· Article ·

A Study on Sino-American Cybersecurity Cooperation from the Perspective of Global Cybersecurity Governance

Zhengqin Wang[1,*], Zheng Yang[2]

[1] School of English Studies, Dalian University of Foreign Languages, Dalian, China

[2] School of English Studies, Dalian University of Foreign Languages, Dalian, China

* Corresponding Authors: Zhengqin Wang. Email: 2891831760@qq.com

Received: 24 September 2024 Accepted: 3 October 2024 Published: 30 October 2024

Abstract: This paper explores the current status, challenges, and future prospects of Sino-American cybersecurity cooperation. With the rapid advancement of information technology, cybersecurity has become a global issue, significantly impacting national security, economic stability, and social order. As the world's largest economies and major cyber powers, cooperation between China and the United States is crucial in the cybersecurity field. This paper provides an overview and analysis of the importance of cybersecurity, the main threats faced, and the global trends in cybersecurity development, with a particular focus on the cybersecurity policies and current situations of China and the United States. It emphasizes the necessity of Sino-American cybersecurity cooperation, including addressing the challenges of globalization and interconnectivity, meeting economic interdependence needs, considering strategic security factors, leveraging cultural exchange opportunities, and fulfilling global governance responsibilities. Future directions include deepening technological innovation and collaboration, strengthening legal frameworks and international rule-making, enhancing cultural exchanges and educational cooperation, and promoting innovation and development in global cybersecurity governance.

Keywords: Cybersecurity; Sino-American Cooperation; Information Technology; National Strategy; Global Governance

1. Introduction

With the rapid development of information technology, the internet has become an indispensable part of social and economic activities worldwide. However, the openness and anonymity of cyberspace have also introduced numerous security risks. In recent years, the frequency of cyberattacks has increased significantly, posing serious threats to national security, economic stability, and social order. As Buchanan, B. (2020) pointed out, cybersecurity issues have escalated to the level of national strategy and have become a topic of great concern for governments around the world.

Scholars Clarke and Knake (2012), in their work Cyber War, emphasized that as the world's two largest economies and major cyber powers, the efforts of China and the United States in cybersecurity cooperation are of critical importance.

This paper aims to explore the current status, challenges, and future prospects of cybersecurity cooperation between China and the United States. By analyzing the background, motivations, and current state of Sino-American cybersecurity cooperation, this study examines the interaction and cooperation mechanisms between the two countries in the field of cybersecurity, and proposes policy recommendations to promote further cooperation.

This paper adopts a combination of literature review and case analysis methods. First, a comprehensive review of Chinese and English literature is conducted to outline the cybersecurity policies of China and the United States, the current state of cooperation, and the main challenges faced. Second, by analyzing typical cases of Sino-American cybersecurity cooperation, the paper summarizes the successes and failures to draw lessons. Finally, considering the current international cybersecurity landscape, the paper offers future prospects and policy recommendations for Sino-American cybersecurity cooperation.

2. Overview of Cybersecurity

Cybersecurity, also known as information security, refers to the ability to protect network systems and their information from natural disasters, malicious attacks, and unauthorized access through technical measures, management practices, and legal regulations. Schneier, B. (2015) identifies the core objectives of cybersecurity as confidentiality, integrity, and availability—ensuring that information is not accessed or altered by unauthorized parties while guaranteeing that legitimate users can normally access network resources. As the global digitalization process accelerates, the internet has permeated various industries, becoming a crucial infrastructure for societal operations. Scholar Chertoff, M. (2018) argues that the importance of cybersecurity is reflected in national security, economic stability, social order, and personal privacy. Cyberattacks can lead to the leakage of state secrets, the paralysis of critical infrastructure, and pose severe threats to national security. Cybercrime and hacking cause significant economic losses to businesses, disrupt market order, and hinder economic development. Activities like cyber fraud and the spread of rumors undermine social stability and erode public trust. Cybersecurity vulnerabilities can result in the leakage of personal privacy, causing numerous disruptions and risks to individuals' lives.

The primary threats to cybersecurity include malware, cyberattacks, data breaches, insider threats, and advanced persistent threats (APTs). Malware such as viruses, worms, and trojans disrupt, steal information from, or control infected computer systems. Cyberattacks, like Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and phishing, aim to disrupt network services or steal sensitive information. Data breaches occur when sensitive information is accessed and used by unauthorized parties due to system vulnerabilities or human error. Insider threats stem from malicious actions by personnel within an organization, such as data theft or system sabotage. Advanced

Persistent Threats (APTs) involve prolonged, sophisticated cyberattacks supported by organizations or states, typically targeting specific governments or enterprises. Addressing these threats presents significant challenges, including technological complexity, talent shortages, inadequate legal frameworks, insufficient international cooperation, and difficulties in information sharing. As cyber technology evolves, so do the methods of attack and defense, increasing the complexity of cybersecurity. The demand for cybersecurity professionals outpaces supply, and the shortage of skilled professionals limits the enhancement of cybersecurity capabilities. Existing laws and regulations cannot comprehensively cover all aspects of cybersecurity, with legal frameworks lagging behind technological advancements. The transnational nature of cyberattacks makes it difficult for individual countries to respond effectively, necessitating stronger international cooperation. Barriers to information sharing between businesses and governments weaken overall cybersecurity defenses.

The development of global cybersecurity shows some notable trends. The United Nations Institute for Disarmament Research (UNIDIR) (2017) discussed international security trends and realities in detail in The Cyber Index. Governments and businesses worldwide are increasing their investments in cybersecurity to enhance defense capabilities and address threats. The Internet Governance Forum (IGF) (2020), in Policy Options for Connecting and Enabling the Next Billion(s), explored policy options for internet connectivity and the associated security challenges. More countries are enacting and implementing cybersecurity-related regulations to regulate online behavior and protect information security. Emerging technologies such as artificial intelligence, blockchain, and quantum computing are being applied in the field of cybersecurity, providing new tools and methods for defense. Public and corporate awareness of cybersecurity is steadily increasing, with a growing emphasis on security consciousness. The cybersecurity policies of major countries and regions vary in focus. The U.S. government has developed comprehensive cybersecurity strategies, including the National Cybersecurity Strategy and the Cybersecurity Framework, to promote cybersecurity cooperation between the public and private sectors. The European Union has implemented the Cybersecurity Act and established the European Union Agency for Cybersecurity (ENISA) to strengthen cooperation and information sharing among member states. China has issued the Cybersecurity Law to promote the cybersecurity grading protection system and enhance the security of critical infrastructure. Important international cooperation mechanisms, such as the International Telecommunication Union (ITU), aim to improve global cybersecurity through the development of international standards and the promotion of cooperation. The United Nations Cybercrime Convention seeks to combat cybercrime and foster international cooperation. The Asia-Pacific Economic Cooperation (APEC) promotes cooperation and information sharing among member states through its cybersecurity working group.

3. Current State of Cybersecurity in China and the United States

Before elaborating on the cooperation between the two states, it’s necessary to analyze the current situations of China and the United States separately.

3.1 China's Cybersecurity Policies and Current State

China places great importance on cybersecurity, elevating it to the level of national strategy. In 2016, China issued the Cybersecurity Law, which provides detailed regulations across various aspects, including network operations, data protection, and personal privacy, aiming to ensure cybersecurity and safeguard national sovereignty and public interests. Additionally, the Chinese government highlighted cybersecurity measures in its China's Policies on Asia-Pacific Security Cooperation (2017). In recent years, China has also intensified efforts to protect critical infrastructure by implementing laws and regulations such as the Regulations on the Security Protection of Critical Information Infrastructure, enhancing cybersecurity protection for key sectors like energy, finance, and transportation. China's current cybersecurity landscape is characterized by a relatively comprehensive legal framework and steadily increasing technological capabilities. However, the country also faces challenges, including frequent cyberattacks and rampant cybercrime. The widespread adoption of new technologies such as 5G, the Internet of Things (IoT), and artificial intelligence (AI) has further increased the complexity and importance of cybersecurity.

3.2 The United States' Cybersecurity Policies and Current State

As an early leader in information technology, the United States has developed a mature policy framework and practical experience in the field of cybersecurity. U.S. cybersecurity policies cover multiple levels, with the Department of Homeland Security outlining detailed measures to address cyber threats, including national strategic planning, legislative protections, and technical defense measures.

On the technological front, the United States leverages its strong technological prowess and innovation capacity to develop a range of cybersecurity technologies and solutions. U.S. cybersecurity companies hold a leading position in the global market, continually introducing new security products and services to counter increasingly sophisticated cyber threats.

However, despite having advanced technology and robust policy support, the United States continues to face cybersecurity challenges. Cyberattacks occur frequently, posing threats not only to government agencies but also to the information security of the private sector and individual users. Moreover, as technology evolves and new applications emerge, new cybersecurity issues, such as data privacy breaches and cybercrime, are constantly arising, presenting fresh challenges to U.S. cybersecurity policies.

In summary, the U.S. experience and practices in cybersecurity offer valuable lessons, particularly in terms of technical defenses and emergency response mechanisms. At the same time, China, in formulating and implementing its cybersecurity policies, also considers the importance of international cooperation and exchange to jointly address transnational cyber threats and maintain peace and stability in cyberspace.

3.3 Comparative Analysis of Cybersecurity Capabilities Between China and the United States

China and the United States each possess distinct advantages in the field of cybersecurity, yet there are also significant differences between them. In terms of policy and legal frameworks, China has been refining its cybersecurity system through a series of laws and regulations in recent years, while the United States boasts a more mature and systematic legal framework. In terms of technological strength, the United States maintains a global leading position due to its robust capacity for technological innovation and its leading cybersecurity companies. China has also made significant progress in the research, development, and application of network technologies, particularly demonstrating strong potential in areas such as 5G, artificial intelligence, and big data. In terms of responding to cybersecurity threats, both China and the United States face multiple threats from both domestic and international sources, but the United States has more extensive experience in international cooperation and information sharing. Overall, both China and the United States have their own strengths in the field of cybersecurity, but they both face common challenges such as technological complexity, talent shortages, and insufficient international cooperation.

4. Background of U.S.-China Cybersecurity Cooperation

In the context of accelerating globalization and digitalization, cybersecurity has become an unavoidable shared challenge and a critical issue for both the United States and China. Despite differences and competition in political, economic, and cultural domains, cooperation in cybersecurity between the two countries is particularly urgent and necessary.

4.1 Challenges of Global Interconnectivity

As scholar Segal, A. (2016) pointed out, the way nations behave in the digital age is undergoing significant changes. With the widespread adoption of the internet and the increasing degree of globalization, cybersecurity issues have transcended national borders, becoming a global challenge. As the world's two largest economies and leaders in information technology, the stability of the cybersecurity landscape in both China and the United States directly impacts the security and stability of global cyberspace. In the face of increasingly complex and pervasive cyber threats, it is difficult for any single country to respond effectively on its own. Strengthening international cooperation and information sharing is essential to jointly address these cybersecurity challenges.

4.2 The Need for Economic Interdependence

The economies of China and the United States are highly interdependent, and the security of information technology and network infrastructure is directly related to the stability and sustainability of economic development in both countries. Cybersecurity incidents can cause direct losses to businesses and individuals and may also affect investment decisions by multinational corporations and the smooth conduct of international trade. By enhancing cybersecurity cooperation, China and the

United States can build a relationship of mutual trust and benefit, fostering economic development and innovation in information technology, and contributing positively to the healthy development of the global economy.

4.3 Strategic Security Considerations

At the strategic level, cybersecurity has become an essential component of national security. As two of the most influential countries in the world, the national security and international strategic interests of China and the United States are closely interconnected. Cyberattacks and information warfare have become critical tools in modern warfare. By strengthening cybersecurity cooperation, China and the United States can jointly resist external threats and protect political stability and social security.

4.4 Opportunities for Cultural Exchange

Despite political and economic competition, cooperation in cybersecurity can serve as a vital bridge to enhance mutual understanding and trust between China and the United States. Through technical exchanges, sharing experiences, and conducting joint research, the two countries can deepen their understanding of cybersecurity challenges, jointly explore effective solutions and best practices, and promote the peaceful use and shared development of cyberspace worldwide.

4.5 Responsibility for Global Governance

As significant participants in global cyberspace, China and the United States have a responsibility to promote the construction and improvement of the global cybersecurity governance system. By establishing and strengthening mechanisms for cybersecurity cooperation, China and the United States can demonstrate their leadership and sense of responsibility on the international stage, driving the creation of global cybersecurity standards and norms, and jointly maintaining the security and stability of global cyberspace.

In conclusion, U.S.-China cybersecurity cooperation is not only in the interests of both nations but also crucial for the security and stability of global cyberspace. By deepening cooperation and building mutual trust, China and the United States can jointly address various cyber threats, fostering the healthy development and sustainable use of global cyberspace.

5. Current State and Challenges of U.S.-China Cybersecurity Cooperation

The history of U.S.-China cooperation in cybersecurity is long, and while progress has been made, numerous challenges and complexities remain.

5.1 Areas of Cooperation and Progress

U.S.-China cooperation in cybersecurity mainly covers areas such as information sharing, technical cooperation, policy dialogue, and the formulation of international rules. Through regular high-level dialogue mechanisms, such as the U.S.-China Joint Working Group on Cybersecurity

(JWG) and the Strategic and Economic Dialogue (SED), both parties have enhanced communication and cooperation on cybersecurity policies and legislation. Additionally, the two countries have undertaken a series of cooperative actions in combating cybercrime, jointly responding to cyberattacks, and enhancing the security of critical infrastructure, achieving some degree of success.

However, despite these positive developments, cooperation still faces numerous challenges, such as differences and disagreements in areas like information-sharing mechanisms, data privacy protection, the formulation of technical standards, and accountability. The substantive progress in U.S.-China cybersecurity cooperation is influenced by political and economic factors, and the depth and breadth of this cooperation still need further strengthening and expansion.

5.2 Technical and Experience Exchange

Technical and experience exchange is a vital part of U.S.-China cybersecurity cooperation. The two countries have engaged in extensive collaboration in areas such as security technology research and development, cyber defense technology, and emergency response capabilities. For instance, the U.S. and China have conducted multi-level cooperation and exchanges in cyberattack detection and prevention technologies, information security certification standards, and cybersecurity talent development. Furthermore, U.S.-China cooperation has deepened through case studies and best practice exchanges in cybersecurity governance within multinational corporations and large enterprises.

5.3 Policy and Legal Frameworks

The policy and legal frameworks form a critical foundation for U.S.-China cybersecurity cooperation. The two countries have different legal systems and governmental management models in cybersecurity legislation, policy formulation, and enforcement oversight. While China and the United States have respectively established the "Cybersecurity Law" and the "Cybersecurity Framework," differences exist in the scope of legal application, data privacy protection, and national security reviews. These discrepancies create uncertainty and risks for cross-border data transmission for multinational corporations and individuals.

Moreover, U.S.-China differences in formulating international rules and global governance in cybersecurity also present challenges. For example, in areas such as international internet governance, data flow, and cross-border information management, the U.S. and China have significant differences in principles like data sovereignty, information security, and the freedom of cyberspace. These differences not only affect the depth and breadth of bilateral cooperation but also pose new challenges for global cybersecurity governance.

5.4 Cultural and Trust Building

Cultural and trust building is a crucial factor in promoting U.S.-China cybersecurity cooperation. Enhancing mutual understanding and trust on cybersecurity issues can be achieved through increased cultural exchange, academic research, and expert dialogues. The U.S. and China have engaged in active cooperation in cybersecurity talent development, academic research collaboration, and

international conference exchanges, promoting cultural and personnel exchanges and strengthening mutual trust and the willingness to cooperate in cybersecurity.

6. Analysis of Successful Cases in Sino-American Cybersecurity Cooperation

As significant players in the global cybersecurity domain, China and the United States have achieved several notable successes through multi-level and multi-domain cooperation. These cases not only reflect the collaborative outcomes in addressing common cybersecurity challenges but also provide valuable experience and practice for the security and stability of the global cyberspace.

Under the framework of Sino-American cybersecurity cooperation, several key areas stand out:

6.1 Intergovernmental Dialogues Promoted Cooperation Mechanism

Intergovernmental security dialogues and cooperation between China and the United States play a crucial role in maintaining national security and the stability of the global cyberspace. From September 9 to 12, 2015, Meng Jianzhu, the special envoy of President Xi Jinping, a member of the Political Bureau of the Central Committee of the Communist Party of China, and Secretary of the Central Political and Legal Affairs Commission, led a delegation of officials from the Ministry of Public Security, the Ministry of State Security, the Ministry of Justice, and the Cyberspace Administration to visit the United States. They held discussions with U.S. Secretary of State John Kerry, Secretary of the Department of Homeland Security Jeh Johnson, and National Security Advisor Susan Rice, during which both sides agreed to engage in dialogue and cooperation on cybersecurity.

From September 22 to 25, during the meeting between the Chinese and U.S. heads of state, President Xi Jinping and President Barack Obama held in-depth, candid, and constructive talks. They reached a broad consensus and achieved a series of important outcomes. Among them, both China and the United States agreed to establish a high-level joint dialogue mechanism to combat cybercrime and related issues. Following this, high-level dialogues between the two sides became increasingly frequent, leading to effective cooperation.

On December 1, 2015, State Councilor and Minister of Public Security Guo Shengkun co-chaired the first high-level joint dialogue on combating cybercrime and related issues with U.S. Attorney General Loretta Lynch and Secretary of the Department of Homeland Security Jeh Johnson in Washington. During this dialogue, the two sides reached the "Guiding Principles for China-U.S. Cooperation on Combating Cybercrime and Related Issues" and decided to establish a hotline mechanism, achieving positive results in areas such as cybersecurity cases, cyber terrorism cooperation, and law enforcement training.

The establishment of the above dialogue and cooperation mechanism marks a new phase in China-U.S. cybersecurity cooperation, laying a solid foundation for a series of collaborative outcomes.

6.2 Joint Efforts to Combat Cybercrimes

Since the establishment of the high-level joint dialogue mechanism on combating cybercrime and

related issues, law enforcement agencies of China and the U.S. have made significant progress in clue investigation and case collaboration. In February 2016, the Ministry of Public Security of China received a notification from the U.S. Department of Homeland Security's Immigration and Customs Enforcement, reporting a suspect believed to be located in China who was allegedly distributing child pornography online. The U.S. suspected this individual of child sexual abuse. Following this notification, Chinese authorities quickly identified and apprehended the suspect involved in spreading child pornography and committing sexual offenses against children.

During the examination of the suspect's electronic devices, Chinese police uncovered numerous leads related to the online distribution of child pornography and exchanges of experiences in child sexual abuse, promptly sharing this information with U.S. authorities to aid their investigation.

The joint law enforcement cooperation between China and the U.S. in the field of cybersecurity has played a crucial role in combating the online dissemination of child pornography and addressing real-life cases of child sexual abuse. An efficient and smooth law enforcement collaboration has gradually emerged under the high-level dialogue mechanism, with both sides conducting mutual investigations and cooperation on cases involving the online distribution of child pornography, commercial espionage, cyber fraud, and the use of technology for planning and executing terrorist activities. In the same year, China provided the U.S. with leads on 20 "zombie networks" and phishing websites impersonating Chinese banks, which the U.S. positively responded to for verification and action.

7. Future Prospects of Sino-American Cybersecurity Cooperation

As key players in the global cybersecurity domain, China and the United States face a future filled with challenges and opportunities in the face of increasingly complex and diverse cybersecurity threats. Against the backdrop of current globalization and technological innovation, Sino-American cybersecurity cooperation will encounter several key areas of development and challenges.

7.1 Deepening Technological Innovation and Cooperation

Building on existing cooperation and exchanges, China and the United States can further strengthen collaboration in the field of cybersecurity technology innovation and application. With the continuous development of new technologies such as Artificial Intelligence (AI), blockchain, and big data, these technologies not only provide new defensive means for cybersecurity but also offer new avenues for attackers. Therefore, China and the United States can promote the widespread application of new technologies in cybersecurity through joint research and development and sharing best practices, enhancing the intelligent level of network protection and effectively addressing increasingly complex network threats.

To deepen cooperation in technological innovation and collaboration, China and the United States can take the following specific measures:

(1) Strengthen technological cooperation between multinational corporations and research

institutions. For example, establish joint laboratories and research and development centers to jointly research and develop advanced cybersecurity technology solutions, including intelligent threat detection and automated emergency response.

(2) Promote technology transfer and knowledge sharing between multinational corporations and innovative enterprises. By establishing technology cooperation platforms and patent sharing mechanisms, facilitate the rapid application and promotion of new technologies, and enhance the cybersecurity protection capabilities of enterprises on a global scale.

(3) Enhance cooperation and exchange between higher education institutions and research organizations. By establishing cybersecurity research institutes, joint laboratories, and academic exchange programs, cultivate and attract more cybersecurity professionals, promote in-depth cooperation between academia and industry, and jointly address future cybersecurity challenges.

7.2 Strengthening Legal Frameworks and International Rule-Making

In the context of globalization, cybersecurity faces complex challenges such as cross-border data flow, data privacy protection, and cross-border accountability for cyberattacks. China and the United States can strengthen the coordination and formulation of international legal frameworks to promote the establishment of an open, fair, and inclusive global cyber governance system. To deepen cooperation in legal frameworks and international rule-making, China and the United States can take the following measures:

(1) Strengthen transnational cooperation and information sharing. Establish international legal assistance and information exchange mechanisms to improve the efficiency and effectiveness of combating cybercrime and managing cross-border data flows, jointly addressing global cybersecurity threats.

(2) Promote the participation and contribution of multilateral organizations and multinational corporations in cybersecurity governance. Facilitate the establishment and improvement of multilateral coordination mechanisms, formulate global cybersecurity standards and best practices, and promote the open and secure development of the global cyberspace.

(3) Enhance international cooperation and policy dialogue. By organizing international cybersecurity high-level forums, legal seminars, and expert workshops, promote global coordination and cooperation in cybersecurity governance, and jointly address global cyber threats and challenges.

7.3 Deepening People-to-People Exchanges and Educational Cooperation

Culture and trust are essential foundations for cybersecurity cooperation. In the future, China and the United States can enhance understanding and trust on cybersecurity issues through strengthened people-to-people exchanges, youth exchange programs, and academic research cooperation. For example, continue to hold cybersecurity forums, seminars, and exchange visits to provide more opportunities for cybersecurity experts and policymakers to exchange and cooperate, jointly addressing global cyber threats and challenges.

To deepen cooperation in people-to-people exchanges and educational cooperation, China and the United States can take the following measures:

(1) Strengthen academic research and education and training. Establish Sino-American cybersecurity research centers and joint training programs to jointly develop and promote cybersecurity courses and training content, cultivating and attracting more cybersecurity professionals.

(2) Promote cultural exchanges and youth exchange programs. By organizing cultural exchange activities, youth exchange camps, and international student exchange programs, enhance the consensus and cooperation awareness of students and young leaders in cybersecurity concepts and practices, laying a solid foundation for future cybersecurity cooperation.

(3) Enhance civic education and social participation. By carrying out public welfare activities, community education, and social participation projects in cybersecurity, raise public awareness and understanding of the importance of cybersecurity, and strengthen the support and participation of all sectors of society in cybersecurity governance, jointly promoting the construction and development of a global cybersecurity culture.

7.4 Promoting Innovation and Development in Global Cybersecurity

Governance Global cybersecurity governance requires innovation and development in various aspects such as technological innovation, policy coordination, and international cooperation. China and the United States can actively promote the formulation and implementation of international cybersecurity rules within the framework of international organizations such as the United Nations, and strengthen global coordination and governance in the field of cybersecurity. Strengthen the construction and improvement of international organizations and multilateral mechanisms. Actively participate in international cybersecurity cooperation organizations and transnational cooperation mechanisms, promote the formulation and implementation of global cybersecurity standards and best practices, and jointly maintain the openness and security of the global cyberspace.

Promote international cooperation in technological innovation and application. By establishing international technology innovation alliances and open research and development platforms, facilitate the rapid application and promotion of new technologies in cybersecurity protection and emergency response, and strengthen global cybersecurity cooperation and coordination.

Enhance public participation and social governance. By carrying out cybersecurity education and public awareness campaigns, raise public awareness and understanding of the importance of cybersecurity, and enhance the support and participation of all sectors of society in cybersecurity governance, jointly promoting the security and stability of the global cyberspace.

8. Conclusion

This paper has delved into the current state, necessity, challenges, and prospects of Sino-American cooperation in the field of cybersecurity. As two of the world's major cyber powers, China and the United States face increasingly complex and diverse cybersecurity threats, making

cooperation particularly important and urgent. Through an analysis of current cooperation models and case studies, it is evident that certain achievements and progress have been made in areas such as joint working groups, multinational corporate cooperation, and intergovernmental security dialogues. However, the cooperation process also faces multiple challenges, including technological differences, policy disagreements, and cultural barriers. To further deepen cooperation, it is necessary to strengthen technological innovation and application, promote the coordination and formulation of international legal frameworks, deepen people-to-people exchanges and educational cooperation, and promote innovation and development in global cybersecurity governance.

Future research can explore multi-national cybersecurity cooperation models and case studies from a global perspective, analyze the application of emerging technologies in cybersecurity, study the role and challenges of international legal frameworks in cybersecurity governance, explore the impact of cultural differences on cybersecurity cooperation, and discuss the role and mechanisms of public participation in global cybersecurity governance. These research directions will help to further improve and expand the theory and practice of Sino-American and global cybersecurity cooperation, contributing more wisdom and strength to the construction of a secure and stable global cyberspace.

Acknowledgement

None.

Funding Statement

None.

Author Contributions

Zhengqin Wang: writing original draft, validation, investigation.

Zheng Yang: methodology, writing review and editing supervision.

All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials

None.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1]. Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geo politics. *Harvard University Press.*

[2]. Knake, R. K., & Clark, R. A. (2012). Cyber war: The next threat to national security an d what to do about it. *The ECSSR.*

[3]. Schneier, B. (2015). Data and goliath: The hidden battles to collect your data and control your world. *WW Norton &Company.*

[4]. Chertoff, M. (2018). Exploding Data: Reclaiming Our Cyber Security in the Digital Age. *Atlantic Books.*

[5]. United Nations Institute for Disarmament Research (UNIDIR). (2017). *The Cyber Index: International Security Trends and Realities.*

[6]. Internet Governance Forum (IGF). (2020). *Policy Options for Connecting and Enabling the Next Billion(s).*

[7]. Information Office of the State Council of the People's Republic of China. (2017). *China's Policies on Asia-Pacific Security Cooperation.*

[8]. U.S. Department of Homeland Security. (2018). *Cybersecurity Strategy.*

[9]. Segal, A. (2016). The hacked world order: How nations fight, trade, maneuver, and manipulate in the digital age. *Hachette UK.*

[10]. Lewis, J. A. (2006). Cybersecurity and critical infrastructure protection. *Center for Strategic and International Studies*, 9.

[11]. Segal, A. (2020). China's alternative cyber governance regime. *Council on Foreign Relations*, 1-8.