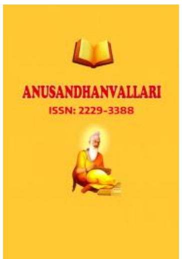

Anusandhanvallari
Vol 2025, No.1
September 2025

ISSN 2229-3388

Digital Battlegrounds: Cybersecurity, Espionage, and the High-Stakes Rivalry Between the US and China

Ishita Tripathi[1*], Prof. (Dr.) S.S Bindra[2]
[1]PhD scholar, Department of Amity Institute of International Relations, Amity University, Noida, Uttar Pradesh, India
*Corresponding Email Id: ishitatripathi397@gmail.com
ORCID ID: https://orcid.org/0009-0002-6826-1189
[2]Director Research, Amity Institute of International Relations, Amity University, Noida, Uttar Pradesh, India
Email: bindrasukhwant@gmail.com
ORCID ID:0009-0003-0664-7569

Abstract: Over the past decade, cyberspace has become a decisive arena of strategic rivalry, reshaping both the practice and the theory of international relations. What began as episodic intrusions aimed at stealing intellectual property has evolved into a sustained contest over critical infrastructure, technological innovation, and the future of global governance. The United States and China stand at the centre of this transformation. Through a series of high-profile cases—including the Equifax breach (2017), the Microsoft Exchange server compromise (2021), and the exposure of the Volt Typhoon campaign (2023–2024)—cyber operations have steadily escalated in scope and ambition.

This study adopts a qualitative approach, combining historical analysis, case study evaluation, and policy review, to examine the trajectory of Sino–U.S. cyber relations from 2017 to 2025. It highlights not only the tactics and strategies employed by both states but also the broader implications of these confrontations for global stability. The analysis suggests that while cyber conflict has deepened bilateral mistrust, it has simultaneously spurred the development of new mechanisms for resilience, the expansion of multilateral attribution practices, and the gradual articulation of emerging norms in cyberspace.

The paper concludes that cyber rivalry is no longer a subsidiary aspect of great-power politics but a structuring force of the international order. The manner in which Washington and Beijing navigate this domain will profoundly influence the balance between competition and cooperation in global affairs over the coming decades.

Keywords: *Cybersecurity; Cyber espionage; U.S.–China relations; Strategic rivalry; Digital governance; Critical infrastructure; Cyber sovereignty; International order]*

INTRODUCTION

Over the past decade, cyberspace has ceased to be a peripheral concern of policymakers and has instead become one of the principal stages upon which great-power rivalries unfold. Unlike the more traditional domains of land, sea, or air, the cyber domain is both invisible and omnipresent, linking national economies, defence systems, and societies in ways that blur the lines between civilian and military targets. For the United States and China, cyberspace is no longer simply a technical space but a strategic battleground. In Washington, the fear of a "cyber Pearl Harbor," as articulated by former U.S. Secretary of Defence Leon Panetta, continues to shape perceptions of vulnerability. More recently, FBI Director Christopher Wray (2024) warned that Chinese hackers were "preparing to cripple American critical infrastructure at a moment's notice." From Beijing's side, President Xi Jinping has emphasized that "without cybersecurity, there is no national security; without informatization, there is no modernization," underscoring the centrality of digital power to China's rise.

Two theoretical perspectives in International Relations help illuminate this contest: Realism and Constructivism. A Realist reading of Sino–U.S. cyber rivalry views it as the natural extension of power politics into a new domain.

States, operating in an anarchic system, pursue every available advantage, and the digital sphere is no exception. China's repeated involvement in intellectual property theft, from the Equifax breach in 2017 to the Volt Typhoon campaign (2023–2024), reflects an effort to accelerate its technological development and reduce strategic dependence on foreign powers. The United States, in turn, has responded with indictments of Chinese military hackers, sanctions against technology firms such as Huawei, and the strengthening of cyber defences through U.S. Cyber Command. From this perspective, cyberspace is simply another theatre in which the logic of survival and relative gains prevails.

Constructivist theory, however, highlights dimensions that Realism alone cannot explain. Cyberspace is not only contested because of material advantage but also because of competing ideas about what it should be. The United States promotes an open and interoperable internet, one that underpins trade, innovation, and the global flow of information. China, by contrast, has advanced the concept of "cyber sovereignty," which legitimizes strict state control over digital infrastructure, surveillance of content, and a domestically bounded internet. These competing visions have become embedded in foreign policy positions and diplomatic alignments: while Washington rallies allies behind voluntary norms discouraging attacks on civilian infrastructure, Beijing, often with Russian support, pushes for legally binding codes of conduct that emphasize state control.

The clash, therefore, is not only over capabilities but also over identity and legitimacy. For China, defending cyber sovereignty is part of a broader narrative of resisting Western dominance and asserting its path to modernization. For the United States, securing cyberspace is inseparable from its role as a guarantor of the liberal international order. As Joseph Nye (2021) has argued, "cyber power both constrains and enables," creating paradoxical relationships of dependence even as it deepens mistrust. In this sense, Constructivism reminds us that cyberspace is a social and political construct, defined as much by the narratives and norms that surround it as by the technologies that underpin it.

This paper builds on these theoretical insights to analyse the trajectory of Sino–U.S. cyber conflict between 2017 and 2025. It examines the origins of key incidents, the strategies deployed to mitigate their consequences, and the broader impacts on bilateral relations and global governance. The central claim is that cyberspace is no longer a secondary aspect of international politics but a structuring force, one that will significantly shape whether the future world order tilts toward confrontation, fragmentation, or limited cooperation.

METHODOLOGY

This study adopts a qualitative, case-study research design to analyse the trajectory of Sino–U.S. cyber relations between 2017 and 2025**.** The time frame was chosen to capture the first Trump administration, during which cyber issues rose to the forefront of bilateral tensions, through to the present period of entrenched rivalry. The analysis is framed through two dominant International Relations theories: Realism and Constructivism. Realism is used to explain the pursuit of strategic advantage and balancing behaviours, while Constructivism highlights the role of identity, norms, and competing narratives such as "cyber sovereignty" versus an "open internet." This dual-theoretical approach allows the study to capture both the material power dynamics and the ideational contestations inherent in cyber politics.

1. **Historical-Comparative Analysis**: Examines the evolution of U.S.–China cyber relations since the late 1990s, tracing escalation from small-scale intrusions to state-backed systemic operations (Rid & Buchanan, 2015).
2. **Case Study Approach**: Analyses key incidents—Operation Aurora (2009–10), OPM breach (2014), Equifax breach (2017), and Microsoft Exchange hack (2021)—to understand tools, perpetrators, and strategic outcomes (Fruhlinger, 2020b; Ng, 2018).

3. **Policy and Discourse Analysis**: Evaluates legal and institutional frameworks such as the U.S. Computer Fraud and Abuse Act, Cybersecurity and Infrastructure Security Agency (CISA, 2018), and the 2015 U.S.–China Cybersecurity Agreement (U.S. Office of Personnel Management, 2015).
4. **Secondary Literature Review**: Draws upon international relations theories—particularly realism and technological determinism—to contextualize cyber rivalry in broader geopolitics (Allison, 2017; Nye, 2010).

Research Questions

The paper is guided by three central questions:

1. How have major cyber incidents between 2017 and 2025 shaped the strategic competition between the United States and China?
2. What tactics and policy responses have been adopted to mitigate the effects of these incidents, both domestically and internationally?
3. How do competing narratives and norms influence the broader implications of cyber conflict for global governance?

Background and Origins of Cyber Conflicts

Titan Rain (2003–2005): The First Wave of Systematic Cyber Espionage

Between 2003 and 2005, a series of sustained cyber intrusions known as Titan Rain targeted U.S. government agencies, defence contractors, and research institutions. The attacks, widely attributed to hackers affiliated with the Chinese military, exfiltrated sensitive files from organizations such as NASA, Lockheed Martin, and Sandia National Laboratories (Segal, 2017). Unlike earlier, sporadic intrusions, Titan Rain demonstrated a systematic and long-term approach to cyber espionage.

Analysts argue that the campaign served dual purposes: securing intellectual property and advancing China's military modernization. The theft of defence schematics, for example, allowed China to bypass years of costly research and development (Rid & Buchanan, 2015). While the Chinese government denied involvement, cybersecurity experts noted that the sophistication and persistence of the attacks suggested state sponsorship. The episode marked the first time the U.S. recognized cyberspace as a strategic battleground rather than a mere criminal arena.

Operation Aurora (2009–2010): Corporate Intrusions and Strategic Leverage

In 2009–2010, Operation Aurora shook the private sector when hackers linked to China's People's Liberation Army Unit 61398 infiltrated more than 30 American corporations, including Google, Adobe, Morgan Stanley, and Dow Chemical (Council on Foreign Relations, 2010). The attackers exploited Internet Explorer vulnerabilities, gaining access to intellectual property, source codes, and confidential communications.

The most high-profile target was Google. The breach exposed Gmail accounts of Chinese human rights activists, forcing the company to publicly accuse China and reconsider its operations in the Chinese market (Segal, 2017). Google's subsequent decision to relocate its search engine operations to Hong Kong symbolized the intersection of cybersecurity, corporate governance, and human rights. Aurora thus highlighted how cyber operations could not only damage economic assets but also influence corporate geopolitics.

Office of Personnel Management (OPM) Breach (2014): Data as a Weapon

The 2014 breach of the U.S. Office of Personnel Management (OPM) stands as one of the most damaging cyber incidents in history. Hackers, allegedly working for Chinese intelligence, accessed records of more than 21 million current and former U.S. federal employees, including sensitive background investigation forms, health data, and fingerprints (Fruhlinger, 2020a).

This breach differed from earlier cases because it weaponized **personnel data** rather than corporate secrets. Security experts warned that the database could be used to construct detailed psychological and financial profiles of U.S. officials, aiding recruitment of informants or enabling coercion (Miller, 2016). Former NSA Director Michael Hayden called the breach a "tremendous intelligence success for the Chinese" (as cited in Sanger, 2016).

The OPM hack triggered massive reforms in U.S. federal cybersecurity, including billions in funding for IT modernization and stricter vetting of contractors. It also deepened the trust deficit in U.S.–China relations, particularly since it occurred just before the 2015 Obama–Xi Cybersecurity Agreement.

Equifax Breach (2017): Blurring Economic and National Security

In March 2017, hackers linked to China's People's Liberation Army exploited a vulnerability in Apache Struts to breach Equifax, one of the largest U.S. credit reporting agencies (Ng, 2018). The attackers stole personal and financial data of approximately 145 million Americans, including Social Security numbers, birth dates, and credit histories (Fruhlinger, 2020b).

Unlike earlier espionage cases that focused on government data, the Equifax breach blurred boundaries between economic espionage and national security. Financial data could be leveraged for both strategic and coercive purposes—ranging from identity theft to mapping the financial networks of key officials. In 2020, the U.S. Department of Justice formally indicted four Chinese military officers for the breach, underscoring its attribution to state-backed actors (U.S. DOJ, 2020).

The incident generated public outrage, congressional hearings, and stricter regulations for consumer data protection. It also demonstrated that cyber espionage was no longer confined to traditional state secrets but extended into the everyday lives of citizens.

Microsoft Exchange Hack (2021): Global-Scale Vulnerabilities

In early 2021, the hacking group Hafnium, allegedly affiliated with China, exploited four zero-day vulnerabilities in Microsoft Exchange servers. The campaign compromised tens of thousands of organizations globally—including small businesses, municipalities, and non-profits—by allowing hackers to access email systems and install backdoors (Sanger & Perlroth, 2021).

What distinguished this attack was its scale and collateral damage. While earlier operations were targeted, the Exchange hack spread indiscriminately, creating a global cybersecurity crisis. The Biden administration formally attributed the attack to China and rallied allies—including the European Union, NATO, and Five Eyes partners—in a coordinated condemnation (U.S. White House, 2021).

This marked one of the first instances of collective attribution in cyberspace, setting a precedent for multilateral responses to state-sponsored attacks. It also highlighted the fragility of widely used software infrastructure and the urgent need for global cyber norms.

Mitigation Strategies and Their Global Impact

The evolution of U.S.–China cyber rivalry has not only revealed the vulnerabilities of digital infrastructures but has also catalysed the development of sophisticated mitigation strategies. These responses—ranging from technological fixes to diplomatic initiatives—have shaped national policies, corporate practices, and international norms. Examining how the United States and its partners responded to major cyber incidents such as Titan Rain, Operation Aurora, the Office of Personnel Management (OPM) breach, the Equifax breach, and the Microsoft Exchange hack provides insight into the broader trajectory of global cyber governance.

Institutionalization of Cyber Defence

The early intrusions of Titan Rain (2003–2005) underscored the need for a dedicated national cyber defence structure. While the immediate response involved technical measures such as intrusion detection systems and patch management, the longer-term impact was the establishment of U.S. Cyber Command (USCYBERCOM) in 2009 (Segal, 2017). This institutionalization marked a turning point: cyberspace was formally recognized as a distinct domain of warfare alongside land, sea, air, and space. The ripple effect was global, as other countries—including China, Russia, and members of NATO—expanded their own cyber units, fuelling a cyber arms race.

Public-Private Partnerships and Corporate Resilience

The Operation Aurora (2009–2010) attacks revealed the vulnerability of private corporations, particularly in sectors critical to national security. Google's decision to publicly attribute the attack to China and partially withdraw from the Chinese market represented a landmark in corporate transparency (Council on Foreign Relations, 2010). This set a precedent for the disclosure of state-backed cyber intrusions, pushing companies to become stakeholders in national security. In response, the U.S. government enhanced public-private partnerships, launching programs such as Einstein and expanding intelligence-sharing with tech companies (Lindsay, 2015). Globally, Aurora elevated corporate cybersecurity from a compliance matter to a strategic imperative, influencing firms across Europe and Asia to invest heavily in threat intelligence and incident response capabilities.

Data as a National Security Asset

The OPM breach (2014) demonstrated that the theft of personal data could be as damaging as the theft of state secrets. The compromise of over 21 million personnel records, including fingerprints and background checks, forced the United States to modernize its federal IT infrastructure and reframe data protection as a national security concern(Fruhlinger, 2020a). The breach also triggered the 2015 Obama–Xi Cybersecurity Agreement, in which both sides pledged to refrain from state-backed cyber-enabled theft of intellectual property for commercial gain (Sanger, 2016). Although the agreement was criticized for weak enforcement, it established a template for bilateral cyber diplomacy. At the global level, this incident emphasized that privacy, identity, and trust were central to international security, influencing the EU's later adoption of the General Data Protection Regulation (GDPR).

Legal Accountability and Consumer Protection

The Equifax breach (2017) blurred the line between corporate data loss and national security risk. In response, the U.S. Department of Justice indicted four members of China's People's Liberation Army in 2020, illustrating the use of legal instruments and public attribution as deterrence tools (U.S. DOJ, 2020). Domestically, the breach led to congressional hearings and reforms in consumer data protection, while Equifax itself invested over $1 billion in cybersecurity upgrades. The broader impact was the globalization of corporate accountability, as governments worldwide began demanding stricter disclosure of cyber risks and imposing heavier fines for negligence. This shift reframed consumer data protection as part of the international security agenda.

Multilateral Attribution and Norm-Setting

The Microsoft Exchange hack (2021) demonstrated the vulnerability of global software supply chains. What distinguished the response was the collective attribution effort: the U.S., European Union, NATO, and Five Eyes partners jointly condemned China for the attack (U.S. White House, 2021). This multilateral stance elevated cyberattacks from bilateral disputes to matters of international security governance. By coordinating attribution, states sought to establish a normative expectation that large-scale cyber intrusions would trigger collective responses. The Exchange hack thus accelerated efforts to define international cyber norms, particularly regarding zero-day exploit disclosures and responsible state behaviour in cyberspace (Kello, 2017).

Global Consequences of Mitigation Efforts

Taken together, these responses reveal a broader transformation in how the international community perceives and manages cyber threats. Three global consequences stand out:

1. **Militarization of Cyberspace:** Institutional responses such as USCYBERCOM spurred other nations to expand offensive and defensive cyber units, intensifying the global cyber arms race.
2. **Integration of Business into Security Governance:** Aurora and Equifax demonstrated that private corporations are not only targets but also active participants in cyber defence, reshaping the boundaries between state and corporate responsibility.
3. **Fragmentation and Contestation of Norms:** While U.S.-led alliances emphasize transparency and collective attribution, China and Russia promote "cyber sovereignty," advocating state control over digital infrastructures (Creemers, 2015). This divergence has produced competing models of cyber governance, complicating the creation of universal norms.

Impact of the Cyber Battleground on Sino–U.S. Bilateral Ties (2017–2025)

Cybersecurity under the Trump Administration (2017–2020)

The Trump presidency marked a decisive escalation of U.S. policy toward China on cyber issues. In 2018, the U.S. Department of Justice indicted members of PLA Unit 61398 for the Equifax breach (2017), accusing them of stealing data from 145 million Americans (U.S. DOJ, 2020). Then–Attorney General William Barr described it as a "deliberate and sweeping intrusion" highlighting China's campaign to "rob American companies and American citizens of their most sensitive information."

In parallel, the Trump administration moved aggressively on supply-chain security. The 2019 Huawei ban and restrictions on ZTE were justified not only as trade policy but also as measures against cyber-enabled espionage. Trump declared that "foreign adversaries are exploiting vulnerabilities in our technology and communications networks" (White House, 2019). Scholars noted that these measures linked cybersecurity directly to **tech decoupling**, accelerating tensions in both trade and diplomacy (Segal, 2017).

Academics such as James Lewis (CSIS) argued that these actions reflected a long-standing concern: "China has been the world's most active perpetrator of cyber-enabled theft of intellectual property," costing the U.S. economy tens of billions annually (Lewis, 2018).

Cyber Rivalry during Biden's First Term (2021–2024)

President Joe Biden inherited an environment of deep mistrust and elevated cybersecurity to a pillar of national security. His 2021 Executive Order on cybersecurity emphasized "zero trust architecture" and public–private cooperation after the Microsoft Exchange hack, which his administration attributed to Chinese state-backed actors. The coordinated condemnation by the U.S., EU, NATO, and Five Eyes partners represented the first major instance of multilateral attribution against China (White House, 2021).

By 2023–2024, the rivalry extended beyond espionage to pre-positioning in critical infrastructure. U.S. intelligence disclosed Volt Typhoon, a PRC-linked campaign targeting water systems, ports, and communications networks. FBI Director Christopher Wray warned in April 2024 that Chinese hackers were "positioning themselves to deal a devastating blow to our critical infrastructure if and when Beijing decides the time has come" (Reuters, 2024). CISA Director Jen Easterly echoed that the activity was "not just about espionage, but pre-positioning for disruption" (CISA, 2024).

Meanwhile, the Biden administration tightened export controls on advanced semiconductors (2022, 2023), explicitly citing risks of Chinese military AI development. Commerce Secretary Gina Raimondo stated: "We cannot allow China to access advanced chips that could fuel their military modernization" (FT, 2023). Beijing denounced these measures as "technological containment."

The TikTok divest-or-ban law (2024) brought the cyber-tech rivalry into the public sphere. President Biden signed the legislation requiring ByteDance to sell TikTok's U.S. operations or face a nationwide ban, citing risks of Chinese influence operations. TikTok CEO Shou Zi Chew countered: "We aren't going anywhere… we will continue to fight in court" (AP, 2024). The episode hardened public opinion and introduced platform governance as a new axis of bilateral conflict.

The Cyber Dimension in 2025: Entrenched Rivalry and Securitized Interdependence

As of 2025, cyber tensions remain structural and intensifying. The U.S. continues to expand sanctions against Chinese hacking groups (e.g., APT31 indictments, 2024), while China advances its doctrine of cyber sovereignty, asserting the state's right to control its digital domain. President Xi Jinping has emphasized that "without cybersecurity, there is no national security; without informatization, there is no modernization" (China Media Project, 2021).

Corporate leaders have also weighed in. Following the 2023 Storm-0558 intrusion that exposed senior U.S. officials' emails, Microsoft President Brad Smith acknowledged failures, declaring: "We will not solve this problem through silence. Transparency and secure-by-design systems are our path forward" (U.S. Senate testimony, 2024). Such acknowledgments illustrate how tech firms themselves have become front-line actors in geopolitics.

Academics warn that cyber rivalry has become a defining constraint on bilateral cooperation. Harvard's Joseph Nye argues that "cyber power diffuses advantages and magnifies insecurity," making crisis stability harder to maintain (Nye, 2021). Adam Segal (CFR) adds that the "hacked world order" ensures that cyber tensions bleed into trade, climate, and diplomacy, limiting the space for compromise (Segal, 2017).

Synthesis: The Cyber Battleground as a Structuring Force

From 2017 to 2025, the cyber dimension has transformed from a peripheral irritant into a structuring force of Sino–U.S. relations. Its impacts can be summarized as:

1. **Security Polarization:** U.S. indictments, sanctions, and multilateral attributions have entrenched the view of China as the principal cyber adversary.
2. **Tech Decoupling:** Huawei bans, semiconductor export controls, and TikTok restrictions reflect the fusion of cybersecurity with industrial policy.
3. **Diplomatic Distrust:** Cyber intrusions such as OPM, Equifax, and Volt Typhoon eroded trust, undermining cooperation on global issues like climate change.
4. **Global Spillover:** Allies have aligned with U.S. cyber policy (e.g., coordinated attribution), while China has rallied partners around cyber sovereignty, creating rival blocs in cyber governance.

As former NSA Director Michael Hayden remarked after the OPM breach, "The OPM hack is not an espionage case. It's a counterintelligence treasure trove" (Sanger, 2016). That remark captures the essence of the cyber battleground: it is not just about data theft, but about the strategic restructuring of power relations. Sino–U.S. cyber conflict is now inseparable from the future of global order.

Global Impact and Future Prospects for the Cyber Battleground

Globalization of Cyber Conflict

The U.S.–China cyber rivalry has reverberated far beyond bilateral relations, reshaping the norms, alliances, and institutions of the global digital order. As **Adam Segal** (2017) noted, "cybersecurity has moved from the technical margins to the geopolitical core," making it a central axis of global politics. Incidents such as the Microsoft Exchange hack (2021) and the Volt Typhoon campaign (2023–2024) highlighted that vulnerabilities in widely used platforms or critical infrastructure have global spillover effects, impacting small businesses, municipalities, and governments worldwide (White House, 2021; CISA, 2024).

This has compelled other states—including the European Union, Japan, and Australia—to align more closely with U.S. cyber strategies. For example, NATO's 2021 communiqué declared that cyberattacks "could rise to the level of armed attack," signalling an unprecedented willingness to integrate cyberspace into collective defence (NATO, 2021). Meanwhile, China has deepened coordination with Russia and Global South partners around the doctrine of **cyber sovereignty**, framing cyberspace as a domain subject to state control (Creemers, 2015). The divergence between these models has fragmented the global internet into competing **digital blocs.**

Norm Contestation and the Governance Gap

The global response to cyber conflict has revealed a governance gap. Despite efforts at the United Nations Group of Governmental Experts (UNGGE) and the Open-Ended Working Group (OEWG) to establish voluntary norms, consensus on binding rules has remained elusive (UNODA, 2021). The U.S. and allies emphasize attribution, transparency, and restraint in targeting civilian infrastructure, while China and Russia champion state sovereignty and content control.

This divergence risks undermining the universality of cyberspace. As former UN Secretary-General Antonio Guterres warned, "the next major war may begin with a massive cyberattack" (UN, 2020). Without shared norms, cyber escalation could undermine international stability and trust, particularly given the difficulty of attribution and the speed of digital operations.

Economic and Technological Consequences

Cyber conflict has profound implications for the global economy and technology development. Cyber-enabled theft of intellectual property has been estimated to cost the global economy hundreds of billions annually (Lewis, 2018). Export controls on semiconductors, AI chips, and quantum research have fractured global supply chains, contributing to what analysts term a "technological Cold War" (Kello, 2017).

At the same time, the rivalry has accelerated innovation in defensive technologies, including zero-trust architectures, AI-driven threat detection, and post-quantum cryptography. While such advances strengthen resilience, they also deepen inequality between cyber powers and weaker states, raising the prospect of digital dependency in the Global South.

CONCLUSION AND WAY FORWARD

The evolution of Sino–U.S. cyber rivalry from 2017 to 2025 demonstrates how cyberspace has shifted from a peripheral arena of espionage into a core domain of great-power competition. Incidents such as the Equifax breach(2017), the Microsoft Exchange hack (2021), and the exposure of Volt Typhoon (2023–2024) illustrate the progression from theft of intellectual property to systemic pre-positioning in critical infrastructure. The responses to these incidents—ranging from indictments and sanctions to multilateral attribution and regulatory reforms—have not only shaped bilateral relations but also recalibrated the global digital order.

From the Trump administration's emphasis on supply-chain security and tech decoupling to the Biden administration's focus on multilateral attribution, semiconductor controls, and platform governance, cyber tensions have remained a constant driver of distrust. President Xi Jinping's articulation of cyber sovereignty stands in sharp contrast to Washington's vision of an open and secure cyberspace, producing competing models of governance that reverberate across alliances and international institutions. As academics like Joseph Nye (2021) and Adam Segal (2017) have argued, cyber power both constrains and enables states, creating dilemmas of mistrust even as interdependence persists.

At the global level, the rivalry has fragmented cyberspace into competing blocs: U.S.-aligned coalitions emphasizing transparency, attribution, and collective defence versus China-led groupings advancing state-centric digital sovereignty. Meanwhile, the militarization of cyberspace has blurred the lines between espionage, economic competition, and preparations for wartime disruption, raising serious risks of miscalculation in crises such as Taiwan or the South China Sea.

Yet, the cyber battleground is not only a source of division—it also exposes shared vulnerabilities. Attacks on healthcare systems, energy grids, or financial networks would have cascading effects that neither Washington nor Beijing could contain alone. This reality provides an opening for limited cooperation, even amidst rivalry.

Way Forward

As a researcher, I argue that three steps are essential to managing the future of cyber competition:

1. **Institutionalized Dialogue and Guardrails:** Bilateral crisis hotlines, technical working groups, and renewed agreements akin to the 2015 Obama–Xi accord—though imperfect—could provide essential guardrails against escalation.
2. **Multilateral Norm-Building:** The U.S., China, and their allies should engage constructively in UN forums such as the Open-Ended Working Group to establish baseline norms, particularly prohibitions on targeting civilian infrastructure during peacetime.
3. **Shared Investment in Resilience:** Both great powers, along with middle powers and private industry, must prioritize resilience measures—zero-trust architectures, supply-chain security, and post-quantum encryption—that benefit the entire global system.

In conclusion, the Sino–U.S. cyber rivalry will remain one of the defining fault lines of 21st-century geopolitics, shaping trade, diplomacy, and the architecture of international order. But by embedding resilience, building partial trust through dialogue, and converging on minimum standards of responsible behaviour, it is possible to prevent cyberspace from becoming the trigger of the next great-power conflict. The choice before policymakers is stark: allow the digital frontier to harden into a battlefield of perpetual mistrust, or seize the opportunity to craft cyberspace as a domain of both competition and cooperation—a global commons where rivalry is tempered by responsibility.

REFERENCES

1. Allison, G. (2017). Destined for war: Can America and China escape Thucydides’s trap? Houghton Mifflin Harcourt.
2. Council on Foreign Relations. (2010, January 14). Google and China: Operation Aurora.https://www.cfr.org/interview/google-and-china-operation-aurora
3. Creemers, R. (2015). Cyber China: Updating propaganda, public opinion work, and social management for the 21st century. Journal of Contemporary China, 24(93), 85–100. https://doi.org/10.1080/10670564.2014.918403
4. Cybersecurity and Infrastructure Security Agency (CISA). (2018). Cybersecurity and Infrastructure Security Agency Act of 2018. U.S. Department of Homeland Security. https://www.cisa.gov
5. Cybersecurity and Infrastructure Security Agency (CISA). (2024, May). FBI, CISA, and partners release joint advisory on Volt Typhoon. https://www.cisa.gov/news-events
6. Fruhlinger, J. (2020a, March 10). The OPM hack explained: Bad security practices meet China’s Captain America.CSO Online. https://www.csoonline.com
7. Fruhlinger, J. (2020b, February 10). The Equifax data breach explained. CSO Online. https://www.csoonline.com
8. Kello, L. (2017). The virtual weapon and international order. Yale University Press.

9. Lewis, J. A. (2018). Economic impact of cybercrime—No slowing down. Center for Strategic and International Studies. https://csis.org
10. Lindsay, J. R. (2015). The impact of China on cybersecurity: Fiction and friction. International Security, 39(3), 7–47. https://doi.org/10.1162/ISEC_a_00189
11. Miller, C. (2016). The OPM hack: China and lessons for U.S. cybersecurity. Journal of Strategic Security, 9(2), 53–64. https://doi.org/10.5038/1944-0472.9.2.1524
12. Ng, A. (2018, February 10). Equifax breach blamed on Chinese military hackers. CNET. https://www.cnet.com
13. Nye, J. S. (2010). Cyber power. Harvard Kennedy School, Belfer Center for Science and International Affairs.
14. Nye, J. S. (2021). Do morals matter? Presidents and foreign policy from FDR to Trump. Oxford University Press.
15. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. Journal of Strategic Studies, 38(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382
16. Sanger, D. E. (2016). The perfect weapon: War, sabotage, and fear in the cyber age. Crown.
17. Sanger, D. E., & Perlroth, N. (2021, March 7). U.S. blames hackers tied to China for Microsoft breach. The New York Times. https://www.nytimes.com
18. Segal, A. (2017). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age.PublicAffairs.
19. United Nations Office for Disarmament Affairs (UNODA). (2021). Developments in the field of information and telecommunications in the context of international security. United Nations. https://disarmament.un.org
20. United States Department of Justice (DOJ). (2020, February 10). Four Chinese military hackers charged in Equifax breach. https://www.justice.gov
21. United States White House. (2019, May 15). Executive order on securing the information and communications technology and services supply chain. https://trumpwhitehouse.archives.gov
22. United States White House. (2021, July 19). Joint statement on Microsoft Exchange Server compromise.https://www.whitehouse.gov