Asaba Journal of History and International Studies: Department of History, Strategic And International Studies, Dennis Osadebay University, Asaba, Delta State, Nigeria
Volume 1, Number 2 , Nov. – Dec Edition 2025, ISSN: 1595-3467

CYBER DIPLOMACY: THE ROLE OF TECHNOLOGY IN CHINA'S INTERNATIONAL RELATIONS

Okwuobi, Ifeyinwa Augustina
Dept of History, Strategic and International Studies, Dennis Osadebay University, Anwai, Asaba.
augustina.okwuobi@dou.edu.ng

Abstract

Cyber diplomacy has emerged as a critical frontier in international relations, with technology increasingly shaping the way states interact, negotiate, and assert influence on the global stage. This paper examines the role of technology in China's international relations, focusing on how cyber capabilities, digital infrastructure, and information control have become central to its diplomatic strategies. It explores China's approach to cyber sovereignty, its promotion of the Digital Silk Road, and its efforts to shape global norms on internet governance through bilateral and multilateral engagements. The study also analyses China's cybersecurity posture and its implications for geopolitical power dynamics, particularly in relation to the United States, the European Union, and emerging economies. Through a qualitative assessment of policy documents, official statements, and international responses, the paper highlights how cyber diplomacy not only serves China's strategic interests but also redefines traditional diplomacy in the digital age. The findings suggest that China's integration of technology into its foreign policy is both a tool of influence and a mechanism for safeguarding its national interests in an increasingly interconnected world.

Keywords: Cyber Diplomacy, China, Technology, China, Interest

Introduction

The 21st century has witnessed a transformative shift in international relations, driven largely by the rapid advancement of digital technologies (Segal, 2020). Among the key developments in this new diplomatic landscape is the rise of cyber diplomacy, a field where states leverage technological tools and cyber capabilities to shape foreign policy, secure national interests, and influence global norms. At the forefront of this evolution is China—a nation that has not only emerged as a global technological powerhouse but also as an assertive actor in cyberspace diplomacy (China State Council 2010).

China's growing integration of technology into its foreign policy is evident in its pursuit of cyber sovereignty, investment in global digital infrastructure through initiatives like the Digital Silk Road, and active participation in international forums on internet governance. These efforts reflect a strategic vision in which cyberspace is both a domain of competition and

cooperation. As China promotes its own model of digital development and governance, it challenges the traditionally Western-led frameworks of internet freedom, data privacy, and digital rights (Segal, 2020).

However, this strategic use of technology in diplomacy is not without controversy. Concerns over cybersecurity, digital surveillance, and cyber-enabled interference have heightened tensions between China and other global actors, particularly the United States and the European Union. As the line between technological advancement and geopolitical influence continues to blur, understanding the role of technology in China's international relations becomes critical (World Economic Forum, 2023).

This study explores the concept of cyber diplomacy within the context of China's foreign policy, analyzing how technological tools are being employed to expand diplomatic influence, shape global digital norms, and manage international relationships in an increasingly interconnected and contested cyberspace.

Statement of the Problem

In the rapidly evolving digital age, the intersection of technology and international relations has given rise to the concept of cyber diplomacy—a strategic domain where states utilize digital tools to pursue foreign policy goals, protect national interests, and influence global norms. China, as a rising global power, has increasingly integrated technology into its diplomatic strategies through initiatives such as the Digital Silk Road, cyber sovereignty advocacy, and its participation in global internet governance forums. However, this growing cyber influence presents complex challenges and raises concerns among the international community. There is a lack of consensus on the norms and rules governing state behavior in cyberspace, leading to tensions over issues like data security, digital surveillance, and cyber espionage. Despite China's expanding role in shaping the global digital order, scholarly understanding of how technology functions as a tool of diplomacy in its international relations remains limited and fragmented. This research seeks to address the problem by critically examining how China employs technology in its foreign policy, the implications for global cyber governance, and the broader impact on international diplomatic relations and geopolitical stability.

Cybersecurity

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks (Triolo, et-al. 2020). It's also known as information technology security or electronic information security.

Cyber diplomacy

Cyber diplomacy is the practice of using diplomatic tools and strategies to manage international relations in cyberspace. It involves nations, groups, and individuals engaging in diplomatic efforts to safeguard their interests, promote their political, economic, and cultural relations, and maintain peaceful relationships in the digital realm (Triolo, et al. 2020). Essentially, it's about

applying traditional diplomatic principles to the unique challenges and opportunities presented by the internet and digital technologies.

Historical Evolution of China's Cyber Diplomacy

China's approach to international technology engagement has long emphasized "cyber sovereignty" – the idea that states control their own internet space. This concept first appeared in China's 2010 Internet White Paper and was later enshrined in the 2017 "International Strategy of Cooperation on Cyberspace," which asserts each country's right to choose its own cyber regulations (Segal, 2020). Over the 2010s, China built state institutions (e.g. the Cyberspace Administration of China) to coordinate internet policy and began hosting the annual World Internet Conference in Wuzhen, promoting its vision of norms for a controlled, state-centric internet. By the mid-2010s Beijing also began integrating technology into its Belt and Road Initiative, announcing a "Digital Silk Road" in 2015 to export Chinese telecom, surveillance and e-commerce technology abroad. In parallel, China engaged in state-level cyber dialogues (e.g. a 2015 U.S.–China cyber agreement committing both sides to refrain from cyber theft of economic secrets) even as it continued to emphasize bilateral and multilateral rule-making under UN and Shanghai Cooperation frameworks. This evolution set the stage for more recent tech-driven diplomacy.

Major Government Policies and Initiatives

Cybersecurity and Data Laws: China enacted a comprehensive Cybersecurity Law in 2017, requiring data localization and stricter controls on networks. In 2021 it implemented a Data Security Law and a Personal Information Protection Law, imposing broad new restrictions on cross-border data flows (Segal, 2020). Together, these domestic laws aim to tighten Beijing's control over data while projecting Chinese standards globally (e.g. by demanding "secure development" and banning foreign data access.

Digital Silk Road (DSR): Launched in 2015 under the Belt and Road Initiative, the DSR finances overseas telecommunications, cloud, AI, e-commerce, smart city, and surveillance projects. China has signed DSR agreements with dozens of countries, using firms like Huawei, ZTE, Alibaba and others to build infrastructure. For example, China already provides more financing for African ICT projects than all Western donors combined (Zhang, 2022). The DSR explicitly supports Chinese exporters in strategic technology sectors.

Global Data Security Initiatives: In September 2020 President Xi proposed a Global Data Security Initiative (GDSI), a diplomatic framework of eight principles for "open, secure" data flows and mutual non-interference (Triolo, Et-al. 2020). The GDSI was widely seen as a response to the U.S. "Clean Network" campaign against Chinese tech, and China has courted partners (Russia, Pakistan, Tanzania, Ecuador, the Arab League and ASEAN states) to endorse it. More recently, China launched a broader Global Security Initiative in 2023–24, which includes a Global Initiative on Data Security and an AI Governance Initiative as key components (Boulanin, and Verbruggen, 2021). These initiatives reiterate China's push for

multilateral (government-to-government) rule-making in cyberspace and foreign cooperation on "cybersecurity" under Chinese terms.

Other Tech Diplomacy Efforts: China's foreign ministry and party think-tanks have also advanced projects like the Digital Economy Cooperation Initiative (proposed in G20/G20 Leaders' messages) and joint cyber capacity-building programs with developing countries. It has promoted international data governance norms (e.g. at the UN and ITU) favoring state-led standards (Zhang, 2022). At global summits, Chinese leaders stress themes like "common, cooperative, and sustainable security," pushing back against Western multistakeholder models.

Bilateral and Multilateral Cyber Engagements

China's cyber diplomacy involves a patchwork of agreements and dialogues:

- **United States:** The two countries signed a landmark 2015 cyber MOU under Obama (committing both to not conduct cyber-enabled theft of intellectual property). Under Trump and Biden this dialogue stalled, but China remains a focus of U.S. policy – from the Trump-era "Clean Network" to Biden's chip export controls. High-profile cybersecurity incidents (e.g. U.S. indictments of Chinese APT hackers) have increased tensions (Zhang, 2022).
- **Europe and NATO:** The EU conducts a cybersecurity dialogue with China (first high-level talks circa 2018) but has no binding pact. EU member states have assessed Chinese tech as a security risk: France, Sweden and others have restricted Huawei/ZTE from 5G networks in line with EU guidelines. The EU has launched digital regulatory initiatives (like the Data Act and Digital Services Act) that affect Chinese companies, and NATO's 2022 Strategic Concept explicitly calls China a systemic security challenge.
- **Russia and Eurasia:** China and Russia describe their partnership as a "no limits" strategic coordination. They routinely coordinate on cyber issues through the Shanghai Cooperation Organization (SCO), which has agreed on joint counter-terrorism and cybersecurity conventions. In recent Xi-Putin communiqués, the two countries have reaffirmed cooperation on "network and data security" and Internet of Things security.
- **Asia-Pacific (ASEAN, India, etc.):** China engages ASEAN through regular ICT ministerial meetings and the ASEAN-China Information Superhighway project. At the SCO, China aligns with Central Asian partners on cyber norms. Relations with India have soured – in 2020 India banned dozens of Chinese apps (TikTok, WeChat, etc.) citing data security after border clashes. China also dialogues with Japan and South Korea on tech issues, though technical cooperation is limited by geopolitical competition.
- **Africa:** China has expanded cyber diplomacy in Africa via the Forum on China-Africa Cooperation (FOCAC). It offers training centers, e-government projects, and standards cooperation under the Belt & Road framework. For instance, Chinese firms have built

national fiber-optic networks and satellite ground stations in many African countries. These projects are coupled with Beijing's call for countries to respect each other's cyber laws and to jointly fight cybercrime under Chinese leadership.

- **Middle East:** China and the Arab League signed a "Data Security Cooperation Initiative" in 2021 – the first time a regional bloc adopted China's GDSI principles. China also partners with Middle Eastern countries (e.g. UAE, Saudi Arabia) on AI, smart cities, and surveillance programs. In broader forums (e.g. G20, BRICS Summits), China promotes digital development goals with Middle Eastern participation.
- **Latin America & Others:** China holds digital economy dialogues with Latin American blocs (e.g. China-CELAC). Several Latin American countries have adopted Chinese 5G or broadband technology (some later restricted), and China offers financing through the Asia Infrastructure Investment Bank and BRI for ICT projects (Zhang, 2022).
- **International Organizations:** China is active in UN cyber governance. It has participated in the UN Groups of Governmental Experts (UNGGEs) and the ongoing Open-Ended Working Group (OEWG, 2021–2025) on ICT security. China consistently argues for applying international law in cyberspace and is working to incorporate its data governance norms into UN resolutions (Triolo, Et-al. 2020). It also lobbies within the International Telecommunication Union (ITU) for standard-setting influence. Domestically, China hosts the annual World Internet Conference (Wuzhen Summit), showcasing its vision of a state-led, multi-government internet order

Role of Chinese Tech Corporations in Foreign Policy

Chinese technology firms have become tools of Beijing's global strategy:

- **Huawei and ZTE:** These telecom giants spearhead China's overseas infrastructure push. They build 4G/5G networks, data centers, and undersea cables in BRI partner countries (e.g. Huawei Marine has completed dozens of cables in Asia). Despite bans in the U.S., UK, and elsewhere, Huawei still dominates networks in Africa, Asia and parts of Europe. The companies also co-finance tech projects with Chinese state banks. Their global footprint advances China's technical standards and gives Beijing leverage in foreign communications infrastructure (Ministry of Foreign Affairs of the People's Republic of China, 2017).
- **Alibaba and Tencent:** These companies export e-commerce platforms, cloud services, and payment systems. For example, Alibaba owns Lazada (a leading e-commerce platform in Southeast Asia) and has invested in payment startups across Asia (Zhang, 2022). Tencent and Baidu back ventures in AI and digital services abroad (ride-hailing apps like Grab and Go-Jek, local AI research partnerships, etc.). By embedding Chinese apps and online services in other economies, they extend China's digital ecosystem globally (Ministry of Foreign Affairs of the People's Republic of China. 2017).

- **ByteDance (TikTok):** China's social media firms have become flashpoints. TikTok's success worldwide drew scrutiny and bans (U.S. and others citing data/privacy concerns). These controversies have entered diplomatic arenas, with China arguing that tech rules should be fair and non-discriminatory (Ministry of Foreign Affairs of the People's Republic of China. 2017).
- **Supply Chains & Standards:** Beyond products, Chinese companies drive standards-setting (e.g. Huawei's role in 5G specifications, China's promotion of a domestic OS). Beijing actively involves firms in setting international norms (e.g. in AI and "New Generation AI Governance Initiative") (China State Council 2010). In sum, Chinese tech firms act as de facto ambassadors of China's "cyber-sovereignty" model by exporting hardware/software and aligning them with Chinese regulations and norms.

International Organizations and Internet Governance

China actively engages in multilateral forums to promote its cyber agenda. In the United Nations, it has been a leading voice for consensus on cyber norms, participating in each UN cyber GGE and the current OEWG (China State Council 2010). It emphasizes non-interference and the role of states over non-state actors, seeking to enshrine its concepts (e.g. data sovereignty) in UN documents (Boulanin, and Verbruggen, 2021).

In telecommunications, China works through the International Telecommunication Union (ITU), advocating for standards that favor national control. Domestically, China's Cyberspace Administration runs the World Internet Conference (Wuzhen Summit) each year, inviting global officials to endorse China's model of internet governance. China also participates in global networks like BRICS and SCO, pushing for cyber capacity-building in the Global South. Through these channels, Beijing aims to shape the evolving rules of the internet so they align with its interests – promoting a state-centric, multipolar digital order as a counterpoint to Western-led multistakeholder governance (Segal, 2020).

Conclusion

China's cyber diplomacy has emerged as a pivotal pillar of its foreign policy, strategically combining technological exports, digital infrastructure investments, and normative agenda-setting to advance its global influence. From the Digital Silk Road to the Global Data Security Initiative, China has sought to reshape global internet governance by promoting a model centered on state sovereignty, data control, and multilateral rule-making (Segal, 2020). While this approach has won favor among many developing nations, particularly in Africa, Asia, and the Middle East, it has also triggered growing friction with Western democracies concerned about surveillance, cybersecurity risks, and digital authoritarianism (Zhang, 2022). As technology becomes increasingly entangled with national security and global power dynamics, China's cyber diplomacy is redefining international relations and creating new alignments and divisions in global digital governance.

Recommendations

1. **Promote Transparent Multilateral Engagements:** China should increase participation in open, transparent dialogues with diverse international stakeholders (including civil society and private sector actors) to foster trust and reduce fears of cyber authoritarianism.
2. **Strengthen Cybersecurity Confidence-Building Measures (CBMs):** By cooperating with global partners on cyber incident response and threat mitigation, China can help defuse tensions and demonstrate its commitment to a stable cyberspace.
3. **Ensure Ethical Tech Deployment Abroad:** Chinese technology firms and government agencies should adhere to ethical standards and local laws in host countries, especially regarding surveillance, privacy, and digital rights.
4. **Enhance Collaboration with International Organizations:** China should continue active roles in the UN, ITU, and other forums to harmonize its cyber norms with broader international standards and bridge ideological gaps in internet governance.
5. **Encourage Domestic-Global Norm Alignment:** As Chinese data and cybersecurity laws evolve, alignment with global best practices on personal data protection and internet openness can enhance Beijing's soft power and mitigate foreign pushback.

References

Boulanin, V., & Verbruggen, M. (2021). *Artificial Intelligence and Autonomy in Weapon Systems: Understanding the Legal and Ethical Challenges*. Stockholm International Peace Research Institute.

China State Council. (2010). *White Paper on the Internet in China*. Retrieved from http://english.www.gov.cn

Ministry of Foreign Affairs of the People's Republic of China. (2017). *International Strategy of Cooperation on Cyberspace*. Retrieved from https://www.fmprc.gov.cn

Segal, A. (2020). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. PublicAffairs.

Triolo, P., Allison, K., & Brown, E. (2020). *China's Cyber Diplomacy in a New Era of Digital Governance*. Eurasia Group.

U.S.–China Economic and Security Review Commission. (2024). *Annual Report to Congress*. Retrieved from https://www.uscc.gov

UN Open-Ended Working Group (2021–2025). *Progress Reports on Cyber Norms and Confidence-Building Measures*. United Nations Office for Disarmament Affairs.

World Economic Forum. (2023). *Cybersecurity Futures 2030: Navigating a Multipolar Digital Order*. Retrieved from https://www.weforum.org

Zhang, B. (2022). *Digital Silk Road and Global Tech Competition*. *Journal of Contemporary China*, 31(135), 511–528.