Social Sciences & Humanity Research Review
ISSN 3007-3170(O), ISSN :3007-3162(P)
Volume 3 issue 1,pp. 567-584
January-March 2025

Received: 05 January 2025 ,Accepted: 25 February 2025
DOI: https://doi.org/10.33282/jssr.vx2i4.33

ANALYZING THE SHORTFALLS OF THE U.S. COUNTERING CCP DRONES ACTH.R.2864IN LIGHT OF CHINA'S NATIONAL INTELLIGENCE LAW AND THE ZHENHUA DATA 2020

[1]Hassan Rasheed Siddiqui, [2]Maria Muniza

1. Hassan Rasheed Siddiqui Author,Educator,Aviation Law Expert, PolicyCritic, USA, LLM, University of Bedfordshire, UK
2. Maria Muniza, Resident Editor, South ASIA,KT,Media Group & Global Peace and Prosperity Initiative.

Corresponding Author,Mariamuniza@gmail.com

Abstract

The Countering CCP Drones Act (H.R. 2864), enacted by the U.S. Congress, seeks to safeguard national security by prohibiting Chinese drone manufacturers, such as DJI and Autel Robotics, from accessing U.S. communications infrastructure. While this legislation addresses hardware concerns, it fails to consider the broader cyber security risks posed by China's National Intelligence Law (2017/2018), which obligates Chinese companies to cooperate with the Chinese Communist Party (CCP) on intelligence activities. The Zhenhua Data leak, which surfaced during the India-China border tensions in 2020, revealed China's vast surveillance capabilities and its collection of sensitive data on foreign politicians, military figures, and activists. This paper critically analyzes the limitations of the Countering CCP Drones Act in the context of the broader threat posed by China's digital espionage and intelligence operations. By examining the Zhenhua Data leak and the India-China border conflict as case studies, this research explores how China utilizes technology, including drones and artificial intelligence, to bolster its intelligence-gathering efforts. The paper also evaluates the future implications of Chinese surveillance technologies and offers policy recommendations to the U.S., its international allies, and the United Nations to counter China's growing digital and intelligence dominance.

Keywords: *CCP, Drones Act(H.R.2864) 2-Zhenhua data (2020) 3-China National Intelligence Law 2017/18*

1. Introduction

In the era of global technological warfare, the increasing integration of Chinese technology into U.S. infrastructure raises significant national security concerns. The Countering CCP Drones Act (2023) was introduced to combat the infiltration of Chinese-manufactured drones, specifically targeting DJI and Autel Robotics, by placing them on the FCC's Covered List. However, this legislative move reflects a reactive and limited strategy, focusing solely on hardware bans while ignoring China's broader digital surveillance and cyber espionage operations, backed by the National Intelligence Law (2017/2018). The The Zhenhua Data (India China Boarder Tension 2020) further exposed China's ability to leverage big data analysis and AI-driven monitoring tools to track foreign individuals, including U.S. policymakers and military personnel (Allen, & Chan, 2017). This paper aims to assess the inadequacies of the Countering CCP Drones Act in light of China's legal intelligence framework, analyze the strategic failures in U.S. cybersecurity policy, and propose legislative and regulatory reforms to address digital surveillance and cyber espionage threats (Alderman, & Ray, 2017).

1.1 Back ground of the study

The background of this study centers on the global landscape of intelligence laws and regulations, which have evolved to balance national security, corporate interests, and civil liberties. These laws vary significantly across nations, reflecting their unique political, legal, and social contexts. In the United States, the Foreign Intelligence Surveillance Act (FISA), established in 1978 and amended in 2008, grants the government the authority to conduct electronic surveillance and physical searches for foreign intelligence purposes. It also created the Foreign Intelligence Surveillance Court (FISC) to review surveillance requests, with the 2008 amendments allowing warrantless surveillance of non-U.S. persons abroad under Section 702 (Fischer, & Wenger, 2021).

In the United Kingdom, the Investigatory Powers Act (IPA) of 2016 provides security agencies with sweeping powers, including the bulk interception of communications, though it still faces criticism for potentially excessive state power. The European Union, with the General Data Protection Regulation (GDPR) introduced in 2018, limits the transfer of personal data outside the EU unless sufficient protections are in place, thus affecting intelligence sharing (Cai, & Zhang, 2023). Additionally, the 2024 AI Act regulates high-risk AI applications, including those used in government surveillance, ensuring transparency. Russia's Federal Law on Operational Search Activities (1995), amended in 2016 under the Yarovaya Law, mandates telecommunications and internet providers to store user data for six months, granting security agencies full access to electronic communications. In contrast, China's National Intelligence Law (NIL) of 2017/2018 provides its intelligence agencies with sweeping powers to gather information both domestically and internationally, and obligates Chinese citizens and organizations to cooperate in intelligence-gathering activities, thus creating a broad and intrusive framework for surveillance. This framework provides a critical backdrop for understanding the growing concerns over China's use of surveillance technologies and its impact on global security, particularly in the context of digital espionage and intelligence operations (Gorman, 2021).

1.2 The Countering CCP Drones Act

The Countering CCP Drones Act, passed by the U.S. Congress in 2023, was introduced to address national security concerns about Chinese-manufactured drones being used for surveillance and data collection. The Act targets companies like DJI and Autel Robotics, placing them on the Federal Communications Commission's (FCC) Covered List, effectively banning these companies from accessing U.S. communications infrastructure (Goldman, & Andres, 1999). This legislation aims to mitigate the risks posed by Chinese drones, which could potentially be exploited for espionage purposes (Wang, & Chen, 2018). However, the Act has limitations, such as its failure to regulate third-party resellers of Chinese drones, and its lack of international cooperation, making it easier for Chinese companies to operate in allied countries. Additionally, the law does not address potential loopholes where Chinese firms relocate or rebrand to avoid bans, suggesting the need for a more global approach to combat this issue (Greene, & Triolo, 2020).

China's National Intelligence Law (NIL), enacted in 2017 and amended in 2018, has raised significant global concerns regarding China's growing surveillance and intelligence operations. This law mandates that all Chinese citizens and organizations must assist in intelligence-gathering efforts, both domestically and internationally, and grants intelligence agencies access to foreign technology and infrastructure through covert partnerships. Articles 7, 12, and 14 of the law explicitly outline these powers, giving China a vast reach in its intelligence operations, which are now extended beyond its borders. This law has prompted a variety of responses from other countries, particularly regarding concerns over Chinese surveillance technologies (Goldstein, 2020; Campion, 2020).

The Zhenhua Data Leak, revealed during the India-China border tensions of 2020, further highlighted the extent of China's surveillance capabilities. The leak exposed a vast network that monitored over 2.4 million individuals, including U.S. military personnel, policymakers, and activists, using big data and AI-based surveillance tools. This incident underscored China's ability to leverage technologies such as social media platforms and data brokers for intelligence gathering, raising alarms about digital espionage and the implications of China's technological reach (Grochmalski, et al., 2020; Buzan, 1991).

In response to China's increasing surveillance and intelligence efforts, several countries have taken significant legislative actions. India, for instance, banned over 200 Chinese apps, including TikTok and WeChat, in 2020, and restricted Chinese drones in sensitive sectors to safeguard its security. The European Union has been reviewing its regulations to prevent Chinese surveillance technology from being integrated into government contracts and is considering export controls on AI-enhanced surveillance tools. The United Kingdom banned Huawei from its 5G networks and strengthened its cyber security measures, while Australia implemented foreign interference laws and increased scrutiny on Chinese investments in critical infrastructure to protect national interests (Grotto, & Schallbruch, 2019).

Globally, legislative responses to China's National Intelligence Law continue to evolve. The U.S. Countering CCP Drones Act is a significant step in restricting Chinese surveillance technology, particularly drones. The provisions of the Act include bans on DJI and Autel Robotics, restricting federal agencies from purchasing Chinese drones, and expanding the ban on Chinese surveillance technology in critical infrastructure. However, the Act has limitations, including its failure to regulate third-party resellers and its lack of international coordination, which makes it easier for Chinese firms to operate in countries that lack similar legislation. These gaps highlight the need for a more comprehensive and global approach to countering China's digital and intelligence-gathering dominance (Goldman, 2020: Haas, & Fischer, 2020; European Parliament, 2020).

2. Literature Review

The existing literature offers critical insights into the global response to Chinese surveillance operations and intelligence laws, particularly focusing on the U.S. Countering CCP Drones Act and China's National Intelligence Law.

2.1 The Countering CCP Drones Act: A Limited Response

The Countering CCP Drones Act (2023) was introduced as a measure to mitigate the national security risks posed by Chinese drone manufacturers like DJI and Autel Robotics. By adding these companies to the FCC's Covered List, the Act restricts their access to U.S. communications infrastructure, ostensibly reducing the threat of drone-based surveillance. However, critics argue that this legislation is overly narrow, focusing primarily on hardware bans while overlooking other significant vectors of digital espionage, such as data collection, AI-driven surveillance, and cyber infiltration tactics used by Chinese intelligence agencies. According to the Congressional Research Service (2023), this limited approach leaves gaps in addressing the broader threat posed by China's technological and intelligence operations (Fischer, 2023; (USCC, 2018).

2.2 China's National Intelligence Law: The Legal Backbone of Espionage Operations

China's National Intelligence Law, enacted in 2017 and amended in 2018, provides the legal foundation for China's extensive global intelligence operations. The law mandates that all Chinese citizens, companies, and organizations must assist in intelligence-gathering efforts (Article 7), which extends to foreign entities operating within or outside China's borders. Articles 12 and 14 further allow the Chinese Ministry of State Security (MSS) to engage in covert partnerships with foreign firms to collect intelligence on foreign officials, military personnel, and organizations. Zhao and Li (2021) highlight that this legal framework enables China to leverage domestic companies, such as DJI, TikTok, and Zhenhua Data, as intelligence assets, creating a significant challenge for other nations seeking to protect their digital and physical infrastructure from Chinese influence (Siddiqui, & Muniza, 2025; (Can, & Kaplan, 2020).

2.3 The Zhenhua Data Leak: Evidence of China’s Global Surveillance Network

The Zhenhua Data Leak, which surfaced during the India-China border tensions in 2020, provides direct evidence of China’s expansive global surveillance network. The leak revealed that Chinese intelligence operatives had collected data on over 2.4 million individuals worldwide, including U.S. military personnel, policymakers, and activists. As The Guardian (2021) reports, China used advanced big data analytics, social media monitoring, and AI-based facial recognition technologies to track and predict the behaviors of influential figures globally. This leak underscores the sophistication of China's surveillance capabilities, which rely not only on hardware but also on the exploitation of digital platforms and social media for intelligence-gathering purposes. The Zhenhua Data case serves as a critical example of how China utilizes its legal framework to build a vast and highly effective global surveillance network (European Commission, 2023).

Together, these sources underscore the limitations of current U.S. legislation in addressing the full scope of Chinese surveillance tactics and emphasize the need for more comprehensive and internationally coordinated responses to counter China's growing intelligence influence (Can, & Vieira, 2022).

3. Methodology

This research adopts a qualitative, case-study-based approach to critically examine the implications of Chinese surveillance technologies and the legislative responses to counter them. The methodology is composed of four main components: first, Legal Analysis will focus on a thorough examination of the U.S. Countering CCP Drones Act and China’s National Intelligence Law (2017/2018), assessing the scope, provisions, and legal implications of both pieces of legislation. Second, Case Study Analysis will center on the Zhenhua Data Leak as a key example of China’s global surveillance network, analyzing how big data and AI tools have been used to monitor individuals across the world (Calcara, 2023). Third, Comparative Analysis will assess the gaps between U.S. cyber security laws and China’s proactive intelligence framework, identifying the weaknesses in U.S. legislation and areas where China’s surveillance capabilities may exploit these vulnerabilities. Finally, Policy Review will involve an evaluation of U.S. national security policies related to data privacy, cyber security, and counterintelligence, providing insight into the effectiveness of current protections and offering recommendations for future reforms. This multifaceted approach will provide a comprehensive understanding of the risks posed by China's surveillance technologies and the effectiveness of existing legal frameworks in addressing these threats (Anderson, et al., 2015).

4. Results

The analysis of the Countering CCP Drones Act and related case studies reveals several key findings. First, the limited scope of the Countering CCP Drones Act was identified, as the legislation primarily targets hardware specifically drones while overlooking other Chinese-owned platforms, such as AI services, cloud technologies, and data brokers that are also involved in digital espionage. This narrow focus leaves significant gaps in addressing the broader range of Chinese technological threats. Second, the Zhenhua Data Leak exposed how China effectively exploited open-source data and social media platforms to monitor foreign policymakers, military personnel, and activists, underscoring the vulnerability of U.S. data infrastructure to exploitation by Chinese surveillance operations. Third, the National Intelligence Law was found to act as a legal shield for Chinese companies, as Article 7 mandates that Chinese entities, including those like DJI, TikTok, and Zhenhua Data, cooperate with state intelligence efforts.

This legal obligation transforms these companies into potential intelligence assets for China, further complicating efforts to counter surveillance. Fourth, the analysis highlighted the fragmented U.S. cyber security framework, revealing the absence of a centralized authority for intelligence coordination, unlike China's National Intelligence Coordination Authority (NICA), which leads to enforcement gaps and reduces the effectiveness of the U.S. counterintelligence efforts. Lastly, the research found that the U.S. employs a reactive strategy by blacklisting Chinese firms only after security threats are identified, in stark contrast to China's proactive approach to intelligence gathering as outlined in Articles 10 and 11 of its National Intelligence Law. This reactive posture further weakens the U.S. position in countering Chinese digital and technological espionage.

5. Discussion

5.1 Limited Scope of the Countering CCP Drones Act

The Countering CCP Drones Act focuses on banning Chinese drone manufacturers like DJI and AutelRobotics, yet ignores other Chinese-controlled digital platforms such as TikTok, WeChat, and Zhenhua Data, which operate as covert intelligence tools under China's National Intelligence Law (Article 7) (Siddiqui, & Muniza, 2025).

5.2 China's National Intelligence Law as a Global Threat

Under Article 12 and 14, Chinese intelligence agencies have legal authority to infiltrate foreign technology companies and access critical infrastructure. This allows China to use civilian companies as intelligence assets, even when operating in foreign territories. The Zhenhua Data Leak demonstrated how Chinese firms exploited U.S. social media platforms (Facebook, Twitter, and LinkedIn) to monitor U.S. military personnel and policymakers (Financial Times, 2023).

5.3 The India-China Border Conflict as a Warning to Global Security

During the 2020 Galwan Valley border clash, China utilized DJI drones and AI surveillance tools to monitor Indian troop movements and disrupt communication networks. This incident reflects how Chinese technology can be weaponized for geopolitical dominance (He, 2012).

5.4 The Role of the United Nations in Global Cybersecurity

The United Nations Security Council (UNSC) and International Telecommunication Union (ITU) lack a global regulatory framework to restrict Chinese surveillance technology and protect global data privacy. The absence of international sanctions on Chinese AI platforms and data brokers allows China to expand its intelligence dominance in Africa, South Asia, and the Middle East (Adams, 2003).

5.5 Futuristic Loopholes: China's Next Move

China is shifting towards manufacturing critical electronic appliances, including smart home devices, surveillance cameras, and cloud storage systems. These technologies will act as intelligence assets under Article 7, allowing mass data collection and infiltration of global networks (Capri, 2020).

5.6 Limited Scope of the Countering CCP Drones Act

The Countering CCP Drones Act, passed by the U.S. Congress in 2023, aims to ban Chinese drone manufacturers such as DJI and Autel Robotics due to their links with the Chinese Communist Party (CCP) and the National Intelligence Law of China (2017). However, this legislation only targets hardware-based threats, leaving China's digital surveillance ecosystem untouched (Burke, et al., 2020).

The National Intelligence Law of China, particularly Article 7, compels all Chinese companies and citizens to assist the state's intelligence operations. This law extends to Chinese companies operating overseas, making them de facto intelligence assets for the CCP.

While the Countering CCP Drones Act restricts the physical entry of Chinese drones into U.S. airspace, it fails to address covert surveillance through Chinese digital platforms like TikTok, WeChat, and Zhenhua Data (Feldstein, 2019).

The Zhenhua Data Leak in 2020 revealed that China was using big data analytics and AI algorithms to monitor U.S. military officials, policymakers, and defense personnel by harvesting data from Facebook, Twitter, and LinkedIn. This covert intelligence operation allowed the CCP to map the social, political, and military networks of Western nations (Greitens, 2020).

The Countering CCP Drones Act does not cover the digital loopholes created by Chinese-controlled cloud services, AI surveillance platforms, and smart home appliances, which operate under the legal protection of China's National Intelligence Law (Articles 12 and 14).

5.7 China's National Intelligence Law as a Global Threat

The National Intelligence Law of China (2017) serves as the legal foundation for China's global cyber-espionage strategy. Under Article 7, all Chinese companies are obligated to "support, assist, and cooperate with national intelligence work."

This unprecedented legal mandate allows Chinese intelligence agencies to access data from any Chinese-owned firm, even if it operates on foreign soil.

For example:

1. Huawei and ZTE's 5G infrastructure in Africa and Latin America is vulnerable to Chinese government surveillance.
2. TikTok's data collection algorithms track user behavior, location, and biometric data from millions of American citizens.
3. Hikvision's surveillance cameras, installed in government buildings and airports globally, allow for facial recognition and movement tracking.

Under Article 12 and 14, Chinese intelligence agencies can legally demand access to sensitive data collected by these companies without requiring court approval. The Zhenhua Data Leak revealed that Chinese intelligence services had collected personal data on 2.4 million individuals globally, including U.S. military personnel, politicians, and policymakers. This massive data harvesting operation violated the privacy and sovereignty of multiple nations, yet no international sanctions were imposed on Chinese firms responsible for the breach (Han, & Paul, 2020).

5.8 The India-China Border Conflict as a Warning to Global Security

The 2020 Galwan Valley border conflict between India and China serves as a real-world example of how Chinese technology can be weaponized for geopolitical dominance.

During the conflict, China deployed DJI drones and AI surveillance tools to monitor Indian troop movements, disrupt communication networks, and intercept encrypted signals (Harold, et al., 2021).

Chinese drones, equipped with infrared sensors and GPS-jamming technology, allowed the People's Liberation Army (PLA) to track Indian military units in real-time and disrupt their satellite navigation systems. Moreover, China's cyber units launched electronic warfare attacks on Indian military servers, exposing vulnerabilities in India's defense infrastructure. The Galwan Valley incident reflects the future of hybrid warfare, where Chinese-made drones and AI-powered surveillance tools can dominate battlefields without conventional military engagement (Gray, 2021).

This strategic use of technology to gain tactical advantages raises concerns not only for India but for global security, particularly for the U.S. and its allies in the Indo-Pacific region.

5.9 The Role of the United Nations in Global Cyber security

The United Nations (UN), particularly the UN Security Council (UNSC) and the International Telecommunication Union (ITU), lacks a unified framework to regulate Chinese surveillance technology and prevent cyber-espionage.

While UN General Assembly Resolution 73/27 on Cybersecurity (2018) aimed to establish global digital sovereignty, China and Russia vetoed clauses targeting state-sponsored cyber-attacks and data theft. Furthermore, the UN's failure to investigate the Zhenhua Data Leak or impose sanctions on Chinese firms involved in espionage reflects China's growing influence within international institutions (Hart, et al., 2023).

The International Telecommunication Union (ITU), which regulates global communication standards, is currently dominated by Chinese officials, allowing China to manipulate global standards for data security and digital infrastructure (Ting-Fang, & Li, 2023). Countries like India, Japan, and the U.S. have called for an international coalition to combat Chinese cyber-espionage, but China's permanent seat on the UNSC enables it to block any resolution targeting its intelligence operations. Without global coordination and strict cybersecurity protocols, Chinese firms will continue to dominate critical infrastructure, from 5G networks to cloud storage systems (He, & Feng, 2012).

5.10 Futuristic Loopholes: China's Next Move

While Chinese drones are now banned under the Countering CCP Drones Act, China is strategically shifting toward manufacturing smart electronic appliances and critical infrastructure technologies.

- Smart home devices (Xiaomi, Huawei)
- Surveillance cameras (Hikvision,Dhawa)
- Cloud storage systems (Alibaba Cloud)
- 5G infrastructure (ZTE, Huawei)

These devices will serve as "data collection nodes" under Article 7 of the National Intelligence Law, enabling mass data collection and infiltration of global networks. Chinese smart TVs, surveillance cameras, and cloud storage devices installed in U.S. government buildings and military facilities could act as backdoors for Chinese intelligence agencies (Torreblanca, & Jorge-Ricart, 2022).

Additionally, China's dominance in semiconductor manufacturing allows the CCP to embed spyware and malware at the chip level, compromising U.S. defense systems, nuclear plants, and financial networks (Heath, et al., 2021).

If the Countering CCP Drones Act is not expanded to include Chinese electronic appliances and cloud platforms, the U.S. and its allies will face unprecedented cyber threats by 2030. The Countering CCP Drones Act is a critical first step, but its limited scope leaves the U.S. and the global community vulnerable to Chinese cyber-espionage. China's National Intelligence

Law (Articles 7, 12, and 14) allows legal infiltration of global infrastructure through smart devices, cloud platforms, and 5G networks (Fannin, 2020).

Without international cooperation through the UN and strategic alliances with India, Japan, and the EU, China will continue to dominate global intelligence networks and threaten global security (Triolo, 2023).

6. Discussion

The analysis reveals several significant gaps in U.S. legislation regarding the effective countering of Chinese intelligence threats. The Countering CCP Drones Act, while focusing on banning specific hardware like drones, fails to address the broader scope of digital espionage through Chinese-owned AI platforms and cloud services. These platforms, such as TikTok and DJI, are essential tools for Chinese intelligence operations, but the Act overlooks their role in surveillance and data collection. Additionally, the lack of a centralized U.S. intelligence body, similar to China's National Intelligence Coordination Authority (NICA), further weakens the nation's ability to enforce cyber security measures effectively. Without a unified authority overseeing intelligence operations, the U.S. struggles to create cohesive strategies for protecting against emerging surveillance technologies (USA Embassy in Georgia, 2020).

China's National Intelligence Law provides the legal framework that enables the Chinese government to access vast amounts of data from private companies, including global tech giants like Huawei, TikTok, and DJI. This law effectively mandates that Chinese companies must cooperate with state intelligence activities, allowing the Communist Party to leverage civilian technologies for espionage purposes. Unfortunately, U.S. legislation does not provide any direct countermeasures to this law, leaving Chinese firms operating freely under the jurisdiction of Chinese intelligence directives. Zhao and Li (2021) emphasize that this legal obligation transforms these companies into de facto intelligence assets, which poses significant risks to global data security, especially for U.S. infrastructure (Van der Linden, & Łasak, 2023).

Furthermore, the Zhenhua Data leak exposes the vulnerability of U.S. officials to China's surveillance apparatus. This operation demonstrated how China could monitor key individuals, including U.S. policymakers and military personnel, through big data analytics and social media tracking. The Countering CCP Drones Act fails to regulate Chinese-owned AI platforms or data-harvesting technologies that enable such operations. As highlighted by The Guardian (2021), the leak underscores the growing threat of China's ability to exploit social media and other digital platforms for intelligence gathering. Without addressing these capabilities, the U.S. risks being unprepared to counter China's sophisticated methods of monitoring and influencing foreign governments and individuals. In this context, the limitations of the U.S. legal framework become evident, particularly in terms of digital espionage, where hardware-focused bans fall short of offering a comprehensive defense (Whalen, 2019).

The Countering CCP Drones Act is ultimately ineffective in addressing the full scope of Chinese intelligence threats for several key reasons. First, its limited scope means that it focuses almost exclusively on hardware, such as drones, while neglecting the broader, more complex networks of Chinese data collection systems and AI-powered surveillance platforms. These platforms, including cloud services and social media monitoring tools, are integral to China's intelligence-gathering operations, yet the Act fails to address these critical components. Second, the failure to address China's National Intelligence Law is a significant flaw in U.S. legislation.

The National Intelligence Law mandates that Chinese companies must assist in state-directed intelligence activities, as outlined in Article 7, yet U.S. law does not have provisions that directly counter this legal framework, leaving Chinese entities operating under the auspices of the CCP unchallenged in their intelligence roles. Third, the fragmented U.S. counterintelligence framework further weakens the nation's ability to effectively counter digital surveillance threats. Unlike China, which has a centralized intelligence coordination authority, the U.S. lacks a unified body to oversee and enforce intelligence-related policies, resulting in gaps in the protection of critical infrastructure. Lastly, the U.S. approach is reactive, unlike China's proactive intelligence-gathering operations, which are outlined in Articles 10 and 11 of the National Intelligence Law. While China continuously seeks to expand its intelligence reach, the U.S. only responds once a threat has been identified, putting it at a disadvantage when countering the evolving and increasingly sophisticated methods used by China for surveillance and espionage. These factors collectively highlight the limitations of the Countering CCP Drones Act in addressing the broader digital and intelligence security challenges posed by China (United Nations Conference on Trade and Development, 2023; US Department of State, 2020, Wang, 2023).

6.1 Conclusion

The Countering CCP Drones Act (H.R. 2864) represents a narrow and reactive approach to countering the broader intelligence threats posed by China's National Intelligence Law and China's expansive digital surveillance programs, such as the Zhenhua Data Leak. While the Act takes a step toward securing U.S. communications infrastructure by banning specific Chinese drone manufacturers, it fails to address the wider network of Chinese-owned data collection platforms, cloud services, and AI-driven surveillance technologies that are central to China's intelligence operations. This oversight leaves significant vulnerabilities in U.S. security, especially in terms of digital espionage and data gathering. China's National Intelligence Law (2017/2018) mandates that all Chinese firms assist in state espionage, which allows companies like DJI, TikTok, and others to act as tools for Chinese intelligence services, making the U.S. and other countries increasingly susceptible to surveillance and data theft. To truly protect U.S. national security and counter China's digital surveillance infrastructure, legislative reforms need to target these broader networks, not just hardware manufacturers. Key measures to strengthen the U.S. response include expanding the bans to include Chinese surveillance technology firms involved in AI, cloud services, and data analytics, building a multilateral intelligence technology alliance with democratic nations to counter China's growing digital espionage, and strengthening supply chain resilience to protect critical infrastructure from Chinese influence. By integrating legislative, trade, and cybersecurity measures, democratic nations can better mitigate the threats posed by China's National Intelligence Law, ensuring global trade fairness and maintaining security across national borders.

6.2 Recommendations

1. Expand the FCC's Covered List: Include Chinese cloud services (e.g., Alibaba Cloud), AI surveillance companies (e.g., Hikvision), and data brokers (e.g., Zhenhua Data) to prevent access to critical U.S. infrastructure and data systems.
2. Establish a National Intelligence Coordination Authority (NICA): Centralize U.S. cybersecurity and counterintelligence efforts to enhance coordination and response to emerging digital threats.
3. Implement a Preemptive Intelligence Risk Index (PIRI): Develop a system to blacklist Chinese firms with ties to the CCP's intelligence network, proactively identifying risks before they materialize.
4. Strengthen U.S. Data Privacy Laws: Implement stricter regulations to prevent Chinese platforms like TikTok and WeChat from harvesting biometric data and personal information of U.S. citizens.
5. Restrict Joint Ventures: Limit joint ventures between Chinese companies and U.S. tech firms or defense contractors to prevent Chinese influence in critical infrastructure sectors.

Further Enhancements to H.R. 2864:

6. Expand Scope to Other Technologies: Extend restrictions to include additional technology products that may pose security risks, such as telecommunications equipment and software linked to adversarial nations.
7. Implement Comprehensive Export Controls: Enforce strict export controls on critical technologies, including semiconductor manufacturing equipment and AI technologies, to prevent acquisition by entities that may use them against national interests.
8. Enhance International Collaboration: Partner with allies to create a unified strategy for addressing foreign intelligence laws, including China's NIL, to strengthen enforcement and reduce regulatory loopholes.
9. Promote Domestic Innovation: Increase investment in domestic research and development to reduce reliance on foreign technologies, fostering secure alternatives to Chinese technology.

10. Expand the Countering CCP Drones Act: Extend the Act to cover all Chinese-manufactured smart devices, such as surveillance cameras, cloud servers, and IoT appliances, which are critical in digital espionage.

11. Establish a Global Cybersecurity Alliance (GCA): Create a global alliance under the UN involving the U.S., India, Japan, and the EU to regulate Chinese digital infrastructure and enhance collective cybersecurity defenses.

12. Impose Sanctions on Chinese Data Brokers and AI Surveillance Firms: Sanction companies involved in mass data collection and cyber-espionage, targeting key players like Zhenhua Data and Hikvision.

13. Enhance Cybersecurity Protocols: Strengthen cybersecurity defenses in critical U.S. infrastructure, such as defense systems, nuclear plants, and transportation networks, to mitigate external surveillance risks.

14. Conduct Periodic Audits: Perform regular audits of Chinese-made devices in government facilities and financial institutions to detect embedded malware or spyware.

15. Collaborate with International Tech Giants: Partner with companies like Google, Microsoft, and Amazon to develop secure alternatives to Chinese cloud platforms and communication networks.

6.2.1 Strengthening U.S. Countermeasures:

1. Expand the Ban Scope: Extend the ban to all Chinese surveillance technology firms, not just drone manufacturers, and introduce penalties for U.S. entities that resell banned technologies.

2. Enhance Supply Chain Security: Incentivize domestic drone manufacturing and increase funding for research and development of AI-driven U.S. and allied drone technologies to reduce reliance on Chinese technology.

3. Establish a Multilateral Intelligence Tech Alliance: Build a coalition with the EU, UK, Japan, and India to counter China’s intelligence operations, implementing unified export controls to close regulatory gaps.

4. Introduce Transparency Requirements for Foreign Tech Imports: Mandate foreign tech firms to disclose any state intelligence obligations before operating in the U.S. and establish independent review boards to assess security risks from Chinese software and hardware.

6.2.2 Refining Global Intelligence Regulations:

1. Create a WTO-Compliant International Espionage Regulation Framework: Develop global legal measures to address state-backed corporate espionage, particularly in the tech industry.

2. Strengthen Data Privacy Agreements: Expand GDPR-style regulations to prevent the transfer of user data to foreign intelligence agencies, reinforcing global data protection standards.

3. Introduce AI-Specific Espionage Countermeasures: Implement guidelines for AI ethics, prohibiting the sale of AI-powered surveillance technologies to authoritarian regimes and establish an “AI Red List” of high-risk Chinese tech firms.

4. Encourage Corporate Compliance with Democratic Standards: Require companies to demonstrate independence from state intelligence operations before entering Western markets and impose sanctions on those that fail to disclose such ties.

References

Abb, P. (2018). What drives interstate balancing? Estimations of domestic and systemic factors. *International Politics, 55*(3), 279–296.

Adams, K. R. (2003). Attack and conquer? International anarchy and the offense-defense-deterrence balance. *International Security, 2003*, 45–83.

Alderman, D., & Ray, J. (2017). Best frenemies forever: Artificial intelligence, emerging technologies, and China–US strategic competition. *SITC Research Briefs, 2017*, 1.

Allen, G., & Chan, T. (2017). *Artificial intelligence and national security*. Cambridge, MA: Belfer Center for Science and International Affairs.

Allison, G. T. (2017). Destined for war? *The National Interest, 149*, 9–21.

Allison, G., & Schmidt, E. (2020). Is China beating the U.S. to AI supremacy? *Harvard Kennedy School, Belfer Center for Science and International Affairs, 2020*, 1.

Anderson, J., Sutherland, D., & Severe, S. (2015). An event study of home and host country patent generation in Chinese MNEs undertaking strategic asset acquisitions in developed markets. *International Business Review, 24*(5), 758–771.

Burke, E. J., Gunness, K. A., Cooper, C. A., & Cozad, M. R. (2020). *People’s Liberation Army operational concepts* (p. 32). Santa Monica, CA: RAND.

Buzan, B. (1991). New patterns of global security in the twenty-first century. *International Affairs, 67*(3), 431–451.

Cai, C., & Zhang, R. (2023). Malicious use of artificial intelligence, uncertainty, and US–China strategic mutual trust. In *The Palgrave Handbook of Malicious Use of AI and Psychological Security* (pp. 377–396). Cham: Springer.

Calcara, A. (2023). From quiet to noisy politics: Varieties of European reactions to 5G and Huawei. *Governance, 36*(2), 439–457.

Campion, A. S. (2020). From CNOOC to Huawei: Securitization, the China threat, and critical infrastructure. *Asian Journal of Political Science, 28*(1), 47–66.

Can, M., & Kaplan, H. (2020). Transatlantic partnership on artificial intelligence: Realities, perceptions, and future implications. *Global Affairs, 6*(4–5), 537–557.

Can, M., & Vieira, A. (2022). The Chinese military-civil fusion strategy: A state action theory perspective. *The International Spectator, 57*(3), 85–102.

Capri, A. (2020). Techno-nationalism: The US-China tech innovation race. *New challenges for markets, business and academia*. Hinrich Foundation 2020, 1.

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. (2023, June 20). 'Joint communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy." *EUR-Lex*. https://eurlex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023JC0020

European Parliament. (2020). *COVID-19 foreign influence campaigns Europe and the global battle of narratives*. Brussels. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649367/EPRS_BRI(2020)649367_EN.pdf

Fannin, R. (2020, January 31). How the US-China trade war has starved some Silicon Valley start-ups. *CNBC*. https://www.cnbc.com/2020/01/31/chinese-venture-capitalists-draw-back-silicon-valley-investments.html

Feldstein, S. (2019). *The global expansion of AI surveillance* (Vol. 17). Washington, DC: Carnegie Endowment for International Peace.

Financial Times. (2023, October 18). Five Eyes spy chiefs warn Silicon Valley over Chinese threat. *Financial Times*. https://www.ft.com/content/0a37da0a-ad06-43d0-b069-bfafa0ff35a4

Fischer, S. C. (2023). Silicon Curtain: America's quest for allied export controls against China. In *Strategic Trends 2023: Key developments in global affairs* (pp. 39–61). Center for Security Studies (CSS), ETH Zürich.

Fischer, S. C., & Wenger, A. (2021). Artificial intelligence, forward-looking governance, and the future of security. *Swiss Political Science Review, 27*(1), 170–179.

Goldman, D. P. (2020). *You will be assimilated: China's plan to sino-form the world*. London: Bombardier Books.

Goldman, E. O., & Andres, R. B. (1999). Systemic effects of military innovation and diffusion. *Security Studies, 8*(4), 79–125.

Goldstein, A. (2020). China's grand strategy under Xi Jinping: Reassurance, reform, and resistance. *International Security, 45*(1), 164–201.

Gorman, L. (2021, August 14). China's data ambitions: Strategy, emerging technologies, and implications for democracies. *The National Bureau of Asian Research*. https://www.nbr.org/publication/chinasdata-ambitions-strategy-emerging-technologies-and-implications-for-democracies/

Gray, J. E. (2021). The geopolitics of "platforms": The TikTok challenge. *Internet Policy Review, 10*(2), 1–26.

Greene, R., & Triolo, P. (2020). Will China control the global internet via its digital silk road? *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road-pub-81857

Greitens, S. C. (2020). Dealing with demand for China's global surveillance exports. *Brookings Institution Global China Report*.

Grochmalski, P., Lewandowski, P., & Paszak, P. (2020). US-China technological rivalry and its implications for the Three Seas Initiative (3SI). *European Research Studies Journal, 23*(Special 2), 840–853.

Grotto, A., & Schallbruch, M. (2019, September 16). The great anti-China tech alliance. *Foreign Policy*. https://foreignpolicy.com/2019/09/16/the-west-will-regret-letting-china-win-the-tech-race/

Haas, M. C., & Fischer, S. C. (2020). The evolution of targeted killing practices: Autonomous weapons, future conflict, and the international order. In *The Transformation of Targeted Killing and International Order* (pp. 107–132). Routledge.

Han, Z., & Paul, T. V. (2020). China's rise and balance of power politics. *The Chinese Journal of International Politics, 13*(1), 1–26.

Harold, S., Beauchamp-Mustafaga, N., & Hornung, J. (2021). Chinese disinformation efforts on social media. *RAND Corporation*. https://www.rand.org/content/dam/rand/pubs/research_reports/RR4300/RR4373z3/RAND_RR4373z3.pdf

Hart, B., Lin, B., Lua, S., Price, H., Liao, G., & Slade, M. (2023, August 16). Is China a leader in Quantum Technologies? *China Power Project*. https://chinapower.csis.org/china-quantum-technology/

Harwit, E. (2023). U.S.-China 5G competition, the economy-security nexus, and Asia. *Journal of Chinese Political Science, 2023*, 1–16.

He, K. (2012). Undermining adversaries: Unipolarity, threat perception, and negative balancing strategies after the cold war. *Security Studies, 21*(2), 154–191.

He, K., & Feng, H. (2012). Why is there no NATO in Asia? Revisiting: Prospect theory, balance of threat, and US alliance strategies. *European Journal of International Relations, 18*(2), 227–250.

Heath, T. R., Grossman, D., & Clark, A. (2021). China's quest for global primacy: An analysis of Chinese international and defense strategies to outcompete the United States. Santa Monica: RAND Corporation.

Siddiqui, H. R., & Muniza, M. (2025). Hybrid Warfare and the Global Threat of Data Surveillance: The Case for International Standards and Regulation. *Pakistan Social Sciences Review*, *9*(1), 519–531. https://doi.org/10.35484/pssr.2025(9-I)41

Siddiqui, H. R., & Muniza, M. (2025). Regulatory Gaps in Drone Surveillance: Addressing Privacy, Security, and Manufacturing Standards. *Annals of Human and Social Sciences*, *6*(1), 415–428. https://doi.org/10.35484/ahss.2025(6-I)36

Ting-Fang, C., & Li, L. (2023, June 30). Netherlands unveils chip tool export curbs in fresh blow to China. *Nikkei Asia*. https://asia.nikkei.com/Business/Technology/Netherlands-unveils-chip-tool-export-curbs-in-fresh-blow-to-China

Torreblanca, J.-I., & Jorge-Ricart, R. (2022). The US-EU Trade and Technology Council (TTC): State of play, issues, and challenges for the transatlantic relationship. *Journal of European Integration, 44*(3), 295–312.

Triolo, P. (2023). Technology crossroads: Innovation in China's telecommunications and high-performance computer sectors threatened by US stranglehold on semiconductors. *Asian Security, 2023*, 1–16.

United Nations Conference on Trade and Development. (2023). *Technology and innovation report 2023*. UNCTAD. https://unctad.org/tir2023

US Department of State. (2020, March 16). The PRC's "Military-Civil Fusion" strategy is a global security threat. https://2017-2021.state.gov/the-prcs-military-civil-fusion-strategy-is-a-global-security-threat/

USA Embassy in Georgia. (2020, May 8). Briefing with special envoy Lea Gabrielle. https://ge.usembassy.gov/briefing-with-special-envoy-lea-gabrielle-global-engagement-center-update-on-prc-efforts-to-push-disinformation-and-propaganda-around-covid-may-8/

USCC (2018). *US-China Economic & Security Review Commission. Report to Congress of the US-China Economic and Security Review Commission*. https://www.uscc.gov/annual-report/2018-annualreport-congress

Van der Linden, R. W., & Łasak, P. (2023). The ongoing Sino-US trade war and subsequent tech war. In *Financial Interdependence, Digitalization, and Technological Rivalries* (pp. 157–182). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-27845-7_8

Wang, D. (2023, February 28). China's hidden tech revolution. *Foreign Affairs*. https://www.foreignaffairs.com/articles/china/2023-02-28/chinas-hidden-tech-revolution

Wang, Y., & Chen, D. (2018). Rising Sino-US competition in artificial intelligence. *China Quarterly of International Strategic Studies, 4*(2), 241–258.