World Journal of Education and Humanities
ISSN 2687-6760 (Print) ISSN 2687-6779 (Online)
Vol. 6 No. 4, 2024
www.scholink.org/ojs/index.php/wjeh

Original Paper

Cyber Diplomacy during the Biden Administration and Future Prospects

Jianwu Hu[1] & Minghao Li[2]

[1] Hu Jianwu, School of Government, Shanghai University of Political Science and Law, Shanghai, China

[2] Li Minghao, School of Government, Shanghai University of Political Science and Law, Shanghai, China

Received: May 27, 2024 Accepted: July 02, 2024 Online Published: July 29, 2024

doi:10.22158/wjeh.v6n4p45 URL: http://dx.doi.org/10.22158/wjeh.v6n3p45

Abstract

The Biden administration has placed a high priority on cybersecurity and cyber diplomacy during its tenure. This paper delves deeply into the Biden administration's various efforts in the realm of cyber diplomacy, aiming to forge cyber alliances guided by cybersecurity strategy and the concept of small multilateralism. The Biden administration seeks to leverage cyber diplomacy to repair relationships with traditional allies while also strengthening cooperation with emerging market countries, thereby maintaining and enhancing the United States' leadership in global cyber policy. The paper also analyzes the main challenges faced by the Biden administration, including rapidly advancing technology, domestic and international political factors, and competition with global adversaries. Finally, the paper evaluates the current effectiveness of the Biden administration's cyber diplomacy, noting some achievements while arguing that the U.S. cyber diplomacy strategy will need further adjustments and optimizations to address the continuously changing global political and economic landscape.

Keywords

biden administration, cyber diplomacy, global cyber governance, cyber security

1. Introduction

With the acceleration of global digitization, cyberspace has been transformed into a core strategic area of national security, economic development and international relations. The swift advancement of cyber technology, although yielding significant economic and social benefits, also presents unprecedented challenges and risks. Issues such as national-level cyberattacks, transnational cybercrime, and

persistent threats to critical information infrastructure have emerged as urgent concerns for the global community. Moreover, as nations increasingly prioritize cybersecurity and the governance of international cyberspace, the contest to establish rules in this domain has emerged as a key battleground in the foreign policy strategies of major powers. The prominence of cybersecurity within international relations has significantly increased, and accordingly, the importance of cyber diplomacy as an essential element of national foreign policy has also escalated.

At the beginning of his presidency, President Biden explicitly stated that bolstering cybersecurity and ensuring the stability of international cyberspace are crucial elements of his foreign policy agenda. In the face of the complex and volatile international cyber environment, the Biden Administration has taken a series of measures to advance the concept of international cyber governance in the interest of the United States and to firmly combat irresponsible behavior in the network.In April 2022, to bolster the efficiency and influence of cyber diplomacy, the Biden Administration formed the Cyberspace and Digital Policy Directorate (CDP), tasked with orchestrating U.S. strategies and operations in cyber diplomacy. This new organizational framework not only centralizes U.S. efforts in addressing global cyber issues, but also signifies a move towards a more systematic and coordinated approach in the realm of cyber diplomacy. The issue of security and governance in cyberspace covers a wide range of areas, including but not limited to the prevention and combating of cybercrime, the formulation of international cyber laws and rules, and international cyber cooperation and confrontation. In this context, the Biden administration is tasked with three critical objectives: firstly, mending the rifts that emerged between the United States and its allies during the Trump administration; secondly, bolstering U.S. cyberdefense capabilities to preserve national cybersecurity; and thirdly, asserting U.S. leadership in global cyber governance to uphold American hegemony. As President Biden's first term in office draws to a close, this article will delve into the Biden administration's cyber diplomacy efforts, as well as assess the successes and challenges of U.S. cyber diplomacy policy during this period, and analyze its actual influence in the international arena.

2. Definition of Cyber Diplomacy

Currently, there is no universally agreed upon and clear definition of cyber diplomacy within the academic community. Initially, cyberspace was viewed as a “global commons”, and its related problems were mainly regarded as technical in nature, with rules for their solution being formulated by the corresponding technical experts. Consequently, the scholarly interpretation of cyber diplomacy aligns with this viewpoint, equating it with digital diplomacy. This perspective posits that states or non-state actors—including corporations and NGOs—leverage cyberspace, employing cyber tools and technologies to further their diplomatic objectives. However, as technology evolves and cyberspace increasingly intersects with crucial interests like national infrastructure, cyber issues have become internationalized and politicized. Consequently, cyberspace has acquired more political attributes, giving rise to the concept of cyber sovereignty.The cyber agenda's role in foreign policy has garnered

attention from practitioners in the field of diplomacy, prompting the use of diplomatic tools and resources to facilitate cooperation and interaction between state and non-state actors in cyberspace. Allowing only technicians, military, and intelligence agency personnel to manage cyberspace might result in a reversion to a "Hobbesian" state of nature, characterized by chaos and conflict. In light of evolving practices, Western scholars have differentiated between cyber diplomacy and digital diplomacy. They define cyber diplomacy as the application of diplomatic methods, negotiations, and agreements to manage and resolve issues related to cybersecurity within international relations. This approach aims to establish international norms, standards, and rules for cyberspace, prevent cyber conflicts, and foster cooperation among nations to address cyber threats.Digital diplomacy is fundamentally instrumental, serving as a means rather than an end. In contrast, cyber diplomacy employs diplomatic techniques and thought processes to analyze and manage issues that emerge in cyberspace, aligning more closely with traditional diplomatic methods and principles. Although related, cyber diplomacy and digital diplomacy are not interchangeable. Some scholars contend that cyber diplomacy is a dynamic concept, continually evolving through practice. Particularly, the onset of the COVID-19 pandemic has accelerated the digital transformation of traditional methods, blurring the lines between digital and traditional diplomacy. Consequently, further distinctions between the two are now unnecessary.

This article does not aim to delve into the connotations of cyber diplomacy, nor does any official document currently define the term.Despite the complexity of the term, this paper necessitates a clear definition. As the focus of this study is the Biden administration's approach to cyber diplomacy, it adheres to the definition provided by the U.S. Government Accountability Office (GAO): cyber diplomacy is defined as efforts to support U.S. interests in cyberspace internationally, led by the State Department. Elements of this definition include providing foreign assistance to partner countries and engaging in bilateral or multilateral interactions, alongside activities aimed at combating cybercrime, establishing norms for responsible behavior in cyberspace, and developing technical standards.

3. The Biden Administration's Policy Objectives and Means of Advancing Cyber Diplomacy

3.1 Policy Objectives

The Biden administration has built upon the cyberpolicy foundations laid by previous administrations, redefining the core objectives of its cyber diplomacy to address the evolving global political and economic landscape. These objectives not only reflect adjustments in domestic policy but also establish new directions in foreign relations. The Biden administration's goals for advancing cyber diplomacy include reshaping the global cyber alliance, enhancing international cooperation, and asserting dominance in cyberspace governance. Specifically, they can be categorized as follows:

First, the building of global network alliances and partnerships should be strengthened. Early in its tenure, the Biden administration immediately began to repair the crisis of international trust caused by the “America First” policy of the previous administration. By reaffirming the importance of

multilateralism and international cooperation, President Biden enhanced cybersecurity cooperation with traditional allies. This reinforcement was particularly evident in areas such as intelligence sharing, the exchange of cyberdefense technologies, and the conduct of joint cyber exercises. Additionally, the Biden administration has explicitly stated that cyber alliances are not only limited to traditional military and economic powers but also include emerging market nations that are proactive in digital transformation. This policy aims to build a broader network of alliances to collectively address the increasingly complex cyber threats. As noted by U.S. Secretary of State Blinken, cybersecurity is one of the five pillars of modernizing American diplomacy and is central to strengthening alliances and partnerships. This diplomacy is designed to establish a broader circle of cyber alliances, working collaboratively to tackle the increasingly complex cyber threats. U.S. Secretary of State Antony Blinken has also highlighted that cybersecurity represents one of the five pillars of U.S. diplomacy's modernization, serving as a crucial link in strengthening alliances and partnerships.

Secondly, promote global governance and international norms in cyberspace. The “National Cybersecurity Strategy”, released in 2023, is a critical declaration of the Biden Administration's comprehensive commitment to international cyber governance. This strategic document, comprising five pillars, explicitly states that the United States will assume a leadership role in global cyber governance, particularly in the development of a global code of conduct for cyberspace. The Biden Administration advocates for an “open, secure, and trusted” cyber environment, urging enhanced legal and technical cooperation between nations. Additionally, it emphasizes the importance of international collaboration in combating cybercrime and safeguarding online privacy.

Thirdly, maintaining and enhancing U.S. leadership in global cyber technology is a priority for the Biden Administration. Recognizing that dominance in cyber technology reflects economic competitiveness and constitutes a vital aspect of national security, the administration has prioritized bolstering U.S. research and development in critical areas such as artificial intelligence, quantum computing, and 5G technology. Additionally, the U.S. is actively working to diversify and secure the global supply chain, particularly in the sectors of semiconductors and essential technologies. Through partnerships with allies and partner nations, the U.S. aims to establish a more equitable global technology supply chain structure. This structure not only ensures a competitive edge in global technology but also prevents potential adversaries, especially China and Russia, from using technological means to interfere in the internal affairs of the U.S. and its allies.

The formulation of these policy objectives is a direct manifestation of the Biden administration's efforts to sustain its global hegemony. By bolstering cyber diplomacy and fostering international cooperation, the administration aims to solidify its strategic influence and leadership in the global order. By establishing a robust international cyber alliance, advocating for the standardization of global cyber governance, and maintaining a lead in critical technological domains, the Biden administration seeks to ensure that the United States continues to exert a decisive influence on the global political and economic landscape. This layout not only covers deepening cooperation with traditional allies, but also

includes policy investment in emerging market countries in the cyber field, demonstrating the multidimensional and comprehensive nature of U.S. global strategy.

3.2 Means of Advancement

To effectively implement its cyber diplomacy policy, the Biden Administration has adopted a diverse set of measures that reflect a comprehensive approach encompassing technology, diplomacy, and security strategies. These tools are designed to enhance the cybersecurity capabilities of the United States and its allies, advance international norm-setting, and protect critical technology leadership. The Biden Administration emphasizes cross-departmental coordination to ensure consistency and efficiency in cyber policy. To this end, the administration has established the Cyberspace and Digital Policy Directorate (CDP), which is dedicated to coordinating U.S. cyber diplomacy strategy and operations. The directorate not only coordinates domestic and international cybersecurity policies but also oversees collaborations with international bodies, such as the United Nations and the International Telecommunication Union, ensuring the United States' leadership in global cyber governance. Furthermore, the CDP collaborates closely with the Department of Defense, the National Security Agency, the Department of Commerce, and other critical agencies to establish a unified front for cyber defense and diplomacy. In foreign relations, the Biden administration favors advancing cyber diplomacy through an alliance-based approach, aligning with "like-minded" allies and partners to form coalitions. These coalitions work together to coordinate policies and practices for offensive cross-domain cyber deterrence, aiming to influence the behavior of competitors and construct an international order that aligns with U.S. interests. On one hand, the United States must reaffirm its capability and commitment to safeguard the interests of its allies; on the other, the U.S. has consistently emphasized alliance diplomacy since World War II. This strategy proved effective during the Cold War, notably in the containment of the Soviet Union. Now that the U.S.-China rivalry has entered a new phase, with many political observers declaring the onset of a "New Cold War," the U.S. is increasingly reliant on previously proven strategies. In April 2022, the U.S. and over 50 countries issued the Declaration on the Future of the Internet, warning of the threats posed by "digital authoritarianism." This declaration saw more than 60 countries commit politically to foster an Internet that is open, competitive, privacy-protecting, and respectful of human rights.This established the framework for the Biden administration's cyber diplomacy. The Cybersecurity Strategy reflects this policy direction, advocating for the formation of a coalition to address digital ecosystem threats. It emphasizes enhanced collaboration among key allies in sharing threat intelligence, synchronizing cybersecurity practices, and coordinating incident responses, further solidifying this approach.

The cyber alliance is based on cooperation between the United States and its allies, and the Biden administration's cyber alliance can be categorized into the following levels in terms of the paradigm of cooperation. Firstly, the United States heavily relies on its transatlantic alliance, especially NATO, to promote the formation of a future Internet alliance. On one hand, the U.S. views NATO as its most dependable ally, having maintained close relations with NATO member states for years. On the other

hand, most NATO members are developed countries possessing advanced internet technologies and significant sway in the governance of international cyberspace, thereby supporting the U.S. advocacy for a "rules-based international order." Internally, cooperation between the U.S. and NATO countries is focused on high-technology areas such as artificial intelligence and digital technology. In 2021, the U.S. and Europe established the U.S.-European Council on Trade and Science and Technology. After its third ministerial meeting, a declaration was issued stating that both sides would deepen cooperation in digital infrastructure and connectivity, and emerging technologies such as artificial intelligence and quantum information. Additionally, in multilateral cooperation mechanisms, the two parties collaborate on governance rules and agreements. In international organizations addressing global issues, the U.S. and Europe collaboratively propose leaders aimed at dominating cyberspace governance. Doreen Bogdan-Martin, the current Secretary-General of the International Telecommunication Organization, is a notable example of such leadership.

Secondly, the U.S. has enhanced internet cooperation with major non-NATO allies, notably Japan and South Korea. These allies are pivotal to America’s global security strategy and hold key geopolitical positions. Following President Biden's recognition of Kenya as a major non-NATO ally on May 23, 2024, the list of such allies expanded to nineteen. Despite their strategic importance, there is a notable disparity in technological capabilities among these countries, necessitating a tailored approach to cooperation. In technologically advanced nations like Japan, South Korea, Israel, and Australia, the U.S. has focused on high-end technological collaborations. For example, at the 2024 U.S.-Japan Summit, the two countries agreed on a semiconductor cooperation pact aimed at advancing next-generation technologies and enhancing supply chain resilience, alongside investing in human resources for advanced semiconductor research. This agreement covers collaboration on R&D, design, and training, enhancing supply chain stability through shared information and coordinated policies, and expanding research into emerging fields such as quantum computing and artificial intelligence.

Similarly, in 2024, the U.S. and South Korea fortified their cooperation in the 5G technology sector, with a focus on military applications and ICT. At the third U.S.-South Korea ICT Cooperation Committee meeting, both nations agreed to work on applying 5G technology to joint military operations, and to collaborate on defense policy, cybersecurity, and digital infrastructure. Furthermore, the U.S., Japan, and South Korea established a high-level trilateral consultation body to counter the threats posed by North Korea, labeled an 'authoritarian government' by the U.S. This body is dedicated to enhancing cybersecurity cooperation and preventing North Korea from funding its nuclear weapons and WMD programs through cyberattacks.

For the major non-NATO allies in the Americas—Colombia, Argentina, and Brazil—the U.S. has emphasized boosting their cyber defense capabilities. Acknowledging that cyberattacks have broader regional impacts, the U.S. has worked to strengthen cyber defense cooperation through technical assistance for modernizing critical infrastructure, establishing a platform for sharing cyber threat intelligence, and conducting regular joint exercises to improve coordinated responses to cyber

incidents.

Thirdly, integrating the developing world into its strategic framework. In 2024, U.S. Secretary of State Abraham Lincoln addressed the transformative nexus of U.S. science, technology, and foreign policy at San Francisco's Moscone Center. He emphasized America's commitment to fostering amicable relations with a broad spectrum of developing nations, asserting that their technological development and deployment must actively include these countries. Currently, the predominant strategy employed by the United States involves exporting technology to developing countries in exchange for their alignment and cooperation with U.S. policy objectives. For instance, via the 'Digital Hub Africa' program, the United States has facilitated enhancements to the digital infrastructure of African nations and has encouraged these countries to adopt more liberal internet policies. In Latin America, the United States has collaborated with regional countries within multilateral and bilateral frameworks to enhance cybersecurity capabilities.For instance, the U.S. Department of State has initiated the Cybersecurity Partnership Program aimed at bolstering the cyber defense capacities of partner nations through technical exchanges and training programs. This cooperation typically aligns with support for U.S. cyberspace policies and standards. Notably, U.S. engagement in cyberspace champions "small multilateralism", fostering international alliances and partnerships among targeted smaller groups. Given the diverse development levels among developing countries, the U.S. tailors its policies and collaborations accordingly. However, geopolitical considerations remain crucial in selecting partners. The U.S. expects more technologically advanced developing countries to back its efforts in shaping international standards. Universally, the U.S. stipulates that aid-receiving countries must avoid supporting 'authoritarian' states like Russia and Iran.

Finally，Mobilizing multi-stakeholders, including non-State actors such as think tanks, enterprises and non-governmental organizations. On the one hand, compared to government agencies, businesses and non-governmental organizations are often at the forefront of science, technology and innovation and have a deep understanding of market needs, new technologies and future trends. In setting standards and rules that are closely related to the development of the industry, these firms can ensure that the rules further promote technological innovation. At the same time, businesses and NGOs have greater flexibility to respond quickly to changes and emerging challenges in the industry and to update or develop new standards or rules in a timely manner, a characteristic that is particularly important in areas of rapid technological development, such as artificial intelligence and renewable energy. On the other hand, the United States is home to numerous leading network technology giants, including Microsoft, Google, Qualcomm, and OpenAI. These companies are not only pioneers in their respective fields but also wield substantial technological influence. Their significant role extends beyond mere market leadership; they possess considerable clout in the development of protocols and standards, thereby shaping the landscape of global technology governance. For instance, Qualcomm holds numerous critical patents in 5G technology and occupies a central role in mobile communications. By leading the 5G Alliance, Qualcomm orchestrates the development of technical standards that serve its

interests. The United States strategically integrates non-state actors into its cyber alliances, leveraging control points in the internet supply and technology chains to facilitate or impede access, thereby subtly drawing these actors into cooperative frameworks.

The United States orchestrates various actors into small, U.S.-centered coalitions based on their strengths and roles, directing their global redistribution of tasks within the cyber-technology sector. Firstly, the United States aims to establish a secure technology supply chain, necessitating the exclusion of untrustworthy nations or firms and the enhancement of product quality. In the 21st century, as production globalization intensifies, this approach mandates a global restructuring of supply chains. Consequently, the U.S. forms smaller, specialized alliances rather than a single large one, aligning them according to the technological and scientific capabilities of the nations involved. Cooperation with G7 countries and the U.S.-Japan-South Korea alliance typically concentrates on advanced technology sectors, including semiconductors, high-end manufacturing, artificial intelligence, and quantum computing. These countries possess advanced technologies and R&D capabilities, thus cooperation predominantly revolves around technological innovation, research and development, and the sharing and co-development of high-end manufacturing technologies. Conversely, collaboration with countries possessing weaker scientific and technological capabilities primarily emphasizes infrastructure construction, technology transfer, and capacity building. For instance, through assistance programs, the U.S. has supported these countries in building communication networks and enhancing local manufacturing capabilities, activities typically associated with the midstream and downstream sectors of the supply chain. These various small alliances, orchestrated by the United States, leverage their unique technological strengths to deliver top-quality products. Simultaneously, these alliances subject member countries to U.S. constraints and compel them to align with the United States in the geopolitical contest between the U.S. and China. The U.S. strategy seeks to 'decouple' from China and curb Chinese advancements in science and technology, a process known as 'de-Sinicization' that could lead to significant economic losses. Historically, the Second Industrial Revolution marked the U.S.'s ascent to global power by leading industrial production by the late 19th century, which laid the groundwork for its economic hegemony post-World War I. Currently, it is believed that the fourth technological revolution has commenced, with artificial intelligence as a potential hallmark. Drawing on historical precedents, the U.S. undoubtedly views this technological revolution as crucial to sustaining its global dominance. With visible declines in U.S. hegemony and challenges to the post-World War II international order, maintaining technological superiority remains a vital strategy. Furthermore, as cybersecurity emerges as the fifth domain of warfare—joining land, sea, air, and space—and given the borderless nature of cyberspace, the concealment and diversity of cyber threats necessitate international cooperation for effective mitigation.

4. Critique and Challenges of the Biden Administration's Cyber Diplomacy

Grand strategy encompasses the art and science of developing, employing, and synchronizing the diverse elements of national power—diplomatic, economic, military, informational, and others—to secure national security objectives over a long-term horizon. It prioritizes the nation's core security interests and aligns them with its most critical strategic imperatives. The Biden administration's cyber diplomacy fundamentally integrates within its broader cybersecurity strategy. The effectiveness and implementation of this strategy will necessitate longitudinal observation to fully assess its impact and success.

4.1 Progress in Cyber Diplomacy

Biden is nearing the end of his first term as President. During this period, the United States has made significant progress in the areas of cyber diplomacy and international cybersecurity cooperation. For one, according to a GAO report, the United States has used the number of parties to the Convention on Cybercrime, signed in Budapest in 2001, as one of the indicators of its progress in cyber diplomacy. The Convention provides an internationally recognized legal framework that enables countries to cooperate in addressing transnational cybercrime while respecting their respective legal systems. And by defining a wide range of cybercrimes, such as data jamming, system interference, and cyberfraud, it provides States parties with a common set of legal terminology and standards, which is critical for international law enforcement to cooperate in the investigation and prosecution of cybercrime. For the U.S., it is an important tool for the U.S. to demonstrate leadership in the global cybersecurity arena, maintain cyber stability, and promote the synergy of law and technology. Between 2021 and 2024, the number of parties to the Budapest Convention on Cybercrime increases from 43 to 68 countries, adding 25 new parties. The role of the United States in promoting the Budapest Convention emphasizes its leadership in international cyber policymaking. Through this leadership, the United States has not only strengthened its cooperation with traditional allies, but has also fostered relationships with emerging markets and developing countries, which is critical to maintaining its global cybersecurity leadership. In addition, by boosting the cybersecurity capabilities and resources of partner countries, the U.S. is indirectly enhancing its own national security and cyber defense capabilities. According to a newly released White House report, in 2023, U.S. federal agencies reported a whopping 32,211 cybersecurity incidents, an increase of 9.9 percent year-over-year. Although the number of attacks has been increasing each year, no incidents have exceeded the "medium" level of the National Cyber Incident Scoring System (NCISS). "Medium" rating from the National Cyber Incident Scoring System (NCISS). Second, the United States has enhanced its presence in other countries and regions through bilateral or multilateral mechanisms. For example, the United States and its allies and partner nations have effectively increased the speed of identification and response to sophisticated cyberattacks through information-sharing and joint response agreements to cyberthreats. Active participation in international organizations, such as INTERPOL and Europol, has strengthened international law enforcement cooperation and increased the detection rate of transnational cybercrime and the efficiency of the fight

against it. The United States has played an active role in global cyber governance, promoting the development and implementation of international cyber policy. On multilateral platforms such as the United Nations, the United States advocates for an open, secure and credible cyberspace and supports the development and implementation of an international cyber code of conduct. Through these collaborations, the United States has been able to disseminate its own concepts and values of global cybergovernance and make the development of global networks more consistent with its own interests and needs.

Third, the United States has used diplomatic means on the global stage to restrict China's scientific and technological development. On the one hand, the United States has imposed a series of restrictions and sanctions on Chinese science and technology companies, especially those that are competitive in the global market. This includes placing Chinese tech giants such as Huawei and ZTE on the Entity List and restricting them from doing business with U.S. firms, especially with regard to the export of key technologies and software. In addition, the U.S. has increased its scrutiny of Chinese investments through various policy and legal tools, such as the Foreign Investment Risk Review Modernization Act (FIRRMA), to prevent its technology from gaining access to advanced science and technology through mergers and acquisitions of U.S. companies. On the other hand, the U.S. government and media have frequently accused China and Russia of cyber espionage and other forms of cyberattacks, and these allegations are often coupled with specific evidence, such as cyber intrusions into government agencies, critical infrastructure, and U.S. businesses. By emphasizing the cyber activities of these countries, the United States has shaped the international perception that China and Russia are using their cyber capabilities to conduct information warfare and influence operations, which are not only a direct threat to the United States, but also a challenge to global cybersecurity. In addition, the United States has leveraged its influence in international organizations and multilateral forums to promote international condemnation of cyberattacks and cyberespionage, which has increased international attention and response to the issue. This approach has strengthened the U.S. image as a global cybersecurity leader while setting the moral and legal tone for its technological and foreign policy toward China and Russia. The Biden administration formally viewed China as its biggest competitor in its National Security Strategy, and through diplomacy and public opinion building, it not only slowed down and limited China's technological development, but also disseminated U.S. Internet values.

4.2 The Future Prospects of U.S. Cyber Diplomacy

Strategy execution can be broken down into three components: strategic layout, strategic implementation, and strategic adjustment. While the Biden administration's cyber diplomacy has seen some achievements, numerous challenges persist in meeting its established policy objectives, necessitating continual refinements to its cybersecurity strategy. Furthermore, President Biden’s announcement on July 21st that he will not seek reelection has significantly heightened the uncertainty surrounding the future of his administration’s cyber diplomacy efforts.

Firstly, the rapid evolution of technology. The swift advancement of cyber technology is a hallmark of

modern society and simultaneously presents substantial challenges to the Biden administration's cybersecurity and foreign policy initiatives. The relentless progression of technology, notably in fields like artificial intelligence, quantum computing, the Internet of Things, and 5G, has significantly transformed economic and social landscapes while simultaneously altering the cybersecurity threat environment. The adoption of these cutting-edge technologies has added complexity to cyber systems, challenging conventional security measures with increasingly intricate and automated cyberattack methods. Consequently, governments must persistently revise their cybersecurity strategies to keep pace with these technological advancements. This necessitates that governments not only bolster their technical detection and defense capabilities but also foster close collaborations with the private sector and academic institutions to explore and establish new security technologies and protective measures. Furthermore, the rapid pace of technological advancement demands that legal and policy frameworks adapt swiftly to address emerging privacy and ethical concerns. However, the development of laws and policies frequently lags behind technological innovations, exacerbating the uncertainty and complexity involved in policy implementation.

Secondly, numerous countries hesitate to align themselves with either China or the United States. In the context of escalating Sino-American competition in technology and cyberspace, the global community faces a complex choice: whether to side with one or remain neutral. Many nations, particularly developing and smaller states, often opt for neutrality or attempt to balance relations with both powers, aiming to sidestep direct involvement in confrontations. This stance is influenced by careful considerations of economic dependencies, geopolitical influences, and domestic political stability. Specifically, some nations do not unequivocally align with either superpower but rather choose to hedge by betting on both sides. This approach, often summarized by scholars as 'economically dependent on China, security reliant on the United States,' embodies a strategy of hedging. For the Biden administration, this ambivalence poses significant challenges to building global cyber alliances, advancing cyber governance standards, and effectively countering Chinese influence on the international stage. Particularly in critical technological domains, such as the construction of 5G networks and the application of artificial intelligence, this hesitation to take sides complicates the United States' efforts to foster a broad international consensus. Such reluctance hinders the effective implementation of the U.S. global strategy, impacting its ability to set international standards and shape the technological landscape.

Furthermore, deep political polarization within the U.S. significantly challenges the Biden administration's cyber policies. In Congress, stark differences between political parties manifest in their divergent stances on critical issues like cybersecurity, data privacy, and the regulation of technology firms. Republicans argue that social media platforms are overly regulated, impinging on free speech, whereas Democrats contend that these platforms are insufficiently regulated, allowing rampant hate speech, misinformation, disinformation, and illegal content. This partisan divide not only complicates the drafting and enactment of legislation but also jeopardizes the consistency and stability of policy.

Furthermore, the split within domestic political parties and the inconsistency of interest groups' demands pose another significant challenge. On one hand, the sharp polarization in U.S. domestic politics significantly challenges the Biden administration's cyber policy. In Congress, political parties hold starkly different positions and policy propositions on key issues such as cybersecurity, data privacy protection, and regulation of tech companies. Republicans argue that social media is over-regulated, infringing on free speech, while Democrats contend that social media is under-regulated, rife with hate speech, misinformation, disinformation, and illegal content. This division not only impacts the formulation and passage of relevant legislation but also threatens the coherence and stability of policies. In the context of the Russia-Ukraine conflict, the U.S. staunchly supported Ukraine and planned to provide up to $61 billion in military aid (including cyber defense assistance). However, the passage of this aid bill was delayed for months beyond its scheduled approval, pushed through by House Speaker Mike Johnson in the face of vehement opposition.

Lastly, as the Biden administration approaches the end of its term, concerns about policy continuity and sustainability are intensifying. Donald Trump's immediate response to the shooting incident at a Pennsylvania campaign rally on July 13, 2024, has significantly boosted his support compared to Biden's; additionally, the Republican Party's nomination of JD Vance as its vice-presidential candidate, who hails from Ohio, a pivotal swing state, further highlights these concerns. Emerson College's poll indicates that former President Trump leads President Biden in seven swing states. Nationally, 46% of registered voters support Trump, 42% support Biden, and 12% remain undecided. Divisions within the Democratic Party and declining poll numbers have prompted Biden to withdraw from the 2024 race in favor of his Vice President, Harris. Harris shares Biden's policy philosophy, and her election could lead to adjustments in the current cyber diplomacy policy, though major changes in goals and methods are unlikely. Trump's foreign policy, characterized by the "America First" doctrine, contrasts with Biden's approach, and this discrepancy could prompt U.S. allies to seek new cooperative opportunities with China as a hedge against Trump's potential re-election. This uncertainty could adversely affect international cooperation, especially in fields like cybersecurity and diplomacy, which depend on long-term collaboration and trust. Discontinuity in policy may erode international partners' trust in the U.S. and deter their participation in U.S.-led cyber governance and security alliances. Moreover, instability in policy could impact the confidence of investors at home and abroad in key technology sectors, thereby influencing the U.S.'s standing and influence in global scientific and technological competition.

5. Conclusion

During the Biden administration's tenure, cybersecurity and cyber diplomacy have received unprecedented attention, reflecting its concern for and active participation in global cybergovernance. Throughout this period, the United States has been dedicated to preserving its influence and leadership in global cyberspace. This commitment has been demonstrated through the strengthening of

cybersecurity measures, the promotion of international cyber governance regulations, and the establishment of cyber alliances aimed at fostering international cooperation. Nevertheless, these initiatives have also unveiled multiple challenges, such as navigating rapid technological changes, contending with domestic and international political interference, and facing off against global strategic adversaries.

The Biden administration's cyber diplomacy policy, despite its achievements in enhancing multilateral cooperation and international norm-setting, continues to be tested by the speed of technological updates, changes in the international political environment, and the consistency of domestic policies. Especially within the U.S., political divisions and the pluralistic demands of interest groups have challenged the coherence and implementation of cyber policy. In addition, the intensification of U.S.-China competition in science and technology and cyberspace has tested U.S. diplomatic strategy and international influence. In the future, no matter who is elected as the new U.S. president, the U.S. cyber foreign policy needs to be adjusted. On the one hand, it should enhance its ability to synchronize with the development of emerging technologies, and manage the security risks posed by new technologies through rapid adaptation of laws and policies; on the other hand, it should strengthen the coordination and consistency of its internal policies to ensure the stability and effectiveness of its cyber policy. On the international stage, the United States needs to continue to promote the construction of an inclusive international cyber alliance to balance the global power structure, especially in the cyberspace competition with China and other major countries, to find a balance between cooperation and competition.

References

Antony, J. B. (2024). *Technology and the Transformation of U.S. Foreign Policy*. Retrieved May 14, 2024, from https://www.state.gov/technology-and-the-transformation-of-u-s-foreign-policy/

Cyberspace Solarium Commission. (2024). *A Warning from Tomorrow*. Retrieved March 11, 2024, from https://www.insurancejournal.com/research/research/u-scyber-space-solarium-commission/

Gu, C. N., & Sun, C. H. (2024). Analysis and Insights on the Biden Administration's National Cybersecurity Strategy. *Journal of Intelligence*, *43*(04), 46-53.

Han, Z. Y., & Huang, Z. L. (2019). American Grand Strategy in the Post-Cold War Era: Aims,Threat Perception and Strategic Practice. *Contemporary Asia-Pacific Studies*, (05), 30-67+145-146.

Li, Y., & Sun, B. Y. (2021). The Policy Evolution, Organization System and Development Trend of U.S. Cyber Diplomacy. *Information Security and Communications Privacy*, *12*, 59-69.

Ling, S. L. (2023). Splitting Cyberspace and Building Walls: Biden's "Alliance for the Future of the Internet". *International Forum*, *25*(02), 41-60+156-157.

Ministry of Commerce of the People's Republic of China. (2024). *U.S.-EU Trade and Technology Committee will conduct cooperation in digital technology and other fields*. Retrieved April 13, 2024, from http://chinawto.mofcom.gov.cn/article/ap/p/202301/20230103377733.shtml

NATIONAL CYBERSECURITY STRATEGY. (2024). Retrieved April 11, 2024, from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

NK NEWS. (2024). *US, South Korea and Japan to form council to counter North Korean cyber threats*. Retrieved April 28, 2024, from https://www.nknews.org/2023/11/us-south-korea-and-japan-to-form-council-to-counter-north-korean-cyber-threats/

Qi, H. X. (2024). The Risks of Hedging in China-U.S. Competition. *The Journal of International Studies*, *45*(02), 61-77+6.

Riordan, S. (2024). *Cyber Diplomacy vs. Digital Diplomacy: A Terminological Distinction*. Retrieved March 19, 2024, from https://uscpublicdiplomacy.org/printpdf/60751

Rishi, I. (2024). *Washington Takes Its Cyber Strategy Global*. Retrieved May 21, 2024, from https://foreignpolicy.com/2024/05/08/biden-cybersecurity-strategy-blinken-fick-rsa-conference-diplomacy/

Security Inside. (2024). *Disclosure of 11 major events! U.S. government releases 2023 cybersecurity annual report*. Retrieved June 15, 2024, from https://www.secrss.com/articles/67058

The White House. (2024). *United States-Japan Joint Leaders' Statement*. Retrieved April 26, 2024, from https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/10/united-states-japan-joint-leaders-statement/

United States Government Accountability Office. (2024). *Cyber Diplomacy: State's Efforts Aim to Support U.S. Interests and Elevate Priorities*. Retrieved March 21, 2024, from https://www.gao.gov/assets/d24105563.pdf

Zuo, X. Y., & Tang, S. P. (2012). Understanding Strategic Behavior: A Preliminary Analytical Framework. *Social Sciences in China*, (11), 178-202+207.