

U.S.–China Digital Diplomacy and Global Security: An Assessment of Emerging Cybersecurity and Strategic Competition, 2010–2022

Dr. Joseph Ezekiel Obuje

Department of History and International Studies, Federal University of Lafia

Dr. Iortyer Philip Terna

Department of History and International Studies, Federal University of Lafia

Kolawole Michael Oladipupo

Department of History and International Studies, Federal University of Lafia

Abstract: This study examines U.S.–China digital diplomacy and its implications for global security between 2010 and 2025, with particular attention to the intersection of cybersecurity, technological competition, diplomatic engagement, and the changing structure of international power. The study situates the growing digital rivalry between the United States and China within broader transformations in global politics, where cyberspace, artificial intelligence, 5G networks, semiconductor technologies, digital infrastructure, and data governance have become important instruments of state power. Drawing on the realist, liberal institutionalist, and constructivist perspectives, the study analyses the competing interests, institutional constraints, identities, norms, and perceptions that have shaped U.S.–China digital relations. From a realist perspective, cyberspace constitutes an arena of strategic competition in which both powers seek technological advantages, cybersecurity capabilities, and influence over emerging digital infrastructures. The liberal institutional approach highlights the limitations and possibilities of international cooperation in establishing rules and mechanisms for responsible state behaviour in cyberspace. The constructivist perspective, meanwhile, demonstrates how competing national identities, threat perceptions, technological narratives, and interpretations of appropriate cyber behaviour influence bilateral relations. The study further examines the implications of digital rivalry for the global security architecture, including strategic stability, international norms, technological governance, and the prospects for cooperation. It argues that although U.S.–China digital competition has intensified geopolitical tensions, sustained diplomatic engagement, confidence-building measures, institutional dialogue, and mutually accepted norms remain important avenues for reducing miscalculation and promoting strategic stability in cyberspace.

Keywords: Digital Diplomacy, Global Security, Cybersecurity, International Relations, Cyber Threats, Cyber Governance

Introduction

The rapid development of digital technologies has transformed the nature of international relations and security in the twenty-first century. Cyberspace has emerged as an arena of diplomacy, intelligence, economic competition and strategic rivalry, while technologies such as artificial intelligence, 5G, semiconductors and digital infrastructure have become increasingly important to

national power. Within this changing environment, the relationship between the United States and China represents one of the most significant dimensions of contemporary digital geopolitics [1]. Between 2010 and 2025, their relationship increasingly combined economic and technological interdependence with growing concerns over cyber espionage, data security, telecommunications infrastructure, technology transfers and strategic technological advantage.

U.S.–China digital relations have therefore developed beyond conventional technological cooperation into a broader contest over cybersecurity, technological leadership and influence over the emerging digital order. American restrictions on selected Chinese technologies and China's efforts to strengthen technological self-reliance illustrate the extent to which technology has become connected to national security and geopolitical competition [2]. At the same time, both countries have participated in diplomatic and international discussions aimed at addressing cyber threats and developing norms for responsible behaviour in cyberspace. This creates a central tension between strategic competition and the necessity for cooperation in managing shared digital risks [3].

This study examines the security implications of U.S.–China digital diplomacy from 2010 to 2025 through realist, liberal institutionalist and constructivist perspectives. It considers cyberspace as an arena of power politics, examines the possibilities and limitations of international cooperation, and analyses how competing identities, norms and perceptions have shaped bilateral relations. It further assesses the implications of this rivalry for global security architecture and considers opportunities for strategic stability through diplomacy, confidence-building and international norms [4].

Concept of Cybersecurity

According to Shashi Jayakumar, cyber security is defined as the comprehensive set of practices, frameworks, and preventive measures that are employed to protect both individual and institutional assets in the cyberspace.¹⁹ In his edited volume *Cybersecurity: Emerging Issues, Trends and Technologies*, he considers cyber security as a layered process that moves beyond technical mechanisms to involve behavioural awareness, institutional preparedness, and strategic policies. Jayakumar holds that the concept must be understood as more than “system defence”; rather, it is an ongoing process of anticipating threats and minimising vulnerabilities in societies that increasingly depend on digital interconnectivity [5].

National Security

Lawrence Freedman reconceptualises national security as a broad, adaptive practice that extends beyond the military to encompass the security of political, economic and informational domains. John Arquilla frames national security as the art of managing political-psychological effects as much as physical threats. Perception, morale and information flows are core security variables [6]. Arquilla's cyber-era interpretation centres the capacity of non-kinetic operations to produce strategic outcome

Cybersecurity Risks and Geopolitical Tensions

The intensification of U.S.–China digital diplomacy has placed cybersecurity at the centre of both bilateral relations and broader international security debates. Cyber threats are no longer confined to technical networks; they now have profound implications for political stability, economic competitiveness, and strategic deterrence. The United States perceives China's cyber capabilities as instruments of strategic leverage capable of undermining critical infrastructure, intellectual property systems, and national security institutions, ranging from defence to finance. China, conversely, regards U.S. cyber operations, global surveillance programmes, and alliances as deliberate efforts to contain its technological and strategic rise, shaping its cyber policy and digital diplomacy. This reciprocal perception of threat has transformed cyberspace into a contested

domain of geopolitical tension, where digital diplomacy is inseparable from national security considerations. Analysts note that the cyber domain is unique because it enables high-impact, low-cost operations that can influence both domestic and foreign political landscapes, making traditional diplomatic approaches inadequate for conflict prevention. The early cooperative mechanisms established in bilateral dialogues now exist alongside heightened suspicion, demonstrating that cybersecurity has become a structural component of U.S.–China strategic rivalry rather than merely a technical issue [7], [8].

A critical driver of these tensions has been the proliferation of state-sponsored cyber operations, targeting government networks, private corporations, and strategic infrastructure. Both states have increasingly accused one another of espionage, intellectual property theft, and digital sabotage. While each nation frames these operations as defensive, the opposing side interprets them as aggressive acts designed to weaken its technological and economic base [9]. The asymmetric nature of cyber threats which allows small-scale actors to generate disproportionate effects complicates deterrence strategies, making traditional security paradigms less effective. This environment has produced a form of strategic ambiguity in which both the United States and China engage in signalling and counter-signalling, using cyber incidents to demonstrate capabilities without triggering open conflict. In this context, digital diplomacy functions not merely as communication but as a venue for managing tension, negotiating norms, and signalling national resolve to both domestic and international audiences.

Critical infrastructure vulnerabilities have intensified the security dilemma. Telecommunications networks, financial systems, transport logistics, and power grids are increasingly interconnected, creating high-value targets for cyber disruption. The United States has prioritised securing these infrastructures through regulatory frameworks, partnerships between government and private sector, and international cooperation agreements. China, for its part, has focused on network resilience, indigenous technology development, and legal measures to assert state control over critical systems. These contrasting approaches reveal divergent governance philosophies: the

United States emphasises transparency, accountability, and multistakeholder engagement, whereas China prioritises state oversight, sovereignty, and technological self-reliance. These differences exacerbate mistrust in digital diplomacy, making coordination on security protocols challenging. Consequently, both nations must navigate a delicate balance between competition, collaboration, and risk management, illustrating that cybersecurity considerations now fundamentally shape diplomatic interactions [10].

The internationalisation of cyber norms has become another source of friction. While both the United States and China participate in forums such as the United Nations Group of Governmental Experts on Information and Telecommunications in the Context of International Security, their normative objectives diverge sharply. The U.S. promotes open, transparent, and accountable governance of cyberspace, framing cyber threats in terms of law, ethics, and international security obligations. China, in contrast, emphasises cyber sovereignty, control over domestic information flows, and the development of an independent digital ecosystem aligned with state interests. This normative competition shapes bilateral negotiations and creates tensions in multilateral diplomacy, as each power seeks to establish global standards reflecting its own strategic and political preferences. Digital diplomacy thus becomes not only a tool for managing disputes but also a mechanism for projecting national values and shaping international norms.

Methodology

Emerging technologies have further complicated the security environment. Artificial intelligence, quantum communication, cloud computing, and advanced encryption technologies provide unprecedented intelligence, surveillance, and operational capabilities, but also introduce vulnerabilities. Both countries integrate these tools into defence and intelligence planning, with AI-driven cyber operations, algorithmic threat detection, and secure communication networks becoming central to national security. The dual-use nature of these technologies blurs the line between civilian and military applications, creating grey zones in which digital diplomacy must negotiate both technical cooperation and strategic competition. Analysts argue that this integration of emerging technologies into national security architecture elevates the stakes of digital diplomacy, transforming it from a conventional diplomatic instrument into a high-stakes arena of strategic signalling.

Regional and global alliances have amplified cybersecurity tensions. The United States coordinates with NATO, the Quad, and the Five Eyes alliance to strengthen cyber defence, share threat intelligence, and develop collective deterrence strategies. China, simultaneously, promotes its Digital Silk Road and regional cybersecurity initiatives, aiming to extend influence and provide alternative technological standards to developing nations. These initiatives reflect a broader struggle for strategic influence, demonstrating that digital diplomacy is no longer bilateral but increasingly multilateral, with implications for regional security architecture and global governance. The contest for influence highlights the intersection of technology, diplomacy, and strategic competition in shaping the modern international system.

Cybersecurity risks in U.S.–China digital diplomacy have had profound and multi-layered implications. They transform cyberspace from a technical domain into a geopolitical arena in which technology, strategy, and diplomacy intersect. Mutual perceptions of threat, combined with normative divergence and technological competition, have created persistent tensions that challenge traditional diplomatic mechanisms. Understanding these dynamics is critical, as cybersecurity considerations now underpin not only bilateral relations but also regional and global security frameworks. The evolution of digital diplomacy reflects this complex interplay between technology, power, and strategy, establishing cyberspace as a central theatre of 21st-century international relations.

Digital Espionage and Strategic Intelligence Competition

Digital espionage has become a defining feature of U.S.–China relations in the digital age, reflecting the strategic value of information in contemporary power politics. As both states increasingly rely on digital networks for governance, defence, and economic activity, cyberspace has emerged as a critical arena for intelligence gathering. The United States views Chinese cyber espionage as a systematic effort to acquire sensitive military, technological, and commercial information, thereby accelerating China's strategic and economic advancement. China, in contrast, perceives U.S. cyber intelligence operations as part of a broader surveillance architecture designed to maintain American global dominance. This mutual suspicion has transformed digital diplomacy into a space where intelligence competition is both implicit and explicit, shaping bilateral engagements and strategic communication.

The scale and scope of digital espionage distinguish it from traditional intelligence practices. Cyber operations enable persistent access to networks, allowing states to collect vast quantities of data without physical presence. For the United States, the protection of intellectual property and classified information has become a central security concern, influencing diplomatic pressure, sanctions, and indictments against Chinese actors. China rejects these accusations, arguing that cyber espionage is a common practice among major powers and highlighting revelations of

extensive U.S. global surveillance. This exchange of accusations illustrates how digital espionage has eroded trust and complicated diplomatic efforts aimed at stabilising cyber relations.

Strategic intelligence competition is further intensified by the integration of digital technologies into military planning. Cyber espionage now supports broader strategic objectives, including military modernisation, force readiness, and strategic deterrence. Both states seek to exploit digital vulnerabilities to gain insights into command structures, weapons systems, and defence planning. The intelligence value of cyber operations makes restraint difficult, as the perceived costs of non-engagement often outweigh diplomatic risks. Consequently, digital diplomacy increasingly functions as a mechanism for managing escalation rather than preventing espionage itself.

The legal and normative ambiguity surrounding cyber espionage exacerbates tensions. Unlike conventional warfare, international law offers limited clarity on acceptable behaviour in cyberspace. The United States attempts to draw distinctions between legitimate intelligence gathering and cyber-enabled theft of commercial secrets, while China disputes such categorisations. These disagreements hinder the development of shared norms and weaken multilateral efforts to regulate cyber behaviour. As a result, intelligence competition persists within a fragmented normative environment, reinforcing adversarial digital diplomacy.

Emerging technologies have further enhanced the effectiveness of digital espionage. Artificial intelligence, big data analytics, and machine learning allow intelligence agencies to process enormous volumes of information, increasing the strategic value of cyber intrusions. Both states invest heavily in these capabilities, recognising their potential to reshape intelligence competition. This technological acceleration heightens insecurity, as advances by one side generate pressure for countermeasures by the other, deepening the security dilemma within digital diplomacy.

Digital espionage also extends beyond bilateral relations, affecting alliances and global security networks. The United States shares intelligence with allies through established frameworks, reinforcing collective security but also amplifying tensions with China. China, meanwhile, expands intelligence cooperation with strategic partners and enhances its global digital presence through infrastructure projects. These dynamics internationalise the intelligence competition, embedding it within broader geopolitical rivalries.

The development on digital espionage and strategic intelligence competition have become entrenched features of U.S.–China digital diplomacy. They reflect the centrality of information to modern power and underscore the limitations of existing diplomatic and legal frameworks. As intelligence competition intensifies, managing its security implications remains a critical challenge for bilateral relations and global stability.

Result and Discussion

Threats to Global Trade, Technology, and Infrastructure

The escalation of U.S.–China digital diplomacy has generated significant security implications for global trade, particularly as digital technologies become embedded in international economic systems. Digital platforms, cross-border data flows, and technology-driven supply chains now underpin global commerce, making them vulnerable to geopolitical disruption. The United States increasingly frames China's digital expansion as a threat to fair trade, economic transparency, and technological security, while China views U.S. restrictions as attempts to undermine its economic development and global competitiveness. This mutual suspicion has contributed to a securitisation of trade relations, where economic exchanges are assessed through national security lenses. Consequently, digital diplomacy has become a critical arena for negotiating, contesting, and redefining the rules governing global trade in the digital era [11].

Technology restrictions and export controls represent one of the most visible manifestations of this threat environment. The United States has imposed limits on the transfer of advanced semiconductors, artificial intelligence components, and sensitive software to China, citing national security concerns. These measures aim to preserve technological superiority and prevent potential military applications. China, in response, has accelerated efforts to develop indigenous technologies and reduce reliance on foreign suppliers. This reciprocal strategy has disrupted global technology markets, creating uncertainty for multinational corporations and weakening established supply chains. Digital diplomacy thus increasingly functions as an instrument for enforcing economic security objectives rather than facilitating open trade [12].

Digital infrastructure has also emerged as a focal point of strategic concern. Global telecommunications networks, undersea cables, data centres, and cloud services form the backbone of the modern economy. The United States warns that Chinese involvement in such infrastructure poses risks of surveillance, data manipulation, and strategic dependency. China rejects these claims, arguing that infrastructure development is driven by commercial logic and mutual benefit. This disagreement has fragmented global infrastructure development, forcing states to choose between competing technological ecosystems [13]. As a result, digital diplomacy shapes not only bilateral relations but also the structure of global connectivity.

The fragmentation of technology standards further threatens global economic stability. Competing approaches to data governance, cybersecurity regulation, and technical standards have emerged, reflecting broader ideological and strategic divides. The United States promotes open standards and market-driven innovation, while China advances state-led models and alternative governance frameworks. This divergence complicates interoperability, increases costs, and reduces efficiency in global trade. Digital diplomacy becomes a battleground for standard-setting, with long-term implications for economic integration and technological diffusion [14].

Global trade is also affected by the politicisation of digital platforms and digital services. Restrictions on technology firms, investment screening, and digital market access have become tools of strategic competition. These measures undermine trust in the neutrality of global markets and create an environment of uncertainty for international business. The digital economy, once seen as a driver of globalisation, increasingly reflects geopolitical fragmentation shaped by U.S.–China rivalry [15].

Developing countries are particularly vulnerable to these dynamics. As recipients of digital infrastructure investment and technology transfer, they face pressure to align with one side or the other. This alignment influences access to markets, financing, and technological ecosystems, reinforcing dependency and limiting strategic autonomy. Digital diplomacy thus has unequal consequences, reshaping global economic hierarchies and patterns of development. Security implications in the U.S.–China digital diplomacy extend deeply into global trade, technology, and infrastructure. Strategic competition disrupts supply chains, fragments standards, and politicises economic engagement. Understanding these threats is essential for assessing the broader impact of digital diplomacy on global economic stability and international security [16], [17].

Implications for Regional Security in Asia-Pacific

The Asia-Pacific region occupies a central position in the security implications of U.S.–China digital diplomacy due to its strategic importance and high level of technological interdependence.

As both powers intensify digital engagement and competition, regional states increasingly experience security pressures linked to cybersecurity, digital infrastructure, and technological alignment. The United States frames its digital diplomacy in the region around safeguarding open networks, protecting data integrity, and countering perceived Chinese cyber influence. China, in contrast, promotes digital cooperation initiatives that emphasise sovereignty, development, and

non-interference [18]. These competing narratives shape regional security environments, transforming digital connectivity into a critical dimension of strategic rivalry.

Cybersecurity concerns represent a major source of regional tension. Asia-Pacific states are frequent targets of cyber intrusions, disinformation campaigns, and digital espionage, often linked to broader U.S.–China rivalry. As regional governments digitise public services and defence systems, vulnerabilities increase, raising fears of external manipulation and strategic coercion. Digital diplomacy thus becomes intertwined with national security planning, as states seek assistance, partnerships, and capacity-building from either Washington or Beijing. This alignment deepens regional polarisation and complicates efforts to maintain strategic autonomy.

Digital infrastructure development further influences regional security dynamics. Telecommunications networks, smart ports, and data centres funded or supported by either the United States or China are often perceived as strategic assets. U.S. concerns about Chinese technology providers have led to pressure on allies to exclude certain firms from critical infrastructure projects [19], [20]. China, meanwhile, views such exclusions as discriminatory and destabilising. These disputes extend beyond economics, affecting military interoperability, intelligence sharing, and crisis management across the region.

Technology standards and governance frameworks also shape Asia-Pacific security outcomes. Divergent approaches to data governance, surveillance, and digital regulation reflect broader ideological divides. States adopting Chinese digital governance models may prioritise state control and cybersecurity sovereignty, while those aligned with U.S. frameworks emphasise transparency and private-sector innovation. The coexistence of these models creates regulatory fragmentation, undermining regional cooperation and increasing the risk of digital miscommunication during crises.

The implications for regional alliances and partnerships are equally significant. U.S.-led initiatives such as the Quad and AUKUS increasingly incorporate digital security components, including cyber defence and emerging technologies. These arrangements are perceived by China as containment strategies, prompting counter-initiatives and diplomatic resistance. Digital diplomacy thus reinforces alliance politics, heightening security dilemmas and reducing trust among regional actors [21].

Smaller Asia-Pacific states face particular challenges navigating this environment. Balancing economic ties with China and security partnerships with the United States requires careful diplomatic calibration. Digital infrastructure choices, cybersecurity partnerships, and regulatory alignment carry long-term security consequences. Failure to manage these pressures risks entrenching dependency and exposing states to strategic vulnerability.

In essence, U.S.–China digital diplomacy has transformed the Asia-Pacific into a key theatre of digital security competition. Cyber risks, infrastructure disputes, and technological alignment increasingly shape regional stability. These dynamics underscore the need for inclusive security frameworks capable of mitigating digital tensions while preserving regional autonomy [22].

Challenges for International Cooperation and Multilateral Security

The intensifying digital diplomacy rivalry between the United States and China poses profound challenges for international cooperation and multilateral security frameworks. Digital technologies, once viewed as neutral tools for global connectivity, have become instruments of strategic competition, undermining trust within international institutions. The United States promotes a rules-based digital order grounded in transparency, accountability, and liberal norms, while China advances alternative governance models emphasising digital sovereignty and state-led control. These competing visions create normative fragmentation, weakening the ability of multilateral organisations to formulate coherent and universally accepted security standards in cyberspace.

One major challenge lies in the absence of shared norms governing state behaviour in the digital domain. Despite efforts by the United Nations Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG), consensus on issues such as cyber espionage, digital interference, and critical infrastructure protection remains limited. U.S.–China disagreements over attribution, accountability, and enforcement mechanisms obstruct meaningful progress. As a result, cyberspace remains largely unregulated, increasing the risk of miscalculation and escalation during periods of political tension.

Multilateral security institutions also struggle with institutional paralysis caused by great-power rivalry. Forums such as the United Nations, the World Trade Organization, and the International Telecommunication Union increasingly reflect geopolitical divisions rather than cooperative problem-solving. Competing diplomatic pressure from Washington and Beijing often forces smaller states to take sides, eroding the neutrality and effectiveness of these institutions. This dynamic undermines collective security efforts and weakens global governance mechanisms designed to manage transnational digital threats.

Trust deficits further complicate international cooperation. Persistent allegations of cyber espionage, intellectual property theft, and digital surveillance have fostered suspicion between major powers and their allies. Confidence-building measures, such as information sharing and joint cyber exercises, remain limited due to fears of exposing strategic vulnerabilities. Without trust, multilateral security arrangements lack credibility, rendering them ineffective in preventing or managing digital conflicts.

Economic and technological decoupling exacerbates these challenges. U.S.-led restrictions on technology transfer and China's pursuit of technological self-reliance fragment global supply chains and standards. Multilateral cooperation on emerging technologies such as artificial intelligence, quantum computing, and cybersecurity becomes increasingly difficult when rival blocs pursue incompatible regulatory frameworks. This fragmentation weakens collective responses to shared security threats, including cybercrime and digital terrorism.

Developing countries face disproportionate challenges within this fragmented system. Many lack the capacity to influence global digital governance yet bear the consequences of regulatory divergence and security vulnerabilities. Dependence on external digital infrastructure and expertise exposes them to strategic pressure, limiting their ability to pursue independent security policies. Multilateral mechanisms intended to support capacity-building are often constrained by geopolitical competition and funding disparities.

This construct that U.S.–China digital diplomacy has reshaped the landscape of international security cooperation. Competing norms, weakened institutions, and eroding trust challenge the effectiveness of multilateral responses to digital threats. Addressing these challenges requires renewed commitment to inclusive dialogue, confidence-building, and norm development beyond zero-sum competition. Without such efforts, multilateral security frameworks risk becoming casualties of digital geopolitical rivalry.

CONCLUSION

U.S.–China digital diplomacy between 2010 and 2025 demonstrates that cyberspace has become an important arena of great-power competition and global security. Technological capabilities in areas such as artificial intelligence, semiconductors, telecommunications and cyber operations have increasingly become instruments of national power. From a realist perspective, the rivalry reflects the pursuit of strategic advantage and the protection of national security interests. The liberal institutional perspective, however, shows that the transnational character of cyber threats makes cooperation and diplomatic engagement necessary despite persistent strategic distrust.

The constructivist perspective further demonstrates that U.S.–China digital competition is shaped by differing perceptions, identities and interpretations of appropriate behaviour in cyberspace. These differences have contributed to mutual suspicion and competing approaches to digital governance. Consequently, the rivalry has implications beyond the two countries, affecting technological standards, digital infrastructure, supply chains and the wider global security architecture. The study concludes that U.S.–China digital competition is likely to remain an important feature of international politics, but competition does not necessarily preclude cooperation. Diplomatic dialogue, confidence-building measures, crisis communication and internationally accepted norms can help manage areas of disagreement and reduce the possibility of escalation. The challenge for global security is therefore to develop mechanisms capable of balancing technological competition with sufficient cooperation to maintain stability in an increasingly digital international system.

References

- [1] J. S. Nye, Jr., *The Future of Power*. New York, NY, USA: PublicAffairs, 2011, p. 115. wcfia.harvard.edu
- [2] S. Sacks, “China’s Digital Silk Road and the global order,” Council on Foreign Relations, 2021, p. 21.
- [3] N. Inkster, “The U.S.–China technology competition,” International Institute for Strategic Studies (IISS), London, U.K., 2020, p. 21.
- [4] A. Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York, NY, USA: PublicAffairs, 2016, pp. 33, 102. [CFR](http://www.cfr.org)
- [5] S. Jayakumar, Ed., *Cybersecurity: Emerging Issues, Trends and Technologies*. Singapore: Palgrave Macmillan, p. 12.
- [6] L. Freedman, *Security: A New Framework for the 21st Century*. London, U.K.: Hurst, 2020, p. 22.
- [7] J. Arquilla, *The New Tools of War: Information as Power in the 21st Century*. New York, NY, USA: Oxford University Press, 2021, p. 47.
- [8] J. S. Nye, Jr., “Cyber power and global strategy,” p. 43.
- [9] L. Kello, *The Virtual Weapon and International Order*. New Haven, CT, USA: Yale University Press, 2017, p. 88. [Yale University Press](http://www.yaleupress.edu)
- [10] United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Report*. New York, NY, USA: United Nations, 2021, p. 12.
- [11] H. Farrell and A. L. Newman, *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*. New York, NY, USA: Columbia University Press, 2023, p. 127.
- [12] J. E. Hillman, *The Digital Silk Road: China’s Quest to Wire the World and Win the Future*. New York, NY, USA: Harper Business, 2021, pp. 41, 63.
- [13] D. Shambaugh, *China and the World: Security, Technology, and Diplomacy*. Oxford, U.K.: Oxford University Press, 2022, p. 210.
- [14] T. Rid, *Cyber War Will Not Take Place*. Oxford, U.K.: Oxford University Press, 2013, p. 146.
- [15] M. N. Schmitt, “International law in cyberspace,” *Harvard National Security Journal*, vol. 7, 2016, p. 15.
- [16] C. P. Bown, “U.S.–China technology controls and global trade,” Peterson Institute for International Economics, Policy Brief, 2021, p. 18.
- [17] T. Wu, *The Curse of Bigness: Antitrust in the New Gilded Age*. New York, NY, USA: Columbia Global Reports, 2018, p. 92.
- [18] J. Zeng, *China’s Digital Diplomacy and Global Governance*. London, U.K.: Routledge, 2021, p. 88.
- [19] G. Allison, *Destined for War: Can America and China Escape Thucydides’s Trap?* Boston, MA, USA: Houghton Mifflin Harcourt, 2017, p. 213.

- [20] R. Medcalf, *Indo-Pacific Empire: China, America and the Contest for the World's Pivotal Region*. Manchester, U.K.: Manchester University Press, 2020, p. 201.
- [21] E. Goh, "Great power competition and Southeast Asian security," *International Affairs*, vol. 95, no. 4, p. 835, 2019.
- [22] J. Healey, *The Five Futures of Cyber Conflict and Cooperation*. Washington, DC, USA: Atlantic Council, 2022, p. 63.