AN EXAMINATION OF THE US-LED MINILATERAL CYBERSECURITY ALLIANCE AGAINST CHINA

Chen Tianping[*], **Zhang Gaozhan**[**]

DOI: 10.52837/27382702-2025.5.1-28

Abstract

This paper outlines the U.S. cybersecurity strategy under the Biden administration, which emphasizes building an open, free, and secure cyberenvironment and strengthening cyber deterrence and strategic pressure by enhancing cybersecurity cooperation with traditional allies, such as Japan, South Korea, and ASEAN countries. In addition, the U.S. has strengthened cooperation with countries in the Asia-Pacific region in the areas of digital economy and cybersecurity through multilateral mechanisms, such as the Indo-Pacific Economic Framework (IPEF), to ensure that it maintains a leadership position in global cybergovernance. This paper analyzes how the U.S. uses a multi-level and multi-faceted network of cybersecurity cooperation to limit China's influence in global cyberspace, and demonstrates the U.S. strategic intent to maintain dominance in cyberspace and promote regional economic cooperation.

Keywords: Cybersecurity, Minilateralism, Great power competition, China-U.S. relations.

Introduction

On March 2, 2023, the White House released the National Cybersecurity Strategy, outlining initiatives to address potential cybersecurity challenges and safeguard U.S. interests in the digital era. The strategy underscores the importance of an "open, free, global, interoperable, reliable, and secure" cyberspace, aiming to

[*] Chen Tianping, Doctoral Candidate, Institute of International Relations, Nanjing University ✉ chentianping@smail.nju.edu.cn

[**] Zhang Gaozhan, Corresponding author, Doctoral Candidate, Institute of International Relations, Nanjing University, ✉ zhanggaozhan@smail.nju.edu.cn

Received April 20, 2025, revised May 23, 2025, accepted July 22, 2025

build a “defensible and resilient digital ecosystem [22]” while highlighting the significance of alliances grounded in a rules-based international order. The scope of cyber deterrence—particularly in light of potential threats posed by an increasingly capable China—is articulated in a more direct and detailed manner.

By reinforcing collaboration and forming bilateral cybersecurity partnerships with traditional Asia-Pacific allies such as Japan, Korea, and the Philippines, as well as actively seeking new opportunities with regional organizations like ASEAN, the United States is moving toward “minilateralism”—smaller regional coalitions—for multifaceted cybersecurity cooperation aimed at limiting China’s global cyber influence [20: 49–70]. This multi-layered, broad-based, and comprehensive cybersecurity alliance exerts significant strategic pressure on China at both the technological and normative levels. Accordingly, this paper focuses on the mechanisms and underlying logic of constructing a potential U.S.-led minilateral cybersecurity framework.

The Conceptualization of Minilateralism

The idea of minilateralism could be traced back to the Concert of Europe in the early 19th century. Its prominence has increased at a time when major global powers are grappling with significant conflicts, such as the war in Ukraine and the growing divide between the U.S. and China, and offers a perspective characteristic of flexibility and functionality, conferring unique advantages in addressing specific international issues. This paragraph explores the theorization of minilateralism, examines its applications and impact in the scope of international relations, and further elucidates how it is taking on an increasingly significant role in the geopolitics of the Indo-Pacific region.

The definition and characteristics of minilateralism

There is broad consensus that minilateral cooperation among major powers has played a pivotal role in upholding a wider multilateral international order since World War II, as it has become prominent when the United States shifted away from Hub-and-Spokes [8: 681-708; 23: 23-25]. Scholars wrote extensively regarding the definition and implications of the concept, emphasizing the differences from multilateralism observed in conventional international cooperation. Moises Naim conceived minilateralism as the “smarter, more targeted approach” that “the smallest possible number of countries needed to have the largest possible impact on solving a particular problem," i.e., the "magic number" [13]. Singh and Teo further clarified that minilateralism can be viewed as a relatively exclusive, flexible, and functional cooperative relationship involving anywhere from three to nine countries [21: 2]. In the contemporary context, as the U.S. strives to reassert and reinforce its influence in Indo-Pacific geopolitics, the defining features of its minilateral approach to coalition-building—namely, constructing a latticework of alliances and partnerships—can be summarized as follows: *Value-based* – Minilateralism places an emphasis on a small group of pivotal countries whose values align closely. With the U.S. as the leading power, the selection of allies tends to strongly reflect its value orientation, enabling the rapid formation of an exclusive alliance to address specific issues within a short timeframe. This approach ultimately serves to build a value-based minilateral alliance that excludes particular countries on targeted concerns.

Convenience – Some scholars suggest that minilateralism is a special form of multilateral relationship [5], set apart from traditional multilateralism by its flexibility and lesser emphasis on formalized mechanisms. Its key feature lies in foregoing strict adherence to rigid norms and procedures, relying primarily on voluntary commitments. This leads to relatively open entry and exit processes, along with more limited obligations for members, thereby significantly mitigating the "abandonment" and "entanglement" dilemmas often found in traditional alliances [11]. Compared to full-scale multilateralism, once the United States approves of countries that share an interest in a given issue, those states can rapidly join the alliance. As a result, member countries can respond more swiftly to the initiator's proposals and cooperate more effectively, thus achieving alliance objectives more quickly.

Issue-focused: The minilateral approach typically centers on a relatively focused set of issues and is organized around specific domains. In most cases, an issue arises first, prompting cooperation among states that share common interests, leading to flexible and loosely structured partnerships. When the United States forms minilateral alliances, it can adapt the agenda in response to shifts in the international environment. Within the broader cooperative objectives of its existing alliance framework, the U.S. can extract more clearly defined issues to create new minilateral coalitions.

The Significance of Minilateralism in the United States' Cyber Strategy

Minilateral mechanisms, through their exclusivity and informality, simplify the decision-making process, enhance cooperation efficiency, and enable rapid responses to cyber threats. Through minilateral cooperation, the United States can effectively unite its allies to address complex cyber threats, enhance comprehensive defense capabilities, and, by collaborating with key Asia-Pacific countries, curb China's expansion in the global cyberspace, thereby maintaining its leadership position. This mode of cooperation also plays a significant role in promoting technological innovation and economic collaboration in a variety of aspects:

1. *Efficient Decision-Making and Cooperation*,
   The excludability and informality of minilateral mechanisms streamline the decision-making process and enhance cooperation efficiency. Member countries can swiftly reach consensus and take action, effectively responding to the rapidly changing cyber environment. The high complexity and dynamic nature of cyberspace require decision-making mechanisms that can react quickly, avoiding the lengthy procedures typical of traditional multilateral cooperation [1: 2]. By limiting the number of members and employing flexible agreement mechanisms, such cooperation ensures that consensus can be rapidly achieved and actions promptly taken in response to cyber threats. This type of mechanism is particularly well-suited to addressing the suddenness and diversity of cyber attacks, enabling the coordination of resources and the implementation of effective defenses in the shortest possible time.
2. *Countering Complex Cyber Threats*, Modern cybersecurity poses complex and diverse threats, making it difficult for a single nation to effectively respond. The globalization and cross-border nature of cyber attacks necessitate closer and more efficient cooperation among countries. Through minilateral cooperation, the United States can unite its allies, share intelligence resources and technologies, and jointly develop defensive measures [19: 30–50]. The borderless nature of cyberspace allows threats to originate from any corner of the world, making international collaboration particularly crucial. By leveraging minilateral alliances, the United States can revitalize traditional alliance systems. For instance, it can draw on relevant experiences from the traditional Five Eyes alliance and apply them to minilateral cybersecurity and intelligence-gathering groups such as the "U.S.-Japan-South Korea" and "U.S.-Japan-Philippines" coalitions.
3. *Enhancing Comprehensive Defense Capabilities*, Minilateral cooperation can significantly enhance the comprehensive defense capabilities among member

countries. Different nations possess unique technical and experiential advantages in the field of cybersecurity, and through collaboration, these strengths can be complementary. The diversity of cyberspace and the rapid iteration of technology make it challenging for a single country to master all defensive technologies comprehensively [18: 69–79]. Through minilateral cooperation, countries can share their technical expertise and experiences, forming a more robust and comprehensive defense system. By leveraging complementary resources and fully utilizing geographical advantages, member states can effectively manage and control threats within the region. Joint exercises and training are also key to enhancing comprehensive defense capabilities. Regular joint drills allow countries to simulate real-world cyber attack scenarios, testing and improving their coordinated response abilities. Through joint training, cybersecurity teams can share best practices and the latest technologies, elevating the overall level of defense.

4. *The Necessity of Strategic Deployment*, In the context of global strategic competition, minilateral cooperation holds significant strategic importance. By collaborating with key countries in the Asia-Pacific region, the United States can effectively curb China's expansion and influence in global cyberspace, thereby maintaining its leadership position in this domain [3: 26–34]. China’s rapid rise in cyberspace poses a challenge to the United States’ dominance in this field. The openness and interconnectedness of cyberspace allow national influence to expand more swiftly and broadly. Through minilateral cooperation, the United States can form a powerful alliance that balances China in terms of technology, norms, and strategic deployment. By cooperating with countries in the Asia-Pacific region, the United States can establish a formidable strategic deterrence force in the area. The intangible and covert nature of cyberspace makes deterrence more challenging, but with strong technological and collaborative defense capabilities, potential attackers can be effectively restrained.

The Application of Minilateralism in the United States’ Cyber Strategy Against China

As cybersecurity increasingly becomes a central issue in international relations, the United States is further strengthening its strategic positioning in cyberspace through minilateralism. This form of minilateral cooperation not only enhances the U.S. leadership in the field of cybersecurity but also significantly boosts its collaborative operational capabilities with allies. This paragraph explores the specific applications of minilateralism in the United States' cyber strategy against China, encompassing U.S.-Japan-Korea cooperation, open minilateral cyber collaborations between the U.S. and ASEAN, U.S.-Japan-India-Australia collaboration, and U.S.-Japan-Philippines cooperation centered on the South China Sea disputes.

1.U.S.-Japan-Korea cooperation

Minilateral cooperation among the United States, Japan, and South Korea is built upon a profound historical and strategic foundation. These three nations share long-standing alliances and a history of strategic collaboration, particularly through the bilateral alliances between the U.S. and Japan, and the U.S. and South Korea. This historical groundwork provides a robust framework of trust and coordination, enhancing the depth and sustainability of their minilateral cooperation [10: 44–63]. The US-Japan-Korea minilateral cooperation is characterized by strong decision-making and execution capabilities. It involves top-level policy consultations and decision-making bodies, such as the U.S.-Japan "2+2" Security Consultative Committee and the U.S.-South Korea Leaders' Summits. These high-level coordination mechanisms ensure a high degree of strategic and policy alignment among the participating nations, facilitating effective and unified actions [42: 71–84]. The cooperation among the United States, Japan, and South Korea extends beyond traditional security issues to include advanced cyber technologies and emerging technological fields such as 5G, quantum encryption, and artificial intelligence. Compared to other minilateral cooperations, the extensive range of topics covered by US-Japan-Korea collaboration grants it greater foresight and influence in technological innovation and cybersecurity. This broad agenda not only strengthens their collective defense capabilities but also positions them as leaders in shaping future technological standards and norms.

(1) Development and Implementation of U.S.-Japan cyberspace cooperation:

Cybersecurity Consultations and Dialogue Mechanisms: The United States and Japan conducted high-level consultations on cybersecurity issues in 2016 and 2020, reflecting the elevation of cybersecurity to a strategic core in bilateral relations. These high-level consultations, particularly during Shinzo Abe's second term as Prime Minister, were advanced to the level of heads of government through leader summits, thereby accelerating the development of bilateral cybersecurity cooperation mechanisms [6: 127-145]. Through the U.S.-Japan Security

Consultative Committee (“2+2”), which involves discussions between the Secretaries of State and Defense, cybersecurity was explicitly incorporated into the agenda. This inclusion provided a foundation for policy design, assessment, and coordination in U.S.-Japan cybersecurity cooperation.

Operational Cybersecurity Exercises: The United States and Japan regularly conduct joint cybersecurity exercises known as “Cyber Guard.” For example, the 2019 exercise simulated a transnational cyberattack to test the collaborative response capabilities of both nations. These exercises not only enhanced the cyber defense skills of both parties but also provided valuable practical experience and strategies for the global cyber defense system. Consequently, they further strengthened the U.S.-Japan capabilities in cyber defense and deterrence while consolidating the United States’ leadership position in global cyberspace.

Global Digital Connectivity Partnership: Launched in 2021, the Digital Cybersecurity Cooperation Partnership (DCCP) further reinforced U.S.-Japan collaboration in cyberspace. The United States and Japan jointly committed to investing $4.5 billion in this partnership ($2.5 billion from the U.S. and $2.0 billion from Japan) to promote the development and application of cybersecurity technologies. This initiative not only advanced several joint research and development projects, including quantum encryption technology and artificial intelligence, but also enhanced the secure transmission and processing of cyber data. Additionally, it boosted the competitiveness of both nations in the global high-tech cybersecurity market [36].

(2) Development and Implementation of US-South Korea Cyber Cooperation

Open Radio Access Network (Open-RAN) Cooperation: During the leaders’ summit in May 2021, President Biden and South Korean President Moon Jae-in jointly decided to leverage Open-RAN technology to develop open, transparent, and efficient 5G and 6G network architectures [39]. This decision reflects the two countries' forward-looking cooperation in emerging technology fields, aiming to promote greater regional coordination and digital innovation, particularly in Southeast Asia. This collaborative project not only aligns with South Korea's New Southern Policy but also is consistent with the United States' vision for a free and open Indo-Pacific region.

Advancing Cooperation on Key and Emerging Technologies: In February 2022, the Biden administration’s new Indo-Pacific strategy emphasized the joint advancement of key and emerging technologies with partners. In May of the same year, President Biden and South Korean President Yoon Suk-yeol further underscored cooperation in areas such as cutting-edge semiconductors, environmentally friendly electric vehicle batteries, artificial intelligence, and quantum technologies. The objective is to strengthen both nations' leadership positions in these critical sectors [39].

Strategic Cybersecurity Cooperation Framework: In April 2023, South Korea and the United States signed the Strategic Cybersecurity Cooperation Framework, which aims to expand bilateral cooperation into the cyber domain, enhancing the structural and formal aspects of their cybersecurity collaboration [33]. In December of the same year, South Korea joined the Critical and Emerging Technologies (CET) Dialogue Mechanism, designed to promote collaboration in information and communication technologies with like-minded countries, including the initiation of an informal trilateral technology dialogue with India. These actions demonstrate the United States' efforts to extend its influence in technological diplomacy [30].

(3) Construction and Implementation of a Multilayered Alliance System

The Biden administration was committed to transcending the traditional hub-and-spokes system, which primarily focuses on military security, by constructing a more multilayered and comprehensive alliance system. This strategy aims to strengthen bilateral relationships such as those between the United States and Japan (US-Japan) and between the United States and South Korea (US-South Korea), as well as trilateral relations among the United States, Japan, and South Korea (US-Japan-South Korea). The objective of this new relational framework is to make cooperation more multifaceted and comprehensive, encompassing a broader range of issues and fields, including cybersecurity and economic collaboration.

On August 18, 2023, the United States, Japan, and South Korea held the first-ever trilateral summit at Camp David. This historic summit produced several significant outcomes, including the Camp David Spirit, the Camp David Principles, and the Trilateral Consultative Agreement. These cooperation documents cover areas such as military security and cybersecurity, demonstrating the broad consensus reached by the three nations within a multilateral framework [34]. Additionally, the United States is promoting the participation of Japan and South Korea in multilateral cooperation mechanisms, such as the Indo-Pacific Economic Framework (IPEF) and the Chip Four Alliance (Chip4). Furthermore, the U.S. is encouraging Japan and South Korea to join the Five Eyes Alliance and for South Korea to participate in the Quadrilateral Security Dialogue Plus (QUAD+). These initiatives not only deepen the strategic ties between Japan, South Korea, and the United States but also help integrate Japan and South Korea more closely into the global security and economic systems. Through these measures, the Biden administration is not only strengthening traditional and emerging security cooperation with major countries in the Asia-Pacific region but also establishing a more robust multilateral cooperation platform for cybersecurity, economic collaboration, and technological development.

2. U.S. – ASEAN open minilateral cyberspace collaborations

As the United States deepens its Indo-Pacific strategy and intensifies strategic competition with China, the ASEAN region has assumed an increasingly important role in America's geopolitical strategy. The United States aims to strengthen its alliances with ASEAN through cyberspace cooperation, contest leadership in cyberspace, and construct a network cooperation sphere designed to curb China's influence [40: 105–133]. The U.S. employs various mechanisms, such as the "U.S.-ASEAN Smart Cities Partnership Program," the "Digital Asia Accelerator," the "Digital Policy Consultative Forum," and the "U.S.-ASEAN Cyber Policy Dialogue," to promote technological collaboration and digital infrastructure investments with ASEAN countries. Specifically, U.S.-ASEAN cooperation extends beyond traditional security domains to encompass digital and cyber technologies, including support for the development of smart cities in ASEAN nations and the promotion and enhancement of high-speed internet infrastructure [28: 99–114].

In this process, the United States' strategic objectives are to enhance the cyber governance capabilities of ASEAN countries, bolster cybersecurity, and promote consistency in technological standards and policies across the region through deepened cyber technology cooperation. This collaboration not only helps improve the cyber defense capabilities of ASEAN nations but also contributes to forming a regional cybersecurity architecture that serves as a counterbalance to China's cyber strategy.

(1) US-ASEAN Cyber Cooperation and Strategic Trends

Institutionalized Cybersecurity Cooperation: On August 20, 2021, the United States and the Singapore Ministry of Defense signed a Memorandum of Understanding (MOU) on cyberspace cooperation, marking a pivotal event that expanded their cybersecurity collaboration into the military domain and institutionalized it. This step underscores the recognition of cybersecurity's critical role in national security and the necessity for higher-level strategic dialogue and cooperation [12].

Bilateral Security Dialogues: In the subsequent months, the United States engaged in security dialogues with Indonesia and Malaysia, placing particular emphasis on collaboration in the field of cybersecurity. This includes the November 2021 security dialogue with Indonesia and discussions with Malaysian business leaders regarding the potential for enhancing cooperation in cybersecurity [25].

Advancing High-speed Communication and Digital Transformation: In March 2022, a joint statement between the United States and Singapore proposed the advancement of secure, interoperable, and advanced high-speed wireless communication technologies in the Indo-Pacific region [37]. Additionally, through cooperation with Japan, the United States further promotes the digital transformation of cities within ASEAN countries. This collaborative effort not only supports ASEAN's digital infrastructure but also aligns with broader regional innovation goals.

US-ASEAN Special Summit: At the "US-ASEAN Special Summit" in May 2022, both parties reached a consensus on strengthening the development of the digital economy. Although the United States' investment in the digital economy was relatively limited, the primary objectives were to reduce ASEAN countries' dependence on Chinese technology, strictly scrutinize technology investments related to China, and attempt to diminish China's cyber influence in the region [35]. Through these measures, the United States not only enhances cybersecurity and technological cooperation with ASEAN countries but also ensures strategic advantages in the global digital economy and high-tech sectors while counterbalancing China's technological expansion. This multi-dimensional cooperation strategy aims to elevate the cyber independence of ASEAN nations, reduce their reliance on major external powers, and bolster regional digital collaboration and technological autonomy.

(2) Utilizing the Indo-Pacific Economic Framework (IPEF) for Cybersecurity and Information Technology Cooperation

The Biden administration, through the initiation and promotion of the Indo-Pacific Economic Framework (IPEF), was committed to establishing a new model of regional economic cooperation. This initiative aims to fill the void left by the Trump administration's withdrawal from the Trans-Pacific Partnership (TPP) [31]. The IPEF encompasses 13 allies and partners in the Indo-Pacific region, including Japan, South Korea, Australia, New Zealand, Fiji, India, Singapore, the Philippines, Vietnam, Malaysia, Indonesia, Thailand, and Brunei. Together, these countries account for approximately 40% of the global GDP, highlighting the extensive foundation and far-reaching impact of their economic collaboration. In the construction of the Indo-Pacific Economic Framework (IPEF), cybersecurity and information technology are central areas through which the United States seeks to enhance cooperation with the Indo-Pacific region. The IPEF focuses on advancing the development of the digital economy and establishing fair, high-standard, and binding rules for digital trade. These rules are designed to ensure cybersecurity and data protection within the region.

Digital Trade and Cybersecurity: The IPEF aims to further integrate the economies of the Indo-Pacific by developing standards and regulations that include digital trade agreements. These agreements emphasize the secure transmission and processing of data, ensuring cybersecurity and data protection among member countries.

Collaboration on Critical Information Technologies: The framework emphasizes strengthening the resilience and security of supply chains in critical information technology industries, such as semiconductors, high-capacity batteries, and medical products. This includes the identification and protection of the entire supply chain, from raw materials to production, processing, and storage, thereby enhancing the robustness and security of information technology product supply chains.

Technological Innovation and Synergy: The IPEF promotes information-sharing systems and supply chain logistics technologies among member countries to address issues of supply chain disruptions and vulnerabilities. These measures have a direct impact on the application of cybersecurity and information technology, fostering technological innovation and collaborative efforts to mitigate risks associated with supply chain weaknesses.

Through these measures, the IPEF not only facilitates economic cooperation within the region but also strengthens the security architecture of cyber and information technologies. This ensures that the Indo-Pacific region maintains its competitiveness and security in the rapidly evolving digital economy. These efforts contribute to building a more secure and open digital and cyber environment, providing member countries with a shared security framework to collectively address the challenges of the digital age.

3. US-Japan-India-Australia Cooperation: Minilateral Cyber and Technology Collaboration under the Indo-Pacific Strategy

In the geopolitical context of the Indo-Pacific region, the United States has strengthened its cooperation with Japan, India, and Australia through the

Quadrilateral Security Dialogue (Quad), particularly in the fields of cybersecurity and information technology. This cooperative relationship aims to enhance technological capabilities and data security within the region through collective efforts, thereby ensuring the security of cyberspace and fostering technological advancements in the Indo-Pacific.

Working Group on Major and Emerging Technologies: This working group is a key component of the Quad framework, focusing on collaboration in areas such as artificial intelligence (AI) and next-generation communication technologies. The purpose of this organization is to establish a cooperative and research framework within these critical technological domains to promote innovation and application, while also strengthening the member countries' positions in global technological competition [32].

Quad Tech Network (QTN): Initiated by Australia at the United States' suggestion, the Quad Tech Network aims to enhance consensus and cooperation among the four nations on technological and cyber issues through both formal and informal channels. The QTN advocates for joint research and dialogue, reinforcing the Quad nations' technological influence in the Indo-Pacific region and promoting technological collaboration and development within the area (Australian National University).

Global Partnership on Artificial Intelligence (GPAI): Under the Quad framework, the United States, Japan, India, and Australia have joined the GPAI, collaborating with the G7 and other countries such as South Korea and Singapore. This partnership integrates efforts from governments, businesses, civil society organizations, and academia with the goal of collectively maintaining the technological advantages of democratic nations and promoting the safe and ethical use of artificial intelligence globally [26].

Digital Indo-Pacific Cooperation Program: The United States has proposed the Digital Indo-Pacific program within the Quad framework, which encompasses high-end technology manufacturing, digital economic transformation, inclusive digital development, and big data governance [16]. This program places particular emphasis on the secure and efficient sharing of data among Asia-Pacific countries, aiming to ensure the safe and efficient flow of data through transnational cooperation and to strengthen collaborative cybersecurity defenses.

Through these initiatives, the United States not only consolidates its technological and cybersecurity cooperation with key democratic partners in the

Indo-Pacific region within the Quad framework but also enhances the overall cybersecurity architecture and technological innovation capabilities of the entire Indo-Pacific region through this minilateral cooperation model. This ensures the security of cyberspace and the protection of data within the region while countering cyber threats and challenges from outside the Indo-Pacific.

4. U.S.-Japan-Philippines cooperation centered on the South China Sea disputes.

In the strategic landscape of the South China Sea region, the United States, Japan, and the Philippines have intensified their cooperation in cyber technologies and maritime surveillance, particularly in addressing “gray zone” challenges to ensure regional security and counter geopolitical competition. This cooperation not only revolves around traditional military and strategic interests but has also significantly expanded into the cyber and digital domains, reflecting the profound impact of geopolitics on technological collaboration and cybersecurity.

(1) Space and Cyber Technology Cooperation

Space Technology Deployment: In 2022 and 2023, the United States and Japan, as well as Japan and the Philippines, signed space cooperation framework agreements to promote bilateral "civilian space dialogues" and attempted to deploy the U.S. “Starlink” technology. In its collaboration with the Philippines, the United States invested in technologies such as drones, low Earth orbit sensors, and automation platforms to enhance the Philippines’ capabilities in maritime and cybersecurity domain [15]. These steps aim to bolster the Philippines' capabilities in space and communication technologies, strengthening its network coverage in remote and maritime areas. This technological support is intended to help the Philippines better monitor its maritime territories and improve its ability to respond to potential military and non-military threats. In terms of promoting cyber technologies, in July 2022, the United States and Japan jointly established the “Asia Open RAN Academy” in the Philippines to advance the promotion of 5G technologies and related standards. This initiative aims to support the Philippines in developing information and communication technologies while serving as a strategic measure to counter China's influence in the regional 5G sector [14]. Within the framework of the trade and technology war against China, the United States leverages military cooperation and foreign capital investments with the Philippines to interfere in Sino-Filipino collaborations in areas such as 5G and the digital economy. U.S. interventions include requiring the Philippines to cease using Huawei's 5G equipment due to concerns over national security and potential threats to U.S.-Philippine intelligence and military cooperation.

(2) Maritime Surveillance, Exercises, and Intelligence Sharing

Enhancing Maritime Vigilance and Surveillance Capabilities: The United States and Japan assist the Philippines in upgrading its maritime vigilance and surveillance capabilities by funding the establishment of national coastal surveillance centers and providing advanced monitoring equipment such as sensors, radars, and communication devices. These facilities and technological support help the Philippines detect and monitor activities in surrounding maritime areas. In 2020, Japan exported four modernized radar systems to the Philippines, further enhancing its maritime surveillance capabilities. The United States, through the construction of shore-based radars and ship-based radar systems, has helped the Philippines establish the National Coastal Watch Center (NCWC) and the Coastal Watch Radar System (CWRS), significantly boosting the Philippines' maritime surveillance and defense capabilities [17].

Strengthening Operational Capacities: By providing equipment and training, the United States has reinforced the operational capabilities of the Philippine Coast Guard, ensuring that the Philippines can effectively monitor and respond to security threats in its maritime zones. The U.S. Coast Guard and the Japan Coast Guard support the Philippine Coast Guard through personnel training, financial assistance, and joint exercises. For instance, the Japan International Cooperation Agency (JICA) has provided the Philippine Coast Guard with over ten maritime patrol vessels, including two of the largest offshore patrol ships. In June 2023, the United States, the Philippines, and the Japan Coast Guard conducted their first joint maritime exercise, marking a new height in trilateral maritime cooperation and coordination.

Intelligence Sharing Mechanisms: Through the U.S.-Japan and U.S.-Philippines Geographical Security Operational Measures Agreement (GSOMIA), a trilateral intelligence-sharing mechanism has been established to enhance joint maritime and aerial domain awareness capabilities. These agreements aim to refine the trilateral intelligence-sharing framework, strengthen joint maritime and aerial domain awareness, and consolidate a U.S.-led Indo-Pacific maritime situational awareness system.

(3) Maritime Situational Awareness and Regional Cooperation

At the fourth Quad Summit, the United States, Japan, India, and Australia jointly proposed the establishment of the Indo-Pacific Maritime Domain Awareness

Partnership (IPMDA). The aim is to construct a maritime situational awareness network led by the United States and involving regional allies and partners, thereby strengthening maritime containment of China. Leaders from the United States, Japan, and the Philippines emphasized their commitment to advancing multilateral maritime situational awareness cooperation through channels such as the Indo-Pacific Maritime Domain Awareness Partnership. They plan to conduct joint training exercises and humanitarian assistance and disaster relief drills to enhance the region's crisis and emergency response capabilities [29]. These cooperative efforts indicate that the United States, Japan, and the Philippines are deepening their security alliances through technological collaboration and strategic dialogue. Together, they are enhancing their technological, cyber, and maritime security capabilities within the region to address complex geopolitical challenges and maintain stability and security in the Indo-Pacific.

In this complex international relations context, the minilateral cooperation among the United States, Japan, and the Philippines reflects the profound impact of geopolitics on technological collaboration and cybersecurity. Within the strategic framework of the South China Sea region, the United States and Japan aim to position the Philippines as a strategic outpost by providing technological support and strengthening cooperation. This strategy intends to contain China's expansion and assertiveness in maritime domains. Through technological assistance and policy pressure, the United States seeks to shape regional security and technological standards while limiting China's influence in this strategically important area. Looking ahead, the further development of this cooperation will depend on the regional security dynamics, changes in the international political and economic landscape, and the strategic choices of the involved countries in safeguarding their security and development interests.

The Impact of the United States on Building a Minilateral Cyber Information Security Alliance Against China

As the United States continues to strengthen its cybersecurity strategy in the Asia-Pacific region, particularly through increasingly deepened cooperation with traditional allies such as Japan, South Korea, the Philippines, and ASEAN countries, its influence on China's cyber information security situation has become progressively significant [27: 1-7]. The United States' cyber strategy is evidently targeted at China, aiming to construct an open, free, and secure cyberspace by enhancing cooperation with Asia-Pacific nations through multilateral mechanisms, thereby ensuring its leadership position in global cyber governance.

Firstly, the United States' cyber cooperation with Japan and South Korea has expanded from bilateral to multilayered collaboration. For example, cybersecurity cooperation between the U.S. and Japan has been reinforced through regular joint cybersecurity exercises and high-level security consultations, enhancing both nations' cyber defense capabilities. This collaboration not only improves their cyber defense technologies but also contributes valuable experience to the global cyber defense system [10: 44–63]. Additionally, the jointly invested digital interconnectivity and cybersecurity partnerships between the U.S. and Japan have further solidified their cooperation in cyberspace, promoting the development and application of cybersecurity technologies. This cooperation significantly enhances both countries' competitiveness in the global high-tech cybersecurity market and exerts substantial strategic pressure on China.

Enhanced Multilateral Cybersecurity

Secondly, the United States has further strengthened cybersecurity cooperation with Asia-Pacific countries by promoting multilateral security collaborations such as the Indo-Pacific Economic Framework (IPEF). The IPEF encompasses areas like digital trade and data security and protection, establishing binding rules to ensure cybersecurity among member nations [4: 26–39]. This not only helps enhance regional cyber defense capabilities but also promotes consistency in technological standards and policies, thereby strengthening the counterbalance to China's cyber strategy.

Moreover, the United States' intervention in the South China Sea issues through enhanced cyber technology and maritime surveillance cooperation with Japan and the Philippines aims to position the Philippines as a strategic outpost in the region [44: 50-67]. By promoting cyber technologies and maritime monitoring cooperation, the United States not only strengthens the strategic position of the Philippines but also enhances the overall security cooperation network in the Indo-Pacific region through technological and intelligence support [43: 50-55]. These measures contribute to maintaining regional stability, countering unilateral actions and expansionist policies, and ensuring the freedom and openness of critical maritime areas such as the South China Sea.

Lastly, the United States' cooperation strategy with ASEAN demonstrates its efforts to reduce ASEAN countries' dependence on Chinese technology and to promote regional technological cooperation and digital infrastructure investments. U.S.-ASEAN cyber cooperation extends beyond traditional security domains into digital and cyber technology fields, highlighting the United States' strategic intent to expand its influence in technological diplomacy. This cooperation includes initiatives aimed at supporting the development of information and communication technologies within ASEAN, thereby serving as a strategic measure to counterbalance China's influence in the regional 5G sector.

The United States' cybersecurity strategy in the Asia-Pacific region has had a profound impact on China's cyber information security landscape. Through close collaboration with regional allies, the United States has not only enhanced its own and its allies' cyber defense capabilities but also exerted significant pressure on China's influence in the global cyberspace. This pressure compels China to adopt more cautious and flexible strategies in cybersecurity and international cyber politics, aiming to safeguard its security and development interests amidst evolving geopolitical dynamics.

China’s Strategic Countermeasures in Cybersecurity: A Response to U.S. Minilateral Containment

Beijing has developed a multi-faceted counter-strategy grounded in normative innovation, institutional counterbalancing, economic leverage, and asymmetric capability development – forming a coherent paradigm fundamentally distinct from Western alliance models.

I. Foundational Framework: Operationalizing Cyber Sovereignty

The “Strategy for International Cooperation in Cyberspace” issued by the Office of the Central Cyberspace Affairs Commission in 2017 shows that China’s strategy is philosophically anchored in the doctrine of cyber sovereignty, directly contesting the U.S. vision of an “open, free, global internet.” This doctrine asserts three irreducible principles: 1. Regulatory Autonomy: Unilateral authority over digital infrastructure and data flows. 2. Content Governance: Absolute discretion in information control and surveillance. 3. Normative Leadership: Rejection of extraterritorial legal imposition.

China builds operational mechanisms including: 1. Legal Architecture: Comprehensive legislation (Cybersecurity Law, Data Security Law, Personal Information Protection Law) creating compliance barriers that technically limiting malicious attacks by foreign companies. 2. Diplomatic Framing: The Global Data

Security Initiative (GDSI) advances an alternative governance model emphasizing non-interference and judicial sovereignty in data affairs, directly countering U.S.-led frameworks. 3. Technical Standardization: Through disproportionate influence in international standards bodies, China promotes protocols compatible with sovereign control principles across critical domains including 5G and artificial intelligence. 4. Strategic Contrast: Whereas U.S. minilateralism constructs exclusionary value-based coalitions, China pursues multilateral institutional penetration to legitimize its governance paradigm.

II. Counter-Alliance Ecosystems: Structural Alternatives

1. The Sino-Russian Strategic Symbiosis

This partnership counters containment through deep integration:

Military Coordination: Regular joint cyber exercises simulate integrated responses to critical infrastructure threats, while dedicated coordination channels enhance operational alignment against perceived Western operations.

Technological Decoupling: Collaborative initiatives develop sovereign alternatives across foundational technologies including operating systems, encryption standards, and financial messaging platforms – significantly diminishing the impact of Western technology restrictions.

Information Warfare: Joint mechanisms amplify narratives framing U.S. alliances as instruments of digital hegemony, leveraging state media ecosystems for global dissemination.

2. Shanghai Cooperation Organization: Institutional Counterweight

China uses the SCO as a scalable platform for alternative governance, and Iran is a member of this organization [41].

(1) Operational Integration: Regional cybersecurity centers facilitate intelligence sharing and coordinated responses to perceived threats. (2) Infrastructure Embedment: Strategic Digital Silk Road investments establish technological dependencies through nationwide communications networks and surveillance infrastructure across member states. (3) Normative Consolidation: Collective declarations explicitly reject participation in exclusive technology alliances while endorsing sovereignty-based governance principles.

III. Resource Mobilization: Integrated Capability Development

1. Technological Autonomy Drive

Massive multi-year initiatives targeting comprehensive supply chain sovereignty; Concentrated research advancing leadership in future network technologies; Significant investment in encryption systems resistant to foreign interception.

2. Whole Nation Coordination

China’s Military-Civil Fusion strategy enables: Seamless collaboration between military cyber units, intelligence services, and technology enterprises; Global proliferation of social control technologies to authoritarian states; Coordinated narrative campaigns amplifying sovereignty discourse while undermining Western initiatives.

3. Asymmetric Posture Development

Comprehensive programs isolating essential services from global networks. Systemic approaches to absorbing sanctions impact through economic scale and market depth. Development of capabilities that compel adversaries to expend disproportionate resources on defense.

U.S. technology restrictions have accelerated Chinese innovation cycles rather than containing capability development. China’s institutional alternatives demonstrate expanding membership while U.S. coalitions maintain static participation.

China has constructed an adaptive counter-containment ecosystem characterized by: (1) Normative Institutionalization: Establishing cyber sovereignty as a legitimate governance model for most developing states. (2) Structural Interdependence: Creating irreversible technological dependencies through infrastructure penetration. (3) Asymmetric Adaptation: Converting containment pressures into innovation catalysts and strategic advantages.

The core divergence remains fundamental: U.S. strategy prioritizes precision containment through exclusive clubs, while China emphasizes systemic endurance through inclusive, interest-based networks. Current evidence suggests U.S. actions have paradoxically strengthened China’s resolve to construct parallel technological ecosystems and governance frameworks. The emergent digital order appears increasingly bifurcated along competing visions – with China’s model demonstrating particular resonance among states prioritizing developmental sovereignty over liberal digital norms. This contest will likely define the cyber-geopolitical landscape for decades, with neither paradigm achieving decisive dominance but China’s approach showing greater organic growth potential in the evolving multipolar system.

Conclusion

The United States' minilateral cybersecurity strategy against China represents a multifaceted and strategically calculated approach to maintaining its leadership in global cyberspace and countering China's growing influence. By leveraging the flexibility and exclusivity of minilateralism, the U.S. has effectively constructed a network of alliances and partnerships with key Asia-Pacific allies, including Japan, South Korea, ASEAN countries, and the Philippines. These collaborations not only enhance the U.S.'s ability to respond to complex cyber threats but also strengthen its strategic position in the Indo-Pacific region. Through initiatives such as the Indo-Pacific Economic Framework (IPEF) and the Quadrilateral Security Dialogue (Quad), the U.S. has promoted technological innovation, economic cooperation, and cybersecurity standards that align with its vision of an open, free, and secure cyberspace.

However, this strategy has also prompted China to develop a robust counter-strategy rooted in the doctrine of cyber sovereignty. China's approach emphasizes regulatory autonomy, normative leadership, and the development of alternative governance models through multilateral institutions such as the Shanghai Cooperation Organization (SCO). By fostering deep integration with strategic partners like Russia and promoting technological self-reliance, China aims to counter U.S. containment efforts and establish its own vision of cyberspace governance.

The evolving dynamics between the U.S. and China in cyberspace highlight the broader geopolitical competition in the Indo-Pacific region. While the U.S. seeks to maintain its dominance through precision containment and value-based alliances, China is building a resilient and adaptive ecosystem that prioritizes systemic endurance and inclusive cooperation. This contest is likely to shape the future of global cyberspace governance, with both paradigms vying for influence in an increasingly bifurcated digital order. As the strategic competition intensifies, the outcomes will depend on the ability of each side to innovate, adapt, and secure the support of regional and global partners.

Bibliography

1. Anuar A., Hussain N. *Minilateralism for Multilateralism in the Post-COVID Age*. Singapore: RSIS Policy Report, 2021, pp. 1-11.
2. Australian National University. *Quad Tech Network*. https://nsc.crawford.anu.edu.au/department-news/18328/quad-tech-network
3. Cai C., Wang, T. *The Cyberspace Strategy of the Trump Administration*. Beijing: Contemporary World, Issue 8, 2020, pp. 26–34.
4. Cai C., Yu, D. *China-ASEAN Digital Economy Cooperation and Its Challenges under the U.S. 'Indo-Pacific Strategy'*. Shanghai: Journal of Tongji University (Social Science Edition), Vol. 34, Issue 2, 2023, pp. 26–39.
5. Ha H. T. *Understanding the Institutional Challenge of Indo-Pacific Minilaterals to ASEAN*. Singapore: Contemporary Southeast Asia, Vol. 44, No. 1, 2022, pp. 1–30.
6. Jiang T. *An Analysis of the U.S.-Japan Cybersecurity Cooperation Mechanism*. Beijing: International Outlook, Vol. 12, Issue 6, 2020, pp. 127–145, 151.
7. International Strategy of Cooperation in Cyberspace (Full Text), China.org.cn, March 7, 2017. http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm
8. Kahler M. *Multilateralism with Small and Large Numbers*. Cambridge: International Organization, Vol. 46, No. 3, 1992, pp. 681–708.
9. Ko The R. *USAID Opens PH-based O-RAN Academy to Upskill Regional Workforce*. Newsbytes.PH, July 3, 2022. https://newsbytes.ph/2022/07/03/usaid-opens-ph-based-o-ran-academy-to-upskill-regional-workforce/
10. Ling S. *The Strengthening and Prospects of U.S.-Japan-South Korea Trilateral Cooperation*. Beijing: Contemporary American Review, Vol. 7, Issue 4, 2023, pp. 44–63.
11. Ma B. *The Decline of Hegemony and the Rise of Minilateralism: A Case Study of the U.S.-Led Quadrilateral Security Dialogue*. Asia-Pacific Security and Maritime Studies, Vol. 4, 2023, pp. 25–50.
12. MINDEF Singapore. *Singapore, US Enhance Defence Cooperation in Cyberspace*, August 23, 2021. https://www.mindef.gov.sg/web/portal/mindef/news-and-events/latest-releases/article-detail/2021/August/23aug21_nr
13. Naim M. *Minilateralism: The Magic Number to Get Real International Action*.

Foreign Policy, June 21, 2009. https://foreignpolicy.com/2009/06/21/minilateralism/

14. Newsbytes, RAFI KO THE, NEWSBYTES.PH, USAID opens PH-based O-RAN Academy to upskill regional workforce, July 3, 2022, https://newsbytes.ph/2022/07/03/usaid-opens-ph-based-o-ran-academy-to-upskill-regional-workforce/.
15. Park S. *From Japan to the Philippines: US Expands SSA Cooperation with Asian Countries*. Space News, https://spacenews.com/from-japan-to-the-philippines-us-expands-ssa-cooperation-with-asian-countries/
16. Rasser M. *Networked: Techno-Democratic Statecraft for Australia and the Quad*. Washington, D.C.: Center for a New American Security, https://www.cnas.org/publications/reports/networked-techno-democratic-statecraft-for-australia-and-the-quad
17. Reyes M. T. *Radar System from Japan Enhances Philippines' South China Sea Surveillance*. Indo-Pacific Defense Forum, https://ipdefenseforum.com/2024/01/radar-system-from-japan-enhances-philippines-south-china-sea-surveillance/
18. Shen Y. *Responding to the Challenges of the Offensive Internet Freedom Strategy—Analyzing China-U.S. Competition and Cooperation in Global Information Space*. Beijing: World Economics and Politics, Issue 2, 2012, pp. 69–79.
19. Shen Y. *The Evolution and Practice of the U.S. National Cybersecurity Strategy*. Beijing: American Studies, Vol. 27, Issue 3, 2013, pp. 30–50.
20. Shen Y., Jiang, T. *The Balance of Offense and Defense in Cyberspace and the Construction of Cyber Deterrence*. Beijing: World Economics and Politics, 2018, pp. 49–70.
21. Singh B., Teo, S. *Introduction: Minilateralism in the Indo-Pacific*, in Singh, B. & Teo, S. (eds.) *Minilateralism in the Indo-Pacific: The Quadrilateral Security Dialogue, Lancang-Mekong Cooperation Mechanism, and ASEAN.* London and New York: Routledge, 2020, pp. 1-12.
22. The White House. *National Cybersecurity Strategy*. Washington, D.C.: The White House, March 2023. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
23. Tow W. T. *The Trilateral Strategic Dialogue, Minilateralism, and Asia-Pacific Order Building*, in Tatsumi, Y. (ed.) *US-Japan-Australia Security Cooperation:*

Prospects and Challenges. Washington, D.C.: Stimson Center, 2015, pp. 23–35.

24. U.S. Coast Guard. *U.S., Philippine, Japan Coast Guards Conduct Trilateral Engagements in the Philippines*. Department of Homeland Security, https://www.news.uscg.mil/Press-Releases/Article/3423307/us-philippine-japan-coast-guards-conduct-trilateral-engagements-in-the-philippi/
25. U.S. Department of Defense. *Readout of Indonesia–United States Security Dialogue 2021*, November 23, 2021, https://www.defense.gov/News/Releases/Release/Article/2852539/readout-of-indonesia-united-states-security-dialogue-2021/
26. U.S. Department of State. *Joint Statement from Founding Members of the Global Partnership on Artificial Intelligence*, June 15, 2020, https://2021-2025.state.gov/joint-statement-from-founding-members-of-the-global-partnership-on-artificial-intelligence/
27. Wang T., Cai C. *The Biden Administration's International Cyber Strategy Framework and Its Internal Defects*. Beijing: Modern International Relations, Issue 8, 2022, pp. 1–7.
28. Wang X., Li T., Chen Y. *The Logic and Effects of the U.S. Constructing a 'New Influence Network' through the 'Indo-Pacific Economic Framework'*. Changchun: Northeast Asia Forum, Vol. 32, Issue 5, 2023, pp. 99–114, 128.
29. White House. *Joint Vision Statement from the Leaders of Japan, the Philippines, and the United States*, April 11, 2024. https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/11/joint-vision-statement-from-the-leaders-of-japan-the-philippines-and-the-united-states/
30. White House. *Launching the U.S.-ROK Next Generation Critical and Emerging Technologies Dialogue*, December 8, 2023, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/12/08/joint-fact-sheet-launching-the-u-s-rok-next-generation-critical-and-emerging-technologies-dialogue/
31. White House. *On-the-Record Press Call on the Launch of the Indo-Pacific Economic Framework*, May 23, 2022. https://web.archive.org/web/20220607040444/https://www.whitehouse.gov/briefing-room/press-briefings/2022/05/23/on-the-record-press-call-on-the-launch-of-the-indo-pacific-economic-framework/
32. White House. *Quad Leaders' Summit Fact Sheet*, May 20, 2023,

https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/05/20/quad-leaders-summit-fact-sheet/

33. White House. *Republic of Korea State Visit to the United States*, April 26, 2023, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/04/26/fact-sheet-republic-of-korea-state-visit-to-the-united-states/
34. White House. *The Trilateral Leaders' Summit at Camp David*, August 17, 2023, https://bit.ly/4l5sUet
35. White House. *U.S.-ASEAN Special Summit in Washington, DC*, May 12, 2022. https://bit.ly/4lQlRYp
36. White House. *U.S.-Japan Competitiveness and Resilience (CoRe) Partnership*, April 16, 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership/
37. White House. *U.S.-Singapore Joint Leaders' Statement*, March 29, 2022, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/03/29/u-s-singapore-joint-leaders-statement/
38. White House. *United States–Republic of Korea Leaders' Joint Statement*, May 21, 2022. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/21/united-states-republic-of-korea-leaders-joint-statement/
39. White House. *United States–Republic of Korea Partnership*, May 21, 2021, https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2021/05/21/fact-sheet-united-states-republic-of-korea-partnership/.
40. Xing R. *The Impact of the U.S. 'Indo-Pacific Economic Framework' on China-ASEAN Relations and Countermeasures*. Beijing: Peace and Development, Issue 6, 2023, pp. 105–133.
41. Xinhua. *Shanghai Cooperation Organization*. July 4, 2023. https://www.xinhuanet.com/world/2023-07/04/c_1129732658.htm
42. Yang Y., Zhang Y. *The Establishment and Impact of the U.S.-Japan-South Korea Trilateral Cooperation Mechanism*. Beijing: International Studies, Issue 6, 2023, pp. 71–84.
43. Zheng X. *'U.S.-Japan-Philippines Trilateral Framework': A New Frontier in the U.S. Indo-Pacific Strategy*. Beijing: Contemporary World, Issue 7, 2023, pp. 50–55.
44. Zhou S. *U.S.-Japan-Philippines Security Cooperation: Motives, Characteristics, and Impacts*. Asia-Pacific Security and Maritime Studies,

Issue 6, 2023, pp. 50–67.

ՉԻՆԱՍՏԱՆԻ ԴԵՄ ԱՄՆ-Ի ԱՌԱՋՆՈՐԴԱԾ ՓՈՔՐԱԹԻՎ ՄԱՍՆԱԿԻՑՆԵՐԻ ՁԵՎԱՉԱՓՈՎ (MINILATERAL) ԿԻԲԵՐԱՆՎՏԱՆԳԱՅԻՆ ԴԱՇԻՆՔԻ ՈՒՍՈՒՄՆԱՍԻՐՈՒԹՅՈՒՆ

Չեն Տյենպին, Ճան Գաոճան

Հիմնաբառեր - կիբերանվտանգություն, մինիլատերալիզմ, մեծ տերությունների մրցակցություն, Չինաստան – ԱՄՆ հարաբերություններ

Ամփոփում

Հոդվածն ուսումնասիրում է ԱՄՆ-ի կիբերանվտանգության քաղաքականությունը Բայդենի վարչակազմի օրոք, որը կարևորում էր բաց, ազատ և անվտանգ կիբեր միջավայրի ստեղծումը և կիբերպաշտպանության ամրապնդումը՝ ավանդական գործընկերների՝ Ճապոնիայի, Հարավային Կորեայի և ԱՍԵԱՆ երկրների հետ համագործակցությունը խորացնելու միջոցով: ԱՄՆ-ն նաև ամրապնդել է Ասիա-Խաղաղօվկիանոսի տարածաշրջանի երկրների հետ համագործակցությունը թվային տնտեսության և կիբերանվտանգության ոլորտում՝ կիրառելով բազմակողմ մեխանիզմներ, ինչպիսին է Հնդ-Խաղաղօվկիանական տնտեսական շրջանակը (IPEF)՝ համաշխարհային կիբերտիրույթում իր առաջատար դերը պահպանելու համար: Աշխատանքում վերլուծվում է, թե ինչպես է ԱՄՆ-ն օգտագործում բազմաշերտ և բազմակողմ կիբերանվտանգության համագործակցության ցանցը՝ սահմանափակելու Չինաստանի ազդեցությունը գլոբալ կիբերտիրույթում և ցույց է տալիս ամերիկյան ռազմավարական նպատակը՝ պահպանել գերակայությունը կիբերտիրույթում և խթանել տարածաշրջանային տնտեսական համագործակցությանը: