

The Adjustment of the U.S. Cybersecurity Competition Strategy Against China in Trump's Second Term

Yixuan Li, Yixuan Zhao, Haiyan Wang
Nanjing University, Nanjing, China

Abstract: The U.S.-China cybersecurity competition entered a new phase of institutional competition during the Trump 2.0 era. In his second term, Trump reshaped U.S. cyber policies with sovereignty as a priority, leading to a three-pronged confrontation between China and the U.S. in economic development, technological blockade, and diplomatic governance. U.S. economic sanctions shifted from tariffs to financial disconnection, while technological blockades expanded from hardware to knowledge networks. Diplomatic pressure leveraged multilateral platforms to solidify anti-China standards. China concentrated on chip and operating system development through national laboratories, established cross-border alert mechanisms via ASEAN and BRICS, and elevated legal status to block long-arm jurisdiction. Limited cooperation potential exists between the two sides in ransomware monitoring, data classification flows, and IoT standard-setting, with political trust deficits and technological differences constituting major obstacles. Third-party experimental environments and voluntary norms have become practical channels to reduce compliance risks.

Keywords: Cybersecurity; Sino-US Rivalry; Digital Sovereignty; Strategic Competition; Trump 2.0

1. Introduction

Cybersecurity, as the cornerstone of national security in the information age, has transcended traditional information protection to become a pivotal variable reshaping strategic equilibrium among major powers and influencing the international power structure. The U.S. Cybersecurity and Infrastructure Security Agency defines cybersecurity as "the art of protecting networks, devices, and data from unauthorized access or criminal use, and the practice of ensuring information confidentiality,

integrity, and availability." [1] Trump's re-election has propelled the Sino-U.S. cybersecurity rivalry into a new phase marked by structural transformation. The Cybersecurity Policy under Trump 2.0 continues and reinforces the "America First" policy logic, demonstrating distinct characteristics of digital sovereignty prioritization and unilateralism tendencies. Its strategic pillars will focus on six key areas: first, implementing "preemptive" offensive measures to deter foreign adversaries' hacking capabilities; second, reforming cybersecurity regulations to reduce compliance burdens; third, achieving federal network modernization; fourth, ensuring critical infrastructure security; fifth, encouraging the development of emerging technological advantages; and sixth, building a business-oriented cybersecurity talent pool.

Despite facing the United States' continuously intensified supply chain scrutiny, data flow restrictions, and technological blockades, China's autonomous and controllable capabilities in the field of cyberspace security still demonstrate remarkable resilience and vitality. The construction of China's cybersecurity capabilities, represented by the protection system for critical infrastructure, an autonomous and controllable technological ecosystem, and the establishment of discourse power in cyberspace governance, not only challenges the Western stereotypical perception of China's cyber defense capabilities but also proposes diversified institutional imagination for the global cyber governance order dominated by the United States. China's breakthroughs in the field of cyberspace security have intensified the deep-seated concerns of American strategic elites about whether the United States can maintain absolute dominance in the digital era, while also exposing the U.S. strategy of attempting to curb China's cybersecurity capabilities development through the "digital decoupling" approach.

2. Evolution of U.S. Cybersecurity Policy

From the first Trump administration through the Biden administration to the second Trump term, the evolution of U.S. national cybersecurity policy demonstrates strategic coherence with distinct trajectory shifts across periods. The cybersecurity objectives during the second Trump administration and the Biden administration period share continuity, both emphasizing the maintenance of America's national security, economic prosperity, and global leadership in the digital era. In terms of policy approaches, the Biden administration further prioritized the instrumentalization and weaponization of cyber technologies, expanding their application to military and other domains. Concurrently, it implemented "rule loosening" to stimulate industrial innovation and ensure its hegemonic position in cybersecurity.

During his first term, the Trump administration prioritized "active defense" to build a more competitive and secure cyberspace, focusing on enhancing national strength, strengthening deterrence, and improving defensive capabilities. This strategy was grounded in the "National Security Strategy" report titled "Promoting Peace Through Strength" [2]. The administration's decision to shift cybersecurity focus to economic domains emerged from the U.S. economic slowdown and the financial struggles faced by its core voter base. As the digital economy rapidly expanded, the Trump administration emphasized building "hard power" in cyberspace over traditional "soft power" approaches, adopting a pragmatic approach to ensure national security through enhanced cybersecurity deterrence.

The Biden administration has been committed to building an "integrated" cybersecurity strategy framework. Its cybersecurity competition strategy primarily revolves around ideological objectives, leveraging international mechanisms and allies to establish U.S. dominance in emerging technologies and global norms. [3] However, constrained by domestic political factors, excessive security tendencies, and geopolitical considerations, its cybersecurity policies have demonstrated indecisiveness in implementation. The Biden-era cybersecurity policy is characterized by "offensive" and "economy-oriented" approaches, aiming to construct a cybersecurity-economic framework aligned with U.S. interests through enhanced public-private collaboration, increased investment in emerging technologies, and the

implementation of a "zero-trust" strategy. Meanwhile, the "integrated" cybersecurity strategy system emphasizes systematic integration, focusing on critical domain hierarchies and coordinating three interconnected systems-strategic planning, policy safeguards, and strategic execution-to form a comprehensive protection network covering all domains.

During his second term, the Trump administration institutionalized cybersecurity policies under the framework of "offense first, technological autonomy, and efficiency supremacy," seeking to consolidate digital hegemony through militarized means. Shortly after taking office, Trump signed an executive order repealing the Biden-era "Executive Order on the Secure, Reliable, and Trusted Development and Use of Artificial Intelligence" issued in 2023.[4] This order originally required companies to submit security test reports before developing high-risk AI systems and mandated addressing algorithmic biases and data misuse. Trump's team deemed these regulations "hindering innovation" and instead established the "minimum regulation" principle through the "Executive Order to Remove Obstacles to AI Innovation in the United States," allowing companies to define AI ethical boundaries autonomously. Behind these seemingly regulatory-reducing executive order revisions lay Trump's unique logic: he believed lengthy rule-making processes would slow innovation, complex compliance requirements would drain corporate vitality, and broad defensive postures couldn't address evolving situations and persistent threats. Thus, the Trump administration's core strategy shifted from "improving rules" to "strengthening capabilities," and from "comprehensive defense" to "focused breakthroughs and offensive deterrence." [5] Meanwhile, offensive cyber operations became the core tool of national deterrence. During his second term, Trump abandoned the Biden-era "values-based" alliances and, in cybersecurity, adopted a "cybersecurity cooperation" strategy that effectively leveraged strategic allies while attempting to transform the Cyber Command into a "digital NATO."

3. Motivation of the U.S. Strategic Adjustment of Cybersecurity Competition with China

The adjustment of U.S. cybersecurity policy toward China is fundamentally driven by the interplay of three factors: technological, domestic political, and international strategic. On the technological front, the rapid development of cutting-edge technologies such as generative AI has intensified U.S. strategic anxiety, prompting it to tighten export controls on high-end chips and monitor cloud computing flows in an attempt to solidify its technological advantages and slow China's catch-up pace. Domestically, the policy rhythm is deeply intertwined with election cycles and the demands of interest groups, with cybersecurity issues often being used as bargaining chips to exchange political support for domestic agendas like immigration and budgeting, thereby shaping a hardline consensus toward China to serve domestic political agendas. Internationally, the U.S. actively builds an exclusive alliance certification system, embedding security standards through multilateral frameworks like the "Quad Mechanism" and upgrading military information protocols with regional countries, aiming to secure rule-making dominance in emerging technology fields and prevent multilateral platforms from diluting its influence. These three logics reinforce each other, collectively driving a profound shift in its cyber strategy toward China from temporary reactions to institutionalized and systematic containment. From a technical perspective, the U.S. strategic realignment in cybersecurity competition with China stems from strategic anxiety and systemic countermeasures triggered by the rapid advancement of disruptive technologies like generative AI.

The iteration of technology has significantly outpaced the response cycle of traditional policy tools, prompting administrative authorities to shift the focus of technological containment to the source of R&D and infrastructure. The core logic lies in viewing computational power advantages as the foundation for defining future military and economic competition, and attempting to solidify its technological gap by building a comprehensive regulatory network covering hardware, software, data, and services, thereby delaying China's catch-up process. With models like ChatGPT driving the servitization of computational power, the United States has added real-time monitoring clauses to cloud computing leases, requiring operators to report the identities and usage durations of overseas

clients weekly. This move aims to block the "computational bypass" risk of directly leasing cloud computing power to circumvent chip embargoes. At a deeper level, the inherent tension in the U.S. technological containment strategy lies in its attempt to counteract through precise control of key materials and achieve vertical breakthroughs in domestic chips, both indicating that the cost of technological decoupling is high and difficult to completely eliminate. The collision between this technological logic and geopolitics is pushing cyberspace competition toward long-term and complex dynamics.

The adjustments to Trump's cybersecurity policy during his second term were driven by three overlapping factors: a conservative shift in political ideology, aggressive strategic directions set by key personnel appointments, and a pragmatic restructuring of domestic governance logic.

At the level of political ideology, the "America First" doctrine has deeply integrated with Republican traditional conservatism, shifting cybersecurity priorities from international rule-making to unilateral actions. This transformation is prominently reflected in the 2025 draft National Cybersecurity Strategy, where its core pillar "shaping adversaries' behavior" emphasizes preemptive deterrence through proactive strikes, sanctions, and technological blockades, replacing the Biden administration's governance framework focused on defense and regulation. Meanwhile, key personnel appointments further solidified this offensive policy path. For instance, after Timothy Ho, commander of the Cyber Command, was removed in April 2025, Deputy Commander William Hartman—who actively promoted "forward-looking deterrence"—assumed the role of acting Director of the National Security Agency, centralizing decision-making mechanisms. The utilitarian approach to domestic governance also drove policy adjustments. Facing fiscal deficits and the US national debt exceeding \$38 trillion, the Trump administration favored cost-shifting through public-private partnerships, such as simplifying cybersecurity regulations and encouraging private sector involvement in defense responsibilities.

From an international perspective, after the EU introduced the Cyber Resilience Act, the US expressed concerns that its certification

standards would be cited by multiple countries. Consequently, it accelerated the establishment of a mutual recognition system excluding China suppliers, incorporating the submarine cable landing review template into a joint statement through the Quad mechanism (US-Japan-India-Australia), and pushed the NATO Cyber Defense Center to include supply chain traceability as a new training subject. Meanwhile, the US upgraded the military information security common protocol with the Philippines and Vietnam, embedding the South China Sea submarine topography data sharing clause into it, ensuring that policy adjustments align with regional security arrangements and preventing the international rule-making authority from flowing to multilateral platforms.

4. The Core Pillars of U.S. Cybersecurity Policy in Trump's Second Term

During his second term, Trump's cybersecurity strategy demonstrated a distinct orientation toward "offensive deterrence" and "technological nationalism." The policy framework was built around six core pillars: implementing "preemptive" offensive measures to counter foreign adversaries' hacking capabilities; reforming cybersecurity regulations to reduce compliance burdens; modernizing federal networks; securing critical infrastructure; fostering emerging technological advantages; and cultivating a business-oriented cybersecurity talent pool. These efforts aimed to systematically reconstruct the U.S. to regain its absolute advantage in the intensifying cyber rivalry with China. [6]

First, implement preemptive offensive measures. The core of this pillar is transitioning from traditional passive defense to "forward defense" -identifying and dismantling threats before they materialize in the adversary's cyberspace. This policy is reflected in expanding the operational authority of the U.S. Cyber Command, authorizing it to conduct "sustained engagement" operations. By proactively disrupting and degrading the adversary's critical cyber infrastructure and command systems, the goal is to escalate the costs and risks of cyber operations to a level the adversary cannot afford, thereby creating effective deterrence. [7] The objective is not only to enhance America's cyber resilience but also to proactively shape a cyberspace environment favorable to the United States.

Second, reform cybersecurity regulations to reduce compliance burdens. The Trump administration argued that excessive compliance requirements stifled corporate innovation and responsiveness. During his second term, he spearheaded sweeping reforms to federal cybersecurity laws, shifting from a rigid "one-size-fits-all" compliance checklist to a risk-based, outcome-driven regulatory framework. By eliminating redundant reporting requirements, streamlining procurement processes, and promoting automated compliance tools, these measures significantly eased compliance pressures on private sector entities, enabling them to focus resources more effectively on combating the most severe cyber threats.

Third, accelerate the modernization of federal networks. This initiative aims to drive comprehensive adoption of the "zero trust" security framework across federal agencies through mandatory directives. At its core is the principle of "never trust, always verify," employing technologies like micro-segmentation, identity authentication and access management, and encrypted traffic analysis to overhaul traditional perimeter-based security models. This modernization effort not only safeguards federal data against advanced persistent threats but also seeks to establish de facto global technical standards for zero trust solutions through government procurement power.

Fourth, ensuring critical infrastructure security. This pillar aims to address the inadequacy of voluntary security standards in critical infrastructure sectors. The policy focuses on establishing mandatory, performance-based cybersecurity baseline requirements for key industries such as energy, transportation, and finance through legislation, rather than specifying technical implementation paths. Simultaneously, it grants the Cybersecurity and Infrastructure Security Agency (CISA) clearer regulatory authority and establishes a "pre-hunting" collaboration mechanism, enabling national technical capabilities to assist critical infrastructure owners in proactively identifying and eliminating latent threats.

Fifth, establishing emerging technological advantages to maintain long-term technological supremacy. This pillar recognizes that competition in cyberspace ultimately boils down to competition in foundational technologies. Therefore, the policy focus is to ensure

America's global leadership in fields such as artificial intelligence, quantum information science, advanced semiconductors, and biotechnology through strategic investments, R&D tax incentives, and favorable immigration policies. Specifically, it emphasizes the deep integration of AI with cyber offense and defense, supports the development of AI-driven security tools, and vigilantly curbs adversaries' influence in setting AI security standards, aiming to secure technological dominance that will shape the future of cyber balance.

Sixth, establish a cybersecurity talent pipeline that is practice-oriented and business-driven. To address the critical shortage of cybersecurity professionals, this pillar has moved beyond the traditional single-track reliance on higher education, advocating instead for a diversified "competency-driven" approach. Key policy measures include vigorously promoting skill-based apprenticeship programs, establishing industry certification standards, and reforming federal government recruitment and compensation systems to attract top-tier cybersecurity talent. The core objective is to build a large-scale talent ecosystem with skills directly aligned to operational needs (e.g., threat hunting, incident response), providing sustainable human capital support for all policy pillars.

5. The Characteristics and Practices of the U.S. Security Competition with China in Trump's Second Term

During his second term, Trump's cyber security competition with China has formed a composite competitive framework, driven by offensive strategies, supported by "preemptive strikes" as tactical leverage, and reinforced by the weaponization of technology and the networking of alliances. Its essence lies in consolidating American cyber hegemony and compressing China's space for cybersecurity development through institutionalized and practical actions. This situation has exacerbated the "security dilemma" between China and the United States in cyberspace, while posing a severe challenge to the stability of the global cyber governance system.

5.1 New Features of Cybersecurity Strategic Confrontation Between the US and China

The Trump administration's second term (2025-present) has witnessed a marked shift

toward aggressive and systematic confrontation in its cybersecurity policy toward China. Centered on the 'America First' doctrine, it has escalated cyber competition with China through three key measures: restructuring strategic narratives, upgrading operational models, and intensifying technological containment alongside strategic alliances. This approach has propelled the Sino-US cyberspace rivalry into a new phase of high-intensity, institutionalized rivalry.

The first is the evolution of the U.S. strategic concept toward China. During the Trump 2.0 era, the "multi-stakeholder governance" framework of the Obama administration and the "integrated deterrence" framework of the Biden administration were abandoned, replaced by an aggressive logic of "peace through strength." The core of his policy is to proactively weaken China's cyber operational capabilities through normalized preemptive defense and low-intensity cyber attacks [8]. This shift is reflected at the institutional level: the Trump administration strengthened the institutional safeguards for offensive cyber forces by enhancing the authority of the Cyber Command, appointing radical cyber officials (such as Alexei Brazel), and significantly increasing the cyber warfare budget (reaching \$189 billion in fiscal year 2026) [9]. Notably, the U.S. deliberately amplifies the "China cyber threat theory," fabricating false narratives to legitimize its offensive policies, which essentially serves the geopolitical goals of technological decoupling from China and alliance containment.

The second aspect is the competition in emerging technology fields. The technological competition is prominently manifested in the militarization of artificial intelligence applications and the standardization competition in quantum cryptography. The Trump administration pushed for the establishment of an AI task force under the Cyber Command, focusing on developing AI-driven attack tools such as vulnerability mining and adaptive malware, attempting to suppress China's defensive resilience through technological disparity. Meanwhile, the United States accelerated the upgrading of its cyber arsenal, including supply chain attack tools that break physical isolation (such as the "Athena" system) and wireless hijacking weapons, and mandated the development of an AI operational roadmap

through the Fiscal Year 2025 National Defense Authorization Act, aiming to convert technological advantages into winning chips. [10] In the quantum domain, the United States explicitly set a post-quantum cryptography (PQC) migration timeline, requiring the quantum-resistance upgrade of the Transport Layer Security (TLS 1.3+) by 2030, intending to seize the initiative in cryptographic transformation. [11]

Third, the tool-based encirclement of the alliance system. The Trump administration instrumentalized cybersecurity policies, no longer emphasizing ideological and value-based alliances. It actively promoted the "NATO Asia-Pacificization" of cybersecurity alliances by integrating allies such as Japan and South Korea into the NATO Center of Excellence for Cooperative Cyber Defense, and by establishing cyber defense hubs in places like Guam, embedding cyberspace competition into the geopolitical strategic framework. This alliance system has a dual objective: first, to unify operational standards through joint exercises (such as "Cyber Guardian") and enhance coordination efficiency; second, to bind allies under the banner of "collective security" and weaken China's discourse power in international rule-making.

5.2 The Evolution of U.S. Cybersecurity Competition Against China

The systematic evolution of Trump's containment strategy toward China during his second term is the core practice of his "America First" philosophy in global competition, marking a profound transformation from singular and fragmented containment measures to systematic, precise, and alliance-based approaches [12]. This evolution has comprehensively replaced the contact framework with a competition paradigm, constructing a composite containment system through a "combination punch" in economic, technological, and diplomatic fields. The system aims to compress China's development space and reshape the international rule order, with both its intensity and complexity reaching historic highs.

The first is economic sanctions, attempting to achieve "precise decoupling". The Trump administration escalated its economic sanctions from the "tariff war" of its first term to more strategic supply chain strikes and financial long-arm jurisdiction. The core of its policy is to

restrict the flow of U.S. capital and technology to China's strategic industries such as new energy and semiconductors through legislative tools like the CHIPS and Science Act and the Inflation Reduction Act. At the same time, the U.S. expanded the coverage of the "Entity List", incorporating over a thousand Chinese companies into the regulatory scope, and abused the authority of secondary sanctions to impose joint penalties on third-country enterprises and Chinese cooperation projects, forcing international companies to take sides between China and the U.S. Notably, the Trump administration particularly strengthened control over financial channels, authorizing the Treasury Department through executive orders to review two-way investments between China and the U.S., restricting long-term capital investments such as U.S. pension funds in Chinese tech companies, and attempting to cut off the capital infusion for China's high-tech innovation cycle.

Secondly, technological blockade to maintain its own "digital hegemony". Technological blockade is the most coherent and aggressive area of U.S. containment against China, with its strategy evolving from "total embargo" to the paradigm of "small yard, high walls". During his second term, Trump further deepened the "small yard, high walls" into a dynamic and precise strike system: on one hand, by revising the Export Administration Regulations, it included new semiconductor materials such as gallium oxide and diamond, as well as GAAFET structural chip design software, in the control list, aiming to stifle China's ability to catch up in advanced process fields; on the other hand, it promoted the functionality of small multilateral mechanisms like the "Chip Four Alliance", jointly implementing a triple blockade on equipment, talent, and standards against China with allies such as Japan, the Netherlands, and South Korea. Additionally, the U.S. used the "digital iron curtain" strategy to contain China's development in emerging technology fields such as artificial intelligence and quantum computing, for example, by establishing the "Critical Technology Protection Fund" under the National Defense Authorization Act of 2025, prohibiting federal agencies from purchasing products and services using China's AI technology.

Third, diplomatic pressure to construct instrumentalized small multilateralism to compress China's strategic space. The Trump administration shifted the focus of diplomatic

pressure from geopolitical containment to the competition for rule dominance and the construction of instrumentalized small multilateralism. Its strategy one is to promote NATO's "Indo-Pacificization," strengthen the operational coordination capabilities of the U.S.-Japan-India-Australia "Quad Mechanism," incorporate the South China Sea issues into collective security agendas, and increase military assistance to Southeast Asian countries through the "2025 Indo-Pacific Security Framework" to compress China's strategic space in the region. Strategy two is to use the "Democratic Technology Alliance" as a vehicle to establish exclusionary technology standards in fields such as 5G, semiconductors, and artificial intelligence. For example, it jointly launched the "Digital Trade and Trust Initiative" with the EU, using data flow rules as barriers to weaken the global competitiveness of China's digital enterprises and systematically undermine China's cultural soft power and international discourse power.

6. China's Response Strategies and Discussion on the Path of Two Countries' Network Cooperation

In response to the upgraded complex containment system by the United States during Trump's second term, China has adopted a series of strategic and systematic countermeasures aimed at breaking the blockade, safeguarding development rights, and reshaping the international competitive landscape. These strategies not only focus on short-term countermeasures but also emphasize long-term structural adjustments, demonstrating China's strategic resolve and institutional confidence in the great power competition.

First, promoting the "dual circulation" and supply chain resilience. China's new development pattern, which takes the domestic large cycle as the mainstay and promotes mutual reinforcement between domestic and international dual cycles, has effectively offset external sanctions pressure. By expanding domestic demand and optimizing supply chain layout, China has enhanced the risk resistance of its economic system. In key areas such as high-end chips and new materials, China has implemented an import substitution strategy to support domestic enterprises in breaking through technological bottlenecks. Meanwhile, China has deepened cooperation with economies such

as ASEAN and the EU through the Regional Comprehensive Economic Partnership (RCEP) and the Belt and Road Initiative, reducing dependence on the US market. For example, the digital economy cooperation agreement signed between China and Central and Eastern European countries in 2025 has provided new opportunities for Chinese enterprises to explore emerging markets. [13] In the financial sector, China has promoted the internationalization of the renminbi, expanded the use of the Cross-Border Interbank Payment System (CIPS), and reduced reliance on the US dollar system.

Second, building an independent and controllable innovation ecosystem. China regards self-reliance and self-improvement in science and technology as a strategic support for national development, overcoming key core technological bottlenecks through the "new national system." In frontier fields such as artificial intelligence, semiconductors, and quantum computing, the Chinese government has increased investment in basic research, established national major science and technology projects, and promoted deep integration of "industry, academia, research, and application." For example, through the implementation of the "National Medium-and Long-Term Program for Science and Technology Development (2021-2035)," China has achieved a transformation from following to keeping pace and leading in areas such as 5G and BeiDou navigation. [14] At the same time, China encourages enterprises to strengthen independent innovation. After suffering from U.S. sanctions, companies like Huawei and ZTE have accelerated the development of independent operating systems and chip design tools, gradually reducing dependence on Western technologies. Additionally, China actively fosters an open-source ecosystem, gathering global developers through platforms like "Open Source China" to jointly build an independent technical standards system.

Third, expanding international cooperation and rule-making discourse power. China adheres to multilateralism and actively participates in the reform of the global governance system to weaken the diplomatic containment by the United States. On platforms such as the United Nations and the World Trade Organization, China advocates an inclusive development philosophy and opposes unilateral sanctions and long-arm jurisdiction. China has also led or

participated in multiple international cooperation mechanisms, such as the Global Data Security Initiative and the BRICS cooperation mechanism, providing alternative cooperation options for developing countries. In the field of technology, China promotes the governance concept of "putting people first and ensuring intelligent development for the better" through platforms like the World Internet Conference and the Artificial Intelligence Governance Forum, enhancing its international discourse power. Additionally, China deepens dialogue with regions such as the European Union and ASEAN to avoid regional countries taking sides and safeguard strategic space.

The Sino-US cyber interaction reveals a complex dynamic of competition and cooperation. Despite intensifying strategic rivalry, both sides maintain essential communication and collaboration in specific domains. This cooperation stems from their shared need to preserve fundamental stability in cyberspace and the practical necessity to prevent uncontrolled competition. [15] Currently, Sino-US cybersecurity cooperation exhibits three prominent features: limited institutionalization, highly concentrated focus areas, and relatively reversible outcomes.

China and the United States have broad prospects for cooperation in multiple fields of cybersecurity. In the field of combating cybercrime, law enforcement agencies of both countries have established case-specific collaboration mechanisms. In 2024, the two sides conducted information sharing in combating transnational ransomware attacks, successfully dismantling a cybercrime gang targeting critical infrastructure. In the protection of critical information infrastructure, the two countries have coordinated early warning and response to major cybersecurity incidents through regional mechanisms such as the Asia-Pacific Computer Emergency Response Team (APCERT). In early 2025, Chinese and American experts jointly issued security protection guidelines for industrial control systems, providing technical references for key industries. In the field of standard-setting, enterprises from both countries have maintained limited cooperation on specific technical standards such as 5G security and IoT device certification, while China's participation in international standard organizations has gradually increased.

However, the risks and challenges remain significant, with the lack of strategic mutual trust being the fundamental obstacle to deepening cybersecurity cooperation between China and the United States. The U.S. National Security Strategy for 2023 positions China as a "primary competitor," and its "preemptive defense" strategy directly conflicts with China's principle of "cyber sovereignty." At the rule level, there are profound differences between the two sides on key issues such as the definition of "cyber attacks" and the conditions for exercising the right of self-defense. The United States tends to expand the interpretation of the scope of application of the right of self-defense under Article 51 of the UN Charter, while China emphasizes the principle of national sovereignty and the leading role of the United Nations. The decoupling at the technical level further exacerbates the difficulty of cooperation, as U.S. restrictions on Chinese companies like Huawei and ZTE weaken the foundation for bilateral cooperation. Additionally, the spillover effects of traditional geopolitical issues such as the South China Sea also cast a shadow over cybersecurity cooperation.

Despite numerous challenges, China and the United States still have room for cooperation in the following areas: First, in the field of AI security governance, both sides can engage in dialogue on emerging issues such as AI weaponization and the regulation of autonomous weapon systems. In 2024, Chinese and American experts held multiple rounds of consultations under the United Nations framework on the definition and regulation of autonomous weapon systems, laying the foundation for future cooperation [16]. Second, in the protection of critical infrastructure, the two countries can establish targeted information-sharing mechanisms, focusing on cybersecurity threats in sectors such as finance and energy. Third, in combating cybercrime, they can improve case-specific collaboration processes to enhance cooperation efficiency. Finally, in the formulation of international rules, both sides can seek consensus on specific implementation details of state conduct norms in cyberspace within the United Nations-led process.

Current developments indicate that Sino-US cybersecurity cooperation will follow a "competitive coexistence" trajectory. On one hand, strategic competition will continue to

constrain the depth and breadth of collaboration, with intense rivalry persisting over rule-making authority and technical standard-setting influence. On the other hand, shared threats like ransomware and critical infrastructure attacks compel both sides to maintain minimal cooperation. Future breakthroughs hinge on three factors: first, political will at the highest level-whether both sides can decouple cybersecurity from other agendas; second, institutional development-whether specialized, routine communication channels can be established; third, pragmatic approaches-whether trust-building can progress through concrete, non-political initiatives.

7. Conclusion

The interaction model between China and the United States in cyberspace during Trump's second term reveals that the current digital competition among major powers has evolved into a comprehensive, multi-level, and rule-based strategic game. The essence of this game is a profound contest between established powers and emerging powers over the right to reconstruct the international order in the digital era. The current confrontation between China and the United States in cyberspace has transcended mere technological offense and defense, evolving into a competition of governance paradigms and rule systems, marking an acceleration of the militarization trend in cyberspace. China, on the other hand, is exploring a digital development path distinct from the Western model by improving its domestic legislative system, building an independent technological ecosystem, and deepening digital cooperation with developing countries. Disagreements between the two sides in core rule areas such as artificial intelligence governance, cross-border data flow, and critical infrastructure protection are becoming increasingly structural, forming a pattern of "systemic competition."

Despite intense competition, maintaining basic stability in global cyberspace and preventing major conflicts align with the shared interests of both nations. In non-traditional security domains such as combating transnational cybercrime and addressing ransomware attacks on critical infrastructure, China and the United States have practical cooperation needs. However, such collaboration remains constrained by strategic trust levels, exhibiting characteristics of limited

scope and fragile outcomes. Future dialogues and crisis management mechanisms in emerging fields like AI security and space cybersecurity will serve as crucial touchstones to test whether the two countries can establish a new balance of "coexistence in competition."

Looking ahead, the outcome of this game will not only determine the power status of the two countries in the digital era but also shape the future order of the global cyberspace-whether it leads to division and confrontation or maintains limited, managed openness. For the international community, including China, how to promote the construction of an inclusive, multilateral, and just global digital governance system while adhering to core security concerns is a long-term and arduous strategic task.

Acknowledgement

This work was supported by The National Undergraduate Innovation Training Program 2025 (NO: 202590002094)

References

- [1] CISA, "What is Cybersecurity?", February 01, 2021, available at <https://www.cisa.gov/news-events/news/what-is-cybersecurity>.
- [2] The White House, "National Security Strategy of The United States of America", Trump White House Archive, December 18, 2017, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- [3] Wang Tianchan, Cai Cuihong. The Biden Administration's International Strategic Framework for Cyberspace and Its Inherent Deficiencies [J]. *Modern International Relations*, 2022, (08):1-7.
- [4] "Removing Barriers to American Leadership in Artificial Intelligence", The White House, January 23, 2025, <https://www.whitehouse.gov/presidential-act ions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>.
- [5] Jiang Zhaoyi, Chen Jiayi, Yang Liuqing. Analysis of U.S. Cybersecurity Policy Toward China During Trump's Second Term [J]. *World Economic and Political Forum*, 2025, (06):121-136.
- [6] Lu Chuanying. The Return of Conservative Thought and the Trump Administration's Cybersecurity Strategy Adjustment [J].

- World Economics and Politics, 2025(1):60-79.
- [7] Wang Xiaofeng. "America First" and the Reconstruction of the Trump Administration's Cyber Strategy [J]. China Information Security, 2025(3):45-52.
- [8] Ding D. Evolution and Analysis of U.S. Cyber Deterrence Policy [J]. Teaching and Research, 2024,43(9):40-47.
- [9] The White House. National Cybersecurity Strategy[EB/OL]. 2023-03-02. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>
- [10] U.S. Department of Defense. FY 2025 Defense Budget: Summary of Funding[EB/OL]. 2025-06-20. <https://www.defense.gov/Spotlights/FY2025-Defense-Budget/>
- [11] Cheng Yuan, et al. The architecture, characteristics and implications of the U.S. "Integrated" cybersecurity strategy system [J]. Journal of Intelligence, 2024,43(9):40-47.
- [12] Dawei. The Path and Logic of the U.S. Strategic Transformation Toward China: From "Contact" to "Containment" [J]. International Political Science, 2023,8(1):58-85.
- [13] Ministry of Commerce. China-Memorandum of Understanding on Digital Economy Cooperation with Central and Eastern European Countries [EB/OL]. 2025-06-18.
- [14] State Council. National Medium-and Long-Term Program for Science and Technology Development (2021–2035) [R]. Beijing: People's Publishing House, 2025.
- [15] Dawei. Cybersecurity Cooperation under the Background of Sino-US Strategic Competition: Dilemmas and Solutions [J]. International Security Studies, 2025,43(2):65-82.
- [16] United Nations Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System. Report of the 2024 Session[R]. New York: UN, 2025.