Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 15 (2), 2023
pp. 347 - 363

Countering China's Digital Espionage and Surveillance: U.S. Sanctions & Strategic Countermeasures, China's Low-Cost Strategy: A Trojan Horse?

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

1. Hassan Rasheed Siddiqui: Author, Aviation Law Expert, L.L.M University OF Bedfordshire (U.K).
2. Maria Muniza; (Former Director Program, Educational FM Radio, Resident Editor South Asia, KT, Media Group.

Correspondence Author: Mariamuniza@gmail.com

ABSTRACT

This research explores the growing threat posed by China's digital surveillance and espionage activities, particularly through its technological advancements in 5G, AI, IoT devices, and telecom infrastructure. It examines China's legal frameworks, such as the National Intelligence Law and the Data Security Law, which mandate Chinese companies to assist in intelligence-gathering efforts, raising concerns over the potential for state-backed espionage. The study analyzes key incidents, including the Zhenhua Data case and Galwan Valley cyberattacks, highlighting the real-world implications of China's surveillance operations. It also evaluates the global response to these threats, emphasizing the inadequacy of current countermeasures and the need for enhanced international collaboration. The paper proposes a comprehensive policy approach, including stricter legislative frameworks, the promotion of domestic innovation, enhanced cybersecurity measures, and international cooperation to counter China's expanding influence in digital espionage. The findings underscore the importance of unified action to protect global digital infrastructure and secure national sovereignty from Chinese technological dominance.

KEYWORDS: *Digital Surveillance, Cyber-security, National Intelligence Law, International Cooperation, Technological Sovereignty.*

Received: 20 July 2023 **Revised**: 22 August 2023 **Accepted**:18 September2 023

1. INTRODUCTION

The rapid expansion of Chinese technology in global markets has raised significant concerns regarding privacy, cybersecurity, and national security. Many Western nations, including the U.S. and European Union (EU) members, have imposed sanctions on Chinese tech companies like Huawei and ZTE, citing espionage and security risks. However, these efforts have been undermined by China's ability to circumvent restrictions through third-party nations and by offering low-cost alternatives to emerging economies. China's digital surveillance state, reinforced by its National Intelligence Law (2017/18), mandates that all Chinese companies cooperate with government intelligence operations, making their global presence a direct threat to national security.

China's penetration into critical infrastructure, communication networks, and emerging technologies presents a high-risk scenario for global security. The The Zhenhua Data (India China Boarder Tension 2020) case in India demonstrated the real-world implications of China's espionage strategy, proving that Chinese companies operate as state-backed intelligence gatherers. Leveraging sophisticated cyber tools, artificial intelligence, and low-cost technology exports, China has embedded itself into foreign institutions, eroding national sovereignty and compromising sensitive data. Despite sanctions and trade restrictions, China continues to adapt by strengthening domestic innovation, expanding strategic

partnerships, and exporting its technology under different branding, making it difficult to regulate effectively.

Recognizing the urgency of countering these threats, several measures have been proposed to mitigate risks. Recommendations include prohibiting high-risk foreign drone manufacturers from supplying technology to government agencies and critical sectors, establishing rigorous cybersecurity certification requirements for commercial drone use, and mandating stringent supply chain vetting to eliminate vulnerabilities. Additionally, import bans on Chinese appliances, particularly smart devices, have been introduced in an effort to prevent backdoor access to critical infrastructure and personal data. However, these measures remain inadequate. The lack of an internationally unified approach allows China to bypass restrictions through proxy companies and third-party agreements, continuing its infiltration of global digital infrastructure.

China's surveillance apparatus represents one of the greatest global cybersecurity threats. Through state-backed legal mandates, cyber intrusions, and strategic acquisitions, China has positioned itself as a digital Trojan Horse, exploiting regulatory gaps to expand its reach. While some nations have imposed targeted sanctions, the global regulatory framework remains insufficient to counter the broader intelligence threat. Without immediate international action, China will continue expanding its control over global data, endangering individual privacy, national security, and democratic institutions worldwide. First-world nations must adopt a cohesive, proactive stance, including legislative cooperation, intelligence-sharing, and technological innovation, to dismantle China's pervasive surveillance network before it further compromises global security.

1.2 BACKGROUND

China has developed an extensive digital surveillance network, leveraging consumer technology, artificial intelligence (AI), and global investments to advance its intelligence-gathering operations. The National Intelligence Law (NIL) (2017/18) legally mandates all Chinese companies to cooperate with state intelligence agencies. This has raised concerns about the security risks posed by Chinese technology companies such as Huawei, Hikvision, and DJI, particularly in nations where their products and services have gained widespread adoption.

While the United States and Japan have imposed stringent trade and investment restrictions against Chinese tech firms, China has continued its surveillance expansion. The National Intelligence Law of China (2017/18) and Data Security Law (2021) provide a legal shield for Chinese companies to operate under state directives, making them legal extensions of the Communist Party's intelligence apparatus.

This research explores the legislative responses of the U.S., Japan, Germany, and other first-world nations to counter China's digital espionage and technological expansion, along with an analysis of India's The Zhenhua Data (India China Boarder Tension 2020) Data case, which revealed China's mass-scale data collection operations.

1.3 RATIONAL OF STUDY

The rationale for this study stems from the increasing global reliance on digital technologies, which has simultaneously amplified vulnerabilities to espionage and cyberattacks. China's aggressive digital surveillance and intelligence-gathering strategies have raised alarm bells among nations worldwide, especially those in the tech sector, prompting the need for robust countermeasures. This research is essential to understand the effectiveness of current legislative frameworks and strategic responses in mitigating these threats. By examining real-world cases such as the Zhenhua Data incident during the India-China border tensions, the study will offer critical insights into the practical implications of China's digital operations and the ongoing challenges faced by high-tech nations. Ultimately, the study aims to inform policy decisions and enhance cybersecurity strategies globally.

1.4 STATEMENT OF PROBLEM

The statement of the problem for this research centers around the growing threat posed by China's digital espionage and surveillance activities, which have raised serious concerns regarding global cybersecurity, national security, and privacy. As China continues to advance its technological capabilities, it is increasingly leveraging these tools for intelligence-gathering purposes, using low-cost strategies that often bypass traditional defense mechanisms. This has led to a strategic dilemma for many countries, particularly high-tech nations like the U.S., Japan, and Germany, that must balance technological innovation

with safeguarding their citizens' data and national security. The research aims to explore the legislative frameworks and countermeasures employed by these nations to combat China's digital espionage efforts, focusing on the practical effectiveness of such strategies. Furthermore, the study will delve into the real-world implications of these espionage activities through the analysis of the Zhenhua Data case, especially within the context of the 2020 India-China border tensions. By analyzing these aspects, the research seeks to understand the broader implications of China's digital strategies and provide insights into how countries can strengthen their defenses against these growing threats.

1.5 RESEARCH OBJECTIVES

1. To analyze China's legal framework supporting surveillance and intelligence gathering.
2. To examine U.S., Japan, Germany, and other high-tech nations' countermeasures against Chinese digital espionage
3. To assess the effectiveness of sanctions and legislative actions in reducing China's access to critical technology
4. To analyze the The Zhenhua Data (India China Boarder Tension 2020) case in India as an example of China's growing intelligence threats.

2. RESEARCH METHODOLOGY

This study employs a qualitative research approach to comprehensively examine China's digital espionage and surveillance strategies, as well as the countermeasures adopted by various nations. The first component of the methodology is Legislative Review, which involves a detailed examination of national security laws and regulations enacted by countries to counter technological espionage, focusing on their effectiveness in safeguarding data and national interests. The second approach is Case Studies, where the research will analyze real-world instances of China's intelligence-gathering operations, specifically highlighting the Zhenhua Data case, which occurred during the 2020 India-China border tensions, to understand the practical impact of these operations on national security. Comparative Analysis is the third element, where the strategies of the U.S., Japan, Germany, and other high-tech nations will be reviewed in the context of their responses to Chinese surveillance technology, highlighting the strengths and weaknesses of their countermeasures. Finally, the study will include an Economic Impact Assessment, evaluating the effects of global sanctions imposed on China, particularly those targeting its tech industry, and their influence on China's economic and technological development. By combining these methods, the study aims to provide a comprehensive understanding of both the threats posed by China's digital surveillance efforts and the strategies employed by other nations to combat them.

3. LITERATURE REVIEW

3.1 A. China's Surveillance Strategy and Legitimization of Espionage

China's surveillance strategy has garnered significant attention in recent years, especially with the enactment of the National Intelligence Law (NIL) in 2017 and the Data Security Law in 2021. These laws explicitly require both private and state-owned companies to cooperate with the Chinese government in gathering and transferring data, which has led to concerns about the potential for espionage. The NIL, in particular, mandates that companies hand over data to state intelligence agencies when requested, irrespective of whether the data is located within or outside of China (Feng & Li, 2020). Similarly, the Data

Security Law strengthens the government's ability to monitor data flows, even across international borders, under the guise of protecting national security (Liu & Zhong, 2021).

These legal frameworks have facilitated China's widespread deployment of surveillance infrastructure in foreign nations, often under the pretext of commercial expansion, while enabling the collection of massive amounts of data through AI-powered systems. This data is used to monitor not only Chinese citizens but also individuals, companies, and governments worldwide, fueling concerns about the scale and scope of China's surveillance capabilities (Shen, 2022). Additionally, Chinese tech giants like Huawei, ByteDance (the parent company of TikTok), Hikvision, and Alibaba have been increasingly scrutinized for their involvement in state-sponsored surveillance activities, with allegations that they support espionage efforts by providing technologies and platforms that enable pervasive data collection (Gao & Zhang, 2023). These companies are often accused of facilitating the Chinese government's global surveillance operations by embedding surveillance technologies in everyday products and services, raising alarms in both Western and non-Western nations about privacy violations and national security risks (Kuo, 2021).

3.2 B. The The Zhenhua Data (India China Boarder Tension 2020) Case in India – A Case Study

The Zhenhua Data case, linked to the India-China border tensions of 2020, exposed China's covert intelligence-gathering operations and highlighted the significant risks posed by its surveillance strategy. Zhenhua Data, a Shenzhen-based technology firm, was found to be illegally collecting personal information on over 10,000 Indian citizens, including government officials, military personnel, and business leaders (Sharma, 2021). The data was compiled through a combination of AI-powered tracking, social media surveillance, and big data analytics, which enabled the company to create highly detailed profiles of individuals. This information was likely used to track, monitor, and potentially influence key figures within India's political and military landscape (Bhat, 2022).

Upon discovery of these operations, the Indian government responded by blacklisting Zhenhua Data and implementing strict measures to restrict data-sharing with Chinese tech companies. Additionally, the case prompted India to strengthen its cybersecurity laws, introducing new regulations to protect national security and combat foreign espionage (Rai, 2021). Furthermore, India banned several Chinese apps, including TikTok, which were believed to be involved in data collection and surveillance activities. The implications of the Zhenhua Data case were far-reaching, as it demonstrated the growing role of cyber-espionage in modern geopolitical conflicts and highlighted the need for countries to develop more robust defenses against such tactics. This incident was a clear indication of China's extensive use of digital platforms for intelligence purposes, making it a significant case in the study of global cybersecurity and international relations.

3.3 C. Legislative Responses to Chinese Digital Espionage

1. United States – National Security Measures

The U.S. has enacted several legislative actions aimed at countering China's technological espionage and enhancing national security. One key measure is the American Security Drone Act (ASDA) of 2023, which prohibits federal agencies from acquiring drones and unmanned aerial vehicles (UAVs) from Chinese manufacturers, such as DJI. This law bans the Department of Defense (DoD), Department of Homeland Security (DHS), and other federal agencies from purchasing Chinese-made drones, restricts funding for state and local agencies that buy Chinese drones, and mandates the phased replacement of any existing Chinese drones in government use. The rationale behind this legislation stems from concerns that Chinese drones may contain backdoor surveillance technology, potentially compromising national security. The ASDA aligns with broader U.S. strategies to secure critical supply chains and ensure that technologies used by the government are sourced from trusted allies. Additional measures, such as the CHIPS and Science Act (2022), prevent U.S. semiconductor firms from supplying China with advanced AI chips, while Executive Orders (2023) restrict U.S. investment in Chinese AI, quantum computing, and military technology sectors. Furthermore, the Entity List maintained by the Department of Commerce restricts exports to Chinese firms

like Huawei, SMIC, and Hikvision, which have been linked to state surveillance activities. A federal procurement ban also prevents U.S. government agencies from using Chinese surveillance equipment.

2. **Japan – Countering Chinese Espionage Through Economic Security Laws**

Japan has responded to the growing threat of Chinese digital espionage through a combination of economic and national security laws. The Economic Security Promotion Act (2022) aims to protect Japan's high-tech industries by limiting foreign investment, particularly from Chinese entities, in critical sectors such as semiconductors, AI, and quantum computing. This law requires government approval for Japanese companies that engage in business dealings with Chinese tech firms, ensuring that sensitive technologies do not fall into the wrong hands. Furthermore, the Cybersecurity Strategy (2023) expands Japan's cybersecurity collaboration with the U.S. and the European Union, while establishing AI-based surveillance monitoring systems to detect and mitigate foreign cyber threats, including those originating from China.

3. **Germany – Strengthening Digital Sovereignty**

Germany has recognized China as a significant cybersecurity threat and has taken measures to strengthen its digital sovereignty. The IT Security Law 2.0 (2021) restricts Chinese companies from participating in Germany's 5G infrastructure and grants the government authority to ban Chinese tech firms if they pose security risks. In addition, the Foreign Investment Control Act limits Chinese acquisitions of high-tech German companies and strengthens the government's review process for foreign direct investment (FDI) in the tech sector. These measures reflect Germany's commitment to safeguarding its technological infrastructure from potential espionage and ensuring that foreign investments do not compromise national security.

4. **USSR (Now Russia) – Hybrid Strategy**

Russia has adopted a hybrid approach to digital security by maintaining strategic cooperation with China while simultaneously protecting its own digital infrastructure. The Sovereign Internet Law (2019) is a key part of this strategy, as it enables Russia to create a domestically controlled internet network, reducing the country's reliance on foreign technologies, including those from China. The law also allows the Russian government to disconnect the country from global networks in the event of cyber threats, providing a level of self-sufficiency in terms of digital security. While Russia and China maintain close ties, Russia's digital sovereignty measures reflect its need to balance cooperation with China and protect its national interests from external threats, including cyber-espionage.

These legislative actions represent a multifaceted approach to countering Chinese digital espionage, with each country tailoring its response to its own geopolitical context and technological priorities. By implementing these laws, the U.S., Japan, Germany, and Russia aim to safeguard their critical infrastructure, reduce vulnerabilities to cyber threats, and ensure that their national security is not compromised by foreign surveillance operations.

4. DISCUSSION

China's National Intelligence Law (NIL), enacted in 2017, has been a focal point in discussions about global security and technological sovereignty. The law, particularly Articles 7, 12, 13, and 14, legally obligates Chinese corporations, citizens, and organizations to support intelligence work, fueling suspicions that Chinese companies cannot operate independently from state influence. As a result, major Chinese technology firms—including Huawei, DJI, and ByteDance (TikTok)—have faced increasing restrictions worldwide.

4.1 Key Articles of the Chinese National Intelligence Law and Their Implications

China has created a comprehensive legal framework that enables the government to exert extensive control over data and intelligence collection both domestically and abroad. The National Intelligence Law (NIL), which was enacted in 2017, provides the legal foundation for a state-sanctioned surveillance model, mandating that all Chinese companies, individuals, and organizations must assist in

intelligence-gathering efforts when requested by the government. The law effectively turns private companies into state intelligence agents, as they are obligated to cooperate with national intelligence agencies, even when operating overseas. This has serious implications for global security, as it raises concerns that Chinese technology companies could be used as tools of espionage, potentially compromising the data of foreign governments, businesses, and individuals.

The Data Security Law (DSL) and Personal Information Protection Law (PIPL), both enacted in 2021, further expand the scope of China's surveillance capabilities. The Data Security Law (DSL) requires all companies operating within China, including foreign firms, to classify and store data based on its importance to national security. The law grants the Chinese government the right to access and control sensitive information, allowing it to monitor corporate and personal data both within China and beyond its borders. Meanwhile, the Personal Information Protection Law (PIPL) gives the Chinese government the power to access data collected from Chinese citizens, even if that data is stored or processed outside of China. This broad jurisdictional reach raises serious concerns about privacy and data sovereignty, as it effectively places all data collected within China under the control of the Chinese government.

Together, these laws establish a legal framework that transforms Chinese technology firms into potential surveillance tools, capable of facilitating the Chinese government's global intelligence operations. The implications of this surveillance model are profound, as it creates a system where companies are compelled to share sensitive data with the government, thus increasing the risks of espionage and cyberattacks. Countries and companies around the world have expressed growing concerns about the potential security risks posed by these laws, particularly as they relate to the use of Chinese-made technologies in critical infrastructure, telecommunications, and digital networks. The global response to China's legal framework has been one of increased caution, with several nations introducing measures to restrict or ban Chinese technology in an effort to safeguard their national security and privacy.

4.2 The Cybersecurity Law and National Intelligence Law

The Cybersecurity Law (2017) and National Intelligence Law (2017) form the backbone of China's legal framework for cyber-espionage and surveillance. These laws require Chinese companies, both domestic and international, to assist in intelligence-gathering activities, making them extensions of state surveillance. The laws mandate that all Chinese organizations and citizens comply with intelligence requests from the Chinese Communist Party (CCP), creating a system where private corporations are compelled to share sensitive data with the government, whether they operate inside or outside of China. This has raised significant concerns about the security risks associated with Chinese-made technologies worldwide, especially in areas such as telecommunications infrastructure, surveillance systems, and consumer electronics.

Article 7 of the National Intelligence Law is particularly critical, as it stipulates that “all organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law.” This provision effectively obligates every Chinese company and individual to assist in intelligence operations, making Chinese firms potential tools for state surveillance. The implications of this provision are far-reaching, as it directly links the operation of Chinese companies like Huawei, Hikvision, and DJI with the Chinese state’s intelligence activities. These companies have been implicated in global security concerns, with their products potentially being used for espionage, particularly in sectors involving critical infrastructure and surveillance.

Article 12 further strengthens the surveillance model by formalizing state-backed intelligence cooperation with private businesses and individuals. It states that national intelligence agencies may establish cooperative relationships with relevant parties to carry out intelligence work. This provision undermines any claims of corporate autonomy by Chinese companies, such as Huawei and DJI, and reinforces the idea that these firms are bound to state control, no matter how independently they may operate in other countries. This deepens the global fear that Chinese companies cannot be trusted with critical technologies, as they are inherently aligned with government objectives.

Article 13 adds another layer of concern by allowing Chinese intelligence agencies to "carry out foreign exchanges and cooperation," raising questions about how China shares and collects intelligence internationally. This lack of transparency in foreign intelligence cooperation intensifies global unease, particularly regarding Chinese companies that have established a presence in critical sectors like 5G infrastructure, surveillance technologies, and global supply chains.

Article 14 strengthens the CCP's ability to compel Chinese businesses and individuals to assist intelligence agencies, making it clear that no organization, including private enterprises, can refuse cooperation with the state. This provision highlights the potential for Chinese companies to be utilized for espionage operations, whether or not they directly participate in government activities. It exemplifies how Chinese tech firms are often entangled with state intelligence efforts, posing significant risks for nations using Chinese technology in their critical infrastructure.

These articles in the National Intelligence Law and Cybersecurity Law illustrate how China has embedded state surveillance and intelligence-gathering into its legal and corporate structures, raising serious security concerns globally. The international community, particularly countries reliant on Chinese technology, has responded with increased scrutiny and regulatory measures to mitigate the risks posed by these laws and to prevent the infiltration of Chinese surveillance tools into sensitive sectors.

4.3 China's Global Cyber Espionage and Surveillance Expansion

China has progressively expanded its cyber espionage and surveillance capabilities beyond its borders, leveraging a combination of legal frameworks, corporate influence, and direct cyber operations. This expansion is not only a tool for monitoring its own citizens but also a method for extending its geopolitical power globally, often in the form of digital warfare and espionage. One of the most prominent instances of this expansion occurred during the Galwan Valley Conflict (2020-2022) between India and China, where tensions escalated over territorial disputes. During this period, reports surfaced suggesting that China conducted cyber intrusions targeting India's critical infrastructure. The Recorded Future cybersecurity group found evidence of Chinese malware within India's power grid, which potentially had the capability to disrupt power supply systems. This case demonstrated how cyber warfare is used as a tool of geopolitical leverage, with China allegedly attempting to cripple vital infrastructure in a strategic neighbor. The use of malware, targeting not just physical infrastructure but also government databases, showcased China's growing role in leveraging cyberattacks as part of its broader foreign policy and military strategy.

Amid rising tensions, India's Ahmedabad Municipal Corporation (AMC) made a significant policy shift by banning the installation of foreign-made surveillance equipment, particularly from Chinese manufacturers. This decision came after cybersecurity analysts and intelligence agencies raised alarms about the vulnerabilities in Chinese-made surveillance systems. Reports indicated that these devices were potentially being accessed remotely by external entities, highlighting the risks associated with Chinese-manufactured surveillance technologies. Notably, during the Galwan Valley standoff, there were reports of China executing a cyber demonstration in which they briefly took control of surveillance networks in several strategic Indian cities, including Ahmedabad. The incident heightened concerns that Chinese-made devices, such as cameras, biometric scanners, and data storage systems, could be exploited for espionage and provide the Chinese government with remote access to sensitive data.

This incident reinforced the argument that Chinese surveillance equipment could be a Trojan Horse for cyber-espionage, allowing China to not only monitor individuals and cities but also potentially gather critical intelligence from foreign nations. The growing reliance on Chinese-made technologies, including surveillance systems and IoT devices, poses a significant national security risk, as evidenced by India's response to the vulnerabilities in its security infrastructure. This situation highlights the broader implications of China's global cyber-espionage strategy, where seemingly innocuous technologies could be weaponized for political and strategic advantage.

4.4 China’s 5G Expansion: A Trojan Horse for Global Surveillance

China's extensive investment in 5G networks, smart cities, and consumer electronics has enabled it to embed surveillance capabilities into a wide range of everyday devices. One of the key players in this global expansion is Huawei, which has become the largest supplier of 5G infrastructure globally. However, this expansion has raised significant security concerns, as nations that adopt Huawei's 5G networks may inadvertently expose their communications to Chinese state surveillance. The 2022 NATO report warned that China's dominance in 5G infrastructure gives it substantial control over global data transmission, allowing it to monitor and potentially manipulate communications worldwide. This highlights the broader risks associated with adopting Chinese-made 5G technology, as it could be used not only for telecommunications but also for state-sponsored intelligence-gathering.

4.5 IoT Devices as a Surveillance Tool

In addition to its 5G infrastructure, China has flooded global markets with affordable smart devices, security cameras, and internet-of-things (IoT) technology. These devices, while convenient for consumers, are capable of collecting vast amounts of personal data, often without the users’ knowledge or consent. According to the Center for Strategic and International Studies (CSIS) in 2023, Chinese-made IoT devices have been found to transmit data back to China, raising concerns about unauthorized surveillance and data harvesting. These IoT devices are increasingly integrated into smart homes, offices, and public spaces, creating an extensive network of surveillance tools that could potentially be exploited for espionage purposes. This global spread of Chinese-made surveillance technology raises critical questions about privacy, data sovereignty, and the risks of foreign state influence over essential technologies.

4.6 China’s Evasion of U.S. Sanctions and Continued Expansion

Despite facing sanctions from the U.S. and other Western nations, China has demonstrated a remarkable ability to bypass these restrictions, ensuring the continued expansion of its technology exports. A 2023 U.S. Department of Commerce report revealed how China exports its technology through third-party countries, particularly in Africa and the Middle East, effectively circumventing direct sanctions. For example, Chinese telecom giants Huawei and ZTE continue to sell telecom equipment through subsidiaries based in countries that have not imposed bans, allowing them to maintain a global presence. Additionally, Chinese AI surveillance tools are marketed under different branding in Latin America, Africa, and Southeast Asia, further extending China's influence in the global surveillance landscape. This strategy enables China to sidestep international sanctions and maintain its position as a key player in the global technology market, while continuing to pose significant risks to international cybersecurity and data privacy. In summary, China’s strategic use of 5G technology, IoT devices, and AI surveillance tools has created a vast network of potential surveillance systems that can be used to monitor global communications and personal data. Despite the efforts of Western nations to restrict these technologies, China has found ways to circumvent sanctions, solidifying its role in shaping global infrastructure and raising concerns about the long-term implications for data privacy and national security.

4.7 China’s Role in the Global Semiconductor Supply Chain

China has strategically manipulated the global semiconductor supply chain to counter the effects of U.S. sanctions, ensuring a steady flow of critical microchips necessary for its surveillance technology. According to a 2024 RAND Corporation report, China has employed a variety of tactics to circumvent U.S. restrictions on the export of advanced semiconductors, ensuring that it maintains access to the essential components required for its growing technological and espionage operations. This includes leveraging third-party countries to acquire the microchips needed for surveillance technologies, which are used in a variety of systems, from 5G infrastructure to IoT devices and AI surveillance tools. By controlling a significant portion of the semiconductor supply chain, China has effectively neutralized many of the sanctions designed to limit its technological advancement and surveillance capabilities.

4.8 The Global Response: Inadequate Measures Against China's Surveillance Tactics

While certain countries have taken steps to address the threat posed by Chinese surveillance tactics, the global response remains fragmented and insufficient. A notable example of this is the European Union's AI Act (2023), which was introduced by the European Commission to regulate foreign AI technologies that could pose security risks. However, the enforcement mechanisms for this regulation remain weak, and Chinese AI firms continue to operate in Europe under different subsidiaries, circumventing the intent of the law. This reflects a broader issue where laws are enacted without strong enforcement, allowing Chinese companies to continue penetrating sensitive markets.

Similarly, India's Data Protection Bill (2023) was introduced as a countermeasure to protect its citizens' data from foreign surveillance, especially from Chinese entities. The bill seeks to prohibit foreign access to sensitive personal data, but its implementation has been challenged by China's deep economic ties with Indian tech companies, making it difficult to fully restrict Chinese surveillance technologies from entering the Indian market.

In response to China's growing technological influence, the U.S. National Cybersecurity Strategy (2023) emphasizes countering China's digital authoritarianism. The strategy has involved concrete actions, such as banning Huawei and ZTE from participating in U.S. telecom networks, restricting the export of AI chips to China, and imposing sanctions on Chinese surveillance companies like Hikvision and Dahua. These efforts aim to limit China's access to critical technologies and curb its ability to expand its global surveillance infrastructure. However, these measures are not foolproof, and China continues to find ways to bypass restrictions, particularly by using third-party countries.

4.9 The Need for a Global Regulatory Framework and Awareness Campaign

Given the inadequate responses thus far, there is an urgent need for a comprehensive, unified global response to counter China's "Trojan Horse" strategy of embedding surveillance capabilities into critical infrastructure worldwide. One potential solution is the development of a Global AI and Data Protection Regulation, led by international bodies like the United Nations. The creation of an AI surveillance regulation treaty could help prevent Chinese companies from embedding spyware into global networks, ensuring that surveillance technologies are not used as tools for espionage. Additionally, countries should enforce stricter compliance mechanisms to prohibit surveillance-laden technologies from being incorporated into critical infrastructure.

Moreover, public awareness campaigns should be launched to educate governments, businesses, and consumers about the risks associated with Chinese-made surveillance technologies. By fostering greater awareness and establishing stronger international regulations, the global community can better protect itself from the risks posed by China's expanding digital surveillance and espionage operations. In conclusion, while individual countries have taken steps to limit China's technological influence, the response has been piecemeal and insufficient. A coordinated global effort to regulate AI technologies, enforce stricter compliance in sensitive sectors, and establish stronger data protection laws is necessary to mitigate the growing threat posed by Chinese surveillance and espionage activities.

4.10 Public Awareness Campaigns

Governments and civil society must play an active role in educating individuals about the risks associated with Chinese-made IoT and communication devices. These devices, including smart home products, security cameras, and telecommunications equipment, may carry hidden surveillance capabilities, posing significant threats to personal privacy and national security. Public awareness campaigns should focus on educating the public about the potential dangers of using these devices, which could unknowingly transmit data back to Chinese entities. Additionally, individuals should be educated on the importance of cybersecurity hygiene, such as using strong, unique passwords, enabling multi-factor authentication, and avoiding risky online behaviors. These steps can significantly reduce the risk of data theft and prevent malicious actors from accessing personal and sensitive information. By raising awareness and encouraging

proactive cybersecurity measures, individuals can better protect themselves from the growing threat of digital espionage.

4.11 Economic and Diplomatic Countermeasures

To address the rising threat of Chinese digital espionage, nations must implement economic and diplomatic countermeasures. Trade restrictions can be imposed on countries or entities that actively facilitate Chinese cyber-espionage, effectively cutting off their access to critical technologies. Such measures can include restricting the sale of sensitive technologies and limiting foreign investments in firms that have ties to Chinese surveillance programs. Additionally, governments should invest in secure, non-Chinese alternatives for global telecom infrastructure, such as 5G networks, by supporting local technology firms or trusted international players. This would reduce dependence on Chinese companies like Huawei and ZTE, which have been linked to espionage concerns. By strengthening the global supply chain with secure alternatives, countries can safeguard their digital infrastructure and reduce vulnerabilities to foreign surveillance.

4.12 A. China's Counter-Response to Foreign Restrictions

Despite increasing international sanctions and restrictions, China has shown resilience and adaptability in continuing to expand its digital surveillance and technological influence. In response to the U.S. chip restrictions, China has heavily invested in developing its domestic semiconductor manufacturing capabilities. This move is aimed at reducing reliance on foreign chip suppliers, particularly from the U.S., and ensuring that China can maintain access to the critical components necessary for its surveillance technology, AI systems, and telecommunications infrastructure. Furthermore, China has sought to expand partnerships with countries like Russia, Iran, and other strategic allies to secure alternative tech supplies and bypass sanctions. These partnerships allow China to access critical technologies and continue its technological development despite restrictions imposed by Western countries. By fostering these relationships, China has ensured a steady flow of technology and resources, which further strengthens its global influence.

Another significant strategy China has employed is strengthening its Belt and Road Digital Initiative (BRI-DI). Through this initiative, China has been able to expand its digital infrastructure projects across Asia, Africa, and Europe, offering loans and investments in telecommunications and tech infrastructure. This initiative not only extends China's geopolitical influence but also allows it to embed surveillance capabilities in critical digital infrastructure worldwide. By controlling such infrastructure, China can gain access to sensitive data across various regions, further enhancing its global surveillance and intelligence-gathering operations.

In conclusion, while international sanctions and restrictions have aimed to curb China's digital surveillance capabilities, China has continued to adapt and expand its influence through domestic manufacturing, strategic alliances, and initiatives like the BRI-DI. The need for a global, coordinated response remains crucial, as China's countermeasures highlight the challenges faced in curbing its growing technological power.

5. CONCLUSION

China's digital surveillance state, supported by the National Intelligence Law (2017/18), poses a major national security risk. While the U.S., Japan, Germany, and other nations have implemented strict countermeasures, China continues to adapt by strengthening domestic innovation and strategic partnerships. However, the measures taken thus far remain far from adequate in addressing the full scope of this growing threat. The global security landscape demands urgent, coordinated action from first-world nations to counter China's increasingly aggressive espionage tactics.

China's penetration into critical infrastructure, communication networks, and emerging technologies presents a high-risk scenario for global security. The The Zhenhua Data (India China Boarder Tension 2020) case in India highlighted the real-world implications of China's espionage strategy, proving that Chinese

companies operate as state-backed intelligence gatherers. These firms leverage sophisticated cyber tools, artificial intelligence, and low-cost technology exports to infiltrate foreign institutions under the guise of commercial partnerships. The global community cannot afford to overlook the extent of this strategic manipulation, as China's digital influence continues to erode national sovereignty and compromise sensitive information across borders.

Recognizing the urgent need for action, several measures have been proposed to mitigate these risks. Recommendations include prohibiting high-risk foreign drone manufacturers from supplying technology to government agencies and critical sectors, establishing rigorous cybersecurity certification requirements for commercial drone use, and mandating stringent supply chain vetting to eliminate vulnerabilities. Additionally, there is a push for increased funding toward domestic drone development to reduce reliance on Chinese-made technology. Furthermore, a growing number of nations are implementing import bans on Chinese appliances, particularly smart devices, due to concerns over built-in surveillance capabilities and data security risks. These bans aim to prevent backdoor access to critical infrastructure and personal data, safeguarding national security interests. However, these efforts alone are not sufficient. The lack of an internationally unified approach allows China to circumvent restrictions through third-party agreements and proxy companies.

China's surveillance apparatus represents one of the greatest global cybersecurity threats. Through state-backed legal mandates, cyber intrusions, and strategic acquisitions, China has embedded itself into global digital infrastructure as a Trojan Horse. While some nations have imposed sanctions and trade restrictions, the regulatory framework remains fragmented and insufficient to counter the broader intelligence threat. Without immediate international action, China will continue expanding its control over global data, endangering individual privacy, national security, and democratic institutions worldwide. It is imperative that first-world nations adopt a cohesive, proactive stance, including legislative cooperation, intelligence-sharing, and technological innovation, to dismantle China's pervasive surveillance network before it further compromises global security

6. RECOMMENDATIONS

1. While the U.S. and other nations have made significant strides in restricting China's access to advanced AI chips, it is equally critical to block China's access to emerging technologies such as **cloud computing** and **quantum technology**. These technologies are pivotal to China's growing surveillance capabilities and its ability to process vast amounts of data. By restricting China's ability to access or develop cutting-edge technologies in these fields, nations can hinder China's ability to advance its digital espionage operations and prevent it from embedding surveillance tools in critical global infrastructure.

2. Governments should invest in **AI-based cybersecurity systems** that can actively monitor and detect data espionage activities. These systems should be capable of identifying malicious activity linked to surveillance technologies, particularly from Chinese-made devices, and blocking unauthorized data transmissions to foreign governments or entities. Such systems can be integrated into both public and private sector operations to enhance real-time monitoring of digital and physical infrastructure and prevent the unauthorized export of sensitive data.

3. To effectively counter China's growing cyber-espionage network, international cooperation is essential. Nations should form a **global intelligence-sharing alliance** focused on digital threats, particularly those originating from China. By sharing intelligence on cyber-attacks, espionage tactics, and emerging threats, countries can bolster their collective defenses and create a unified front against China's surveillance activities. This collaboration should extend to global cybersecurity standards, helping nations develop common frameworks to detect and mitigate surveillance risks, especially in critical infrastructure.

4. To safeguard national security, countries should enhance their **economic security laws**, particularly those governing **investment screening** and foreign acquisitions of sensitive technologies. This will help prevent Chinese firms from gaining control over critical tech sectors like 5G infrastructure, AI, and semiconductor production. Strengthening screening mechanisms can block Chinese investments that pose

risks to national security and prevent Chinese companies from gaining access to vital technology in strategic industries.

6.1 Addressing China's Surveillance Network

The Chinese government has effectively used its domestic laws, cheap technology, and global business operations to build a sophisticated surveillance network that spans across continents. Despite facing international sanctions, China has successfully bypassed these restrictions by leveraging third-party nations, using economic aid and investments as a tool to export surveillance technologies disguised as infrastructure development. The **Galwan Valley incident** in 2020 demonstrated how China can use **cyber warfare** as a strategic tool to target critical infrastructure, underlining the need for stronger international measures to counter such tactics.

6.2 Countering the Trojan Horse Threat

To effectively counter the Trojan Horse threat posed by China's global data intrusion, several key actions must be taken:

- Governments and civil society must lead efforts to raise awareness about the risks of Chinese surveillance technologies embedded in everyday devices, such as IoT devices and smartphones. Public education campaigns should emphasize the importance of safeguarding personal data and the potential national security risks associated with these devices.

- Nations must implement and enforce stricter trade and technology export controls to prevent Chinese companies from circumventing sanctions through third-party countries. Monitoring and closing loopholes in the export control system will help ensure that China is unable to bypass these restrictions and continue expanding its surveillance operations globally.

- A unified global cybersecurity coalition should be developed to establish standardized countermeasures against digital authoritarianism. This coalition can create international norms and enforceable regulations to restrict the flow of surveillance technologies from China, ensuring that foreign governments are not complicit in enabling China's global surveillance network.

By implementing these recommendations, the global community can strengthen its defenses against China's expanding digital espionage and safeguard technological sovereignty. Enhanced international cooperation, stronger legal frameworks, and a concerted public awareness campaign are essential to mitigating the risks posed by China's technological influence and protecting critical global infrastructure from surveillance and cyber-attacks.

6.3 Policy Recommendations to Counter China's Digital Surveillance and Cybersecurity Threats

To effectively counter the growing security risks posed by Chinese technology infiltration, a comprehensive, multi-faceted policy approach is essential. The following recommendations focus on legislative action, cybersecurity enhancement, supply chain security, and international cooperation to mitigate the threats from China's surveillance and intelligence-gathering operations:

6.4 Strengthening Legislative and Regulatory Frameworks

1. Prohibit the import and deployment of Chinese-manufactured smart appliances, drones, telecommunications equipment, and surveillance technologies in critical infrastructure, government agencies, and sensitive sectors. These products, particularly from companies such as Huawei, DJI, and Hikvision, are suspected of facilitating state-backed surveillance and espionage, posing serious national security risks.

2. Require foreign technology firms, especially those based in China, to undergo rigorous cybersecurity evaluations and supply chain audits before being allowed to operate in Western markets. This will ensure that these companies meet high standards for protecting sensitive data and infrastructure, and prevent the infiltration of surveillance technologies under the guise of commercial products.

3. Strengthen Foreign Direct Investment (FDI) regulations to prevent Chinese state-linked entities from acquiring stakes in industries critical to national security, such as telecommunications, energy, and AI development. These sectors are particularly vulnerable to espionage and must be safeguarded from foreign influence that could compromise national security.

6.5 Enhancing Cybersecurity Measures

1. Establish cross-sector cybersecurity regulations that specifically address vulnerabilities in IoT devices, drones, and communication networks. These regulations should be designed to reduce the risk of surveillance and data theft, especially from Chinese technology providers. Standardized security practices should be adopted across sectors that use digital infrastructure and communication technologies.

2. Deploy AI-driven security solutions to monitor, identify, and neutralize Chinese-backed cyber threats in real time. These systems can be used to detect unusual patterns, anomalies, and potential data breaches from surveillance technologies, providing an added layer of protection against espionage.

3. Require companies handling sensitive data to adopt end-to-end encryption, secure firmware updates, and AI-based anomaly detection systems. By improving the cyber resilience of private sector firms, especially those in critical industries, the risks of espionage and data theft can be significantly reduced.

6.6 Regulating the Drone and Smart Appliance Industry

1. Implement universal security standards for drone hardware, software, GPS restrictions, and encryption to prevent unauthorized data collection and surveillance. This includes making sure that all devices meet strict security protocols, such as ensuring that surveillance devices cannot transmit data back to foreign governments without user consent.

2. Ban the use of Chinese-manufactured UAVs (Unmanned Aerial Vehicles) in government operations, military applications, and law enforcement agencies due to the high espionage risks associated with their technology. This step would prevent China from using drones as tools for surveillance in sensitive governmental and security contexts.

3. Enforce strict labeling and reporting requirements for all imported drones and smart devices. This would ensure full transparency regarding the device's software, firmware, security protocols, and data collection capabilities, allowing authorities to assess potential surveillance risks before granting permission for use.

6.7 Expanding Intelligence and International Cooperation

1. Establish a joint intelligence-sharing alliance among key nations, such as the U.S., EU, Japan, India, and other strategic partners, to track, monitor, and counteract Chinese cyber threats. This network would facilitate the exchange of actionable intelligence and provide coordinated responses to cyberattacks.

2. Develop a coordinated international task force aimed at detecting and dismantling China's global cyber espionage infrastructure. The task force would work to identify Chinese-backed surveillance networks, disrupt their operations, and prevent the spread of Chinese surveillance technologies worldwide.

3. Promote technological collaboration among democratic nations to create secure, non-Chinese alternatives to Chinese tech in areas such as 5G, AI, and cloud computing. By investing in secure alternatives, allied nations can reduce their dependency on Chinese technology and limit the influence of Chinese firms in critical global infrastructure.

6.8 Promoting Domestic Innovation and Secure Technology Development

1. Governments must allocate significant funding to domestic firms that specialize in secure AI, telecommunications, and cybersecurity solutions. By investing in research and development (R&D), nations can reduce their reliance on Chinese technology and develop their own secure digital infrastructure. This can include developing homegrown 5G networks, AI-powered security solutions, and secure

communication technologies, ensuring that critical sectors are protected from foreign surveillance and digital threats.

2. To reduce dependence on Chinese-made drones (UAVs), IoT devices, and network hardware, governments should create incentives for local manufacturers. These incentives could include subsidies, grants, or low-interest loans for domestic firms engaged in producing secure alternatives to Chinese technologies. Local manufacturing would not only strengthen national security but also stimulate job creation and technological innovation within the country.

3. Governments should provide tax credits and subsidies to companies investing in the development of cybersecurity innovations and privacy-protecting technologies. These incentives would encourage firms to prioritize security and privacy in their technological developments, ensuring that domestic products meet high standards for cybersecurity and data protection. This can also help create a competitive, secure tech industry capable of offering alternatives to Chinese surveillance products.

6.9 Strengthening Public Awareness and Legal Accountability

1. It is crucial to establish and enforce stringent data protection laws that impose clear legal penalties for unauthorized data collection and espionage activities. These laws should hold companies and individuals accountable for engaging in or facilitating cyber-espionage, particularly when foreign intelligence agencies are involved. By setting legal precedents for violations of data security and surveillance laws, nations can deter cybercriminal activity and reduce the exploitation of personal and corporate data.

2. Public awareness campaigns are essential to educating businesses and individuals about the cybersecurity risks associated with using Chinese-made technology. Governments should launch educational initiatives that highlight the vulnerabilities posed by Chinese surveillance devices and IoT products. These campaigns should target both consumers and corporate sectors, emphasizing the importance of secure technology choices, good cybersecurity practices, and the risks of data theft from foreign-backed surveillance systems.

3. Implement strict regulations on data brokerage and cross-border data transfers to prevent the exploitation of sensitive personal and corporate data by foreign adversaries. These regulations should ensure that companies handling data adhere to high standards of security and privacy. Furthermore, data brokers who facilitate unauthorized data sharing must face strict penalties. This would help protect citizens' privacy and prevent sensitive information from being accessed or misused by foreign entities, particularly in cases where Chinese firms are involved.

6.10 Addressing China's Growing Influence on Global Digital Infrastructure

China's expanding influence over global digital infrastructure, facilitated by its cyber surveillance apparatus, state-backed legal mandates, and strategic acquisitions, poses an unprecedented security challenge. Despite sanctions and trade restrictions, China has successfully circumvented these measures by leveraging third-party countries to access markets and acquire critical technologies. This ongoing ability to bypass international restrictions allows China to continue infiltrating global technology markets, putting national security, privacy, and democratic institutions at risk.

6.11 A Coordinated Approach Is Needed

To effectively counter these threats, Western nations and their allies must take a coordinated approach, focusing on comprehensive cybersecurity measures, domestic innovation, and the creation of international legal frameworks. By taking immediate and united action, countries can begin to protect their critical infrastructures from Chinese digital influence. However, if such measures are not taken, China's continued digital expansion will likely compromise national security, individual privacy, and the integrity of democratic institutions worldwide. The time for a unified, multi-faceted strategy to safeguard digital sovereignty is now.

REFERENCES

1. Bhat, S. (2022). “Zhenhua Data: Exposing China’s Digital Espionage in India.” Journal of International Cybersecurity, 41(2), 198-212.
2. Bhat, S. (2022). Zhenhua Data: Exposing China’s Digital Espionage in India. Journal of International Cybersecurity, 41(2), 198-212.
3. Carson, M., & Jones, P. (2023). Countering China’s 5G Influence in Global Telecom Networks. Telecom Security and Policy Journal, 29(1), 92-104.
4. Center for Strategic and International Studies (CSIS). (2023). Chinese-Made IoT Devices and Their Role in Global Cyber Espionage. CSIS Tech Analysis Series.
5. Clarke, H. (2023). Data Sovereignty in the Age of China’s Surveillance Network. Global Cyber Policy Review, 11(3), 65-78.
6. Deibert, R., & Roio, A. (2022). The Rise of Digital Authoritarianism: The Case of China. Global Governance Review, 12(1), 18-32.
7. European Commission. (2023). The European AI Act: Implications for Global Digital Surveillance. EU Digital Policy Review.
8. Feng, J., & Li, Y. (2020). The National Intelligence Law of China: A Legal Foundation for Espionage? Journal of Cybersecurity Policy, 18(2), 145-161.
9. Gallagher, S. (2022). Technological Sovereignty and National Security: The Role of Cybersecurity in Preventing Espionage. International Security Review, 21(4), 45-59.
10. Gao, J., & Zhang, W. (2023). Huawei, TikTok, and the Expansion of Chinese Surveillance Technologies. Technology and Global Security Review, 29(1), 73-88.
11. International Telecommunications Union (ITU). (2023). Global Trends in 5G and Digital Sovereignty. ITU Reports.
12. Kuo, L. (2021). The Global Reach of China’s Surveillance State. The New York Times, June 10, 2021.
13. Li, Y., & Liu, J. (2023). The Evolution of China’s Surveillance Technology and Its Impact on Privacy. Journal of Global Privacy, 9(1), 54-72.
14. Lim, C., & Lee, S. (2022). China’s Influence on Global 5G and Its Surveillance Implications. Asian Security Journal, 40(2), 222-238.
15. Liu, L., & Zhong, H. (2021). China’s Data Security Law and Its Implications for Global Cybersecurity. International Journal of Cyber Law, 35(4), 210-225.
16. Liu, Z., & Qiao, F. (2023). China’s AI Surveillance Tools: Expansion and Security Threats. Cybersecurity Trends Quarterly, 5(3), 13-25.
17. Matthews, P., & Harris, D. (2022). Assessing the Security Risks of Chinese Telecom Equipment. Telecom Security Review, 19(5), 47-59.
18. McKinsey & Company. (2023). The Future of Global Telecom Infrastructure: Challenges and Opportunities. McKinsey Global Institute.
19. National Institute of Standards and Technology (NIST). (2023). Secure Technology and Surveillance: A Global Perspective. NIST Cybersecurity Framework.
20. Office of the Director of National Intelligence (ODNI). (2023). Annual Threat Assessment: China’s Digital Espionage and Cyber Warfare. U.S. Government Reports.
21. Pitel, L., & Lequesne, C. (2021). The China–Europe Digital Divide: How Surveillance Tech is Reshaping Global Politics. European Journal of International Relations, 27(1), 66-83.
22. Rai, P. (2021). “India's Response to Cyber-Espionage: The Zhenhua Data Case and Its Consequences.” Indian Journal of Cyber Law and Policy, 16(3), 105-121.
23. Rai, P. (2021). India’s Response to Cyber-Espionage: The Zhenhua Data Case and Its Consequences. Indian Journal of Cyber Law and Policy, 16(3), 105-121.
24. Sandoval, D., & Chang, X. (2022). China's Cybersecurity Strategy and Its Impact on Global Supply Chains. Journal of Cybersecurity Studies, 18(4), 254-269.
25. Schwartz, J., & Zhang, W. (2022). Global Governance and the Threat of Chinese Cyber Espionage. Global Security Studies Journal, 34(2), 143-156.

26. Sharma, R. (2021). “Zhenhua Data Leak: A Cyber Espionage Case Study.” Cybersecurity and Global Affairs Review, 11(4), 44-58.
27. Sharma, R. (2021). Zhenhua Data Leak: A Cyber Espionage Case Study. Cybersecurity and Global Affairs Review, 11(4), 44-58.
28. Shen, L. (2022). Artificial Intelligence and the Chinese Surveillance State. Global Technology Analysis Journal, 47(3), 112-125.
29. U.S. Department of Commerce. (2023). Annual Report on Export Control Violations: China’s Semiconductor Supply Chain. U.S. Government Publications.
30. van der Meer, J. (2021). The Global Battle for 5G: China’s Role in Shaping Digital Futures. International Affairs Review, 22(4), 341-355.
31. Williams, T. (2023). China’s Belt and Road Initiative and the Spread of Surveillance Technologies. Global Policy Journal, 27(2), 123-137.
32. Zhang, H., & Li, P. (2023). China’s AI Strategy and Global Surveillance Implications. Journal of Global Security Studies, 15(3), 98-112.
33. Zhao, L., & Wang, Q. (2021). The Impact of China’s National Intelligence Law on Global Cybersecurity. Asian Journal of Cybersecurity, 12(1), 99-113.

a. Publication URL: https://cibgp.com/au/index.php/1323-6903/article/view/2868
Siddiqui, H. R. ., & Leghari, A. . (2007). FAITH, FREEDOM, AND THE FUTURE: RECLAIMING INCLUSIVE DEMOCRATIC VALUES IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 13(1), 107–116. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2868

b. Publication URL: https://cibgp.com/au/index.php/1323-6903/article/view/2870
Siddiqui, H. R. ., & Leghari, A. . (2008). LIBERALISM IN SOUTH ASIA, A CASE STUDY OF CIVIC LEADERSHIP AND INTERFAITH HARMONY. The Journal of Contemporary Issues in Business and Government, 14(2), 90–97. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2870

c. Siddiqui, H. R. ., & Muniza, M. . (2009). SOWING ILLUSIONS, REAPING DISARRAY: MEDIA INFLUENCE, URBAN MIGRATION, AND THE DISMANTLING OF SOCIETAL NORMS IN SOUTH ASIA. The Journal of Contemporary Issues in Business and Government, 15(2), 126–139. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2871

d. Publication URL: https://cibgp.com/au/index.php/1323-6903/article/view/2872
Siddiqui, H. R. . (2011). IN THE COURT OF KNOWLEDGE, JUDGING THE JUDGES OF LEARNING. The Journal of Contemporary Issues in Business and Government, 17(1), 83–91. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2872

e. Publication URL: https://cibgp.com/au/index.php/1323-6903/article/view/2873
Siddiqui, H. R. . (2013). THE PERSONAL LENS IN ACADEMIC EVALUATION: A CRITIQUE OF EDUCATOR BIAS. The Journal of Contemporary Issues in Business and Government, 19(1), 93–101. Retrieved from https://cibgp.com/au/index.php/1323-6903/article/view/2873

f. Siddiqui, H. R. (2016). ESTABLISHING AIR AMBULANCE SERVICES IN PAKISTAN: A REGULATORY AND INVESTMENT FRAMEWORK FOR EMERGENCY MEDICAL AVIATION. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 2(5), 17-30. https://doi.org/10.61841/z1tjva12
Publication URL: https://nnpub.org/index.php/EL/article/view/2828
DOI: https://doi.org/10.61841/txq2w096
Siddiqui, H. R. . (2019). WHO JUDGES THE JUDGES? ADDRESSING INTEGRITY AND SECURITY GAPS IN THE SINDH JUDICIAL RECRUITMENT SYSTEM. International Journal of Advance Research in Education & Literature (ISSN 2208-2441), 5(8), 5-15. https://doi.org/10.61841/txq2w096

g. H.R.(2022).PUBLIC FUNDS, PRIVATE GAINS: INVESTIGATING CORRUPTION IN NADRA’S MEGA CENTER LEASE DEALS. Journal of Advance Research in Social Science and Humanities (ISSN 2208-2387), 8(12), 17-28. https://doi.org/10.61841/2s3kmv78

h. https://crlsj.com/index.php/journal/article/view/448
DOI: https://doi.org/10.52783/crlsj.448

i. Siddiqui, H. R. (2023). STRUCTURAL INJUSTICES IN THE RECOGNITION OF FOREIGN MEDICAL DEGREES BY THE PAKISTAN MEDICAL COUNCIL: A CALL FOR POLICY REFORM. Journal of Advanced Research in Medical and Health Science (ISSN 2208-2425), 9(1), 58-67. https://doi.org/10.61841/vmqgts53
j. https://www.russianlawjournal.org/index.php/journal/article/view/4997
k. Publication URL: https://nnpub.org/index.php/SSH/article/view/2829
Hassan Rasheed Siddiqui, Maria Muniza. (2025). 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. Social Sciences & Humanity Research Review, 3(1), 567–584. Retrieved from https://jssr.online/index.php/4/article/view/94
l. Hasan: 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
m. 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
n. Hassan Rasheed Siddiqui, and Ms. Maria Muniza. 2024. "The Drone's Gaze, Religious Perspective on Privacy and Human Dignity in the Age of Surveillance Mentioning Security Threats & Regulatory Gaps". Al-Qamar, December, 1-12. https://doi.org/10.53762/alqamar.07.04.e01.
o. MS Shahzadi Sarwat Noreen, Talat Ara. (2025). THE ROLE OF INTERNATIONAL LAW IN AI DRONE REGULATIONS. Social Sciences & Humanity Research Review, 3(1), 626–645. Retrieved from https://jssr.online/index.php/4/article/view/98