, C. (1997). The security dilemma revisited. *World Politics*, *50*(1), 171–201.

Hu, J. (2006, August 24). *Jianchi heping fazhan daolu tuidong jianshe hexie shijie*. *People's Daily*, 1–2.

Hvistendahl, M. (2016, October 25). The decline in Chinese cyberattacks: The story behind the numbers. *MIT Technology Review*. https://www.technologyreview.com/2016/10/25/156465/the-decline-in-chinese-cyberattacks-the-story-behind-the-numbers

Jervis, R. (1978). Cooperation under the security dilemma. *World Politics*, *30*(2), 167–214.

Jin, X. (2016, December 6). Woguo chuanmei lingyu youxiao tuijin teshu guanli gu zhidu de sikao. *People's Daily Online*. http://theory.people.com.cn/n1/2016/1206/c83865-28928486.html

Johnson, D. (2020). *Strategic instincts: The adaptive advantages of cognitive biases in international politics*. Princeton University Press.

Johnson, M. (2023). *China's grand strategy for global data dominance*. Hoover Institute.

Kastner, J., & Wohlforth, W. (2025). *A measure short of war: A brief history of great power subversion*. Oxford University Press.

Kumar, A. (2025, May 5). China's blockchain playbook: Infrastructure, influence, and the new digital order. *Center for Strategic and International Studies*. https://www.csis.org/blogs/strategic-technologies-blog/chinas-blockchain-playbook-infrastructure-influence-and-new

Laolao bawo keji jinbu da fangxiang. (2016, December 13). *Communist Party Member Network*. https://fuwu.12371.cn/2016/12/13/ARTI1481594800256510.shtml

Lindsay, J. (2015). The impact of China on cybersecurity: Fiction and friction. *International Security*, *39*(3), 7–47.

Liu, H. (2020). *Jiakuai goujian yi guonei da xunhuan wei zhuti, guonei guoji shuang xunhuan xianghu cujin de xin fazhan geju*. People's Central Government. https://www.gov.cn/guowuyuan/2020-11/25/content_5563986.htm

Lucas, R. (2022, February 22). The Justice Department is ending its controversial China Initiative. *NPR*. https://www.npr.org/2022/02/23/1082593735/justice-department-china-initiative

Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, *46*(3), 570–594.

Mastro, O. (2024). *Upstart: How China became a great power*. Oxford University Press.

Ministry of Foreign Affairs of the People's Republic of China. (2021). Zhong-er zongli di ershiliu ci dingqi huiwu lianhe gongbao. https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202112/t20211201_10460421.shtml

Mueller, R. (2019). *Report on the investigation into Russian interference in the 2016 presidential election*. US Department of Justice.

Office of the Director of National Intelligence. (2023). *Annual threat assessment of the US intelligence community*.

Pearson, M., Rithmire, M., & Tsai, K. (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, *47*(2), 135–176.

Pence, M. (2018). *Remarks by Vice President Pence on the administration's policy toward China*. White House. https://trumpwhitehouse.archives.gov/briefings-statements/remarks-vice-president-pence-administrations-policy-toward-china

People's Central Government. (2015). *Zhonghua renmin gongheguo guojia anquan fa*. https://www.gov.cn/zhengce/2015-07/01/content_2893902.htm

People's Central Government. (2016). *Guowuyuan guanyu yinfa 'Shisanwu' guojia xinxihua guihua de tongzhi*. https://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm

People's Central Government. (2018). *Xi Jinping chuxi quanguo wangluo anquan he xinxihua gongzuo huiyi bing fabiao zhongyao jianghua*. https://www.gov.cn/xinwen/2018-04/21/content_5284783.htm

Pompeo, M. (2020). *Announcing the expansion of the Clean Network to safeguard America's assets*. https://2017-2021.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets

Sanger, D. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. Scribe.

Segal, A. (2021). Huawei, 5G, and weaponized interdependence. In D. Drezner, H. Farrell, & A. Newman. (Eds.), *The uses and abuses of weaponized interdependence* (pp. 149–165). Brookings Institution Press.

Shirk, S. (2023). *Overreach: How China derailed its peaceful rise*. Oxford University Press.

State Council of China. (2023). *Xi Jinping kanwang canjia zhengxie huiyi de minjian gongshanglian jie weiyuan shi qiangdiao: zhengque yindao minying jingji jiankang fazhan, gao zhiliang fazhan*. https://www.gov.cn/xinwen/2023-03/06/content_5745092.htm

Sullivan, J. (2021). *Remarks by National Security Advisor Jake Sullivan at the National Security Commission on Artificial Intelligence Global Emerging Technology Summit*. White House. https://bidenwhitehouse.archives.gov/nsc/briefing-room/2021/07/13/remarks-by-national-security-advisor-jake-sullivan-at-the-national-security-commission-on-artificial-intelligence-global-emerging-technology-summit

Tétrault-Farber, G., & Osborn, A. (2021, March 22). Russia's top diplomat starts China visit with call to reduce U.S. dollar use. *Reuters*. https://www.reuters.com/article/world/russias-top-diplomat-starts-china-visit-with-call-to-reduce-us-dollar-use-idUSKBN2BE0XG

Trump, D. (2017). *National security strategy of the United States*.

Trump, D. (2020). *Executive order on addressing the threat posed by TikTok*. https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok

US Department of Justice. (2021). *Information about the Department of Justice's China Initiative and a compilation of China-related prosecutions since 2018*. https://www.justice.gov/archives/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related

US Department of State. (n.d.). *Building a clean network: Key milestones*. https://2017-2021.state.gov/building-a-clean-network-key-milestones

Walker, J. (2021, July 30). How the Chinese government controls Tencent, the seventh largest company in the world. *Vision Times*. https://www.visiontimes.com/2021/07/30/how-the-chinese-government-controls-tencent-the-seventh-largest-company-in-the-world.html

Wang Yi tong eluosi waizhang juxing huitan [Wang Yi holds talks with Russian Foreign Minister Lavrov]. (2021, March 23). *Xinhua*. https://www.xinhuanet.com/world/2021-03/23/c_1127246950.htm

White House. (2023). *National cybersecurity strategy*.

Wright, N. (2018, July 10). How artificial intelligence will reshape the global order: The coming competition between digital authoritarianism and liberal democracy. *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order

Xi Jinping: Shishi guojia dashuju zhanlue jiakuai jianshe shuzi zhongguo. (2017, December 9). *Xinhua*. http://www.xinhuanet.com//politics/2017-12/09/c_1122084706.htm

Xi Jinping zai dier jie shijie hulianwang dahui kaimu shi shang de jianghua (quanwen). (2015, December 16). *Xinhua*. http://www.xinhuanet.com//politics/2015-12/16/c_1117481089.htm

Xi Jinping zai zhongyang zhengzhiju di shiba ci jiti xuexi shi qiangdiao ba qukuailian zuowei hexin jishu zizhu chuangxin zhongyao tupo kou, jiakuai tuidong qukuailian jishu he chanye chuangxin fazhan. (2019, October 25). *Xinhua*. https://www.xinhuanet.com/politics/2019-10/25/c_1125153665.htm

Xuezhe jiedu: Zhongguo chutai wangluo anquan shencha zhidu sida jiaodian. (2014, May 23). *CCP News Network*. http://theory.people.com.cn/n/2014/0523/c40531-25054345.html

Yang, D. (2018). *Zhengzhi anquan shi guojia anquan de genben*. Ministry of National Defense of the People's Republic of China. http://www.mod.gov.cn/gfbw/jmsd/4809950.html

Zhang, Y. (2023). Strategic vigilance: Mao's 'anti-peaceful evolution' strategy and China's policy toward the United States. *Journal of Cold War Studies*, *25*(2), 93–111.

About the Author

Ziyuan Wang (also professionally known as William Z. Y. Wang) is an associate professor at the Institute of International Relations, China Foreign Affairs University. He completed his PhD at the London School of Economics and Political Science. His research interests include international relations theory, political psychology, China's security environments, and international history. His academic works are published in *International Security*, *Journal of Chinese Political Science*, and *Chinese Journal of International Politics*, along with several leading Chinese journals.