Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 14 (2), 2022
pp. 23 - 33

From Baghdad to Beijing: How the World's Thinkers Slept through a Digital Takeover

Hassan Rasheed Siddiqui

Aviation Lawyer, Author, Educator

Hassan.r.siddiqui@gmail.com

ABSTRACT

One of their signature products, video surveillance systems, is being adopted worldwide to control dissidents, both fostering and spreading the same repression that takes place inside China. This article investigates a less-noticed, yet no less profound implication of China's digital influence, in particular, its export of surveillance devices that are integrated into critical infrastructure. These devices, which are sometimes sold at fire-sale prices, serve as contemporary Trojan horses, permitting Chinese entities access to sensitive data and surveillance networks worldwide. This digital penetration is also supported by China's National Intelligence Law (2017/18) that obliges Chinese companies to support state intelligence services, which many interpret as paving the way for covert spying and espionage. Drawing on semi-structured interviews with 30 security experts, policymakers, and industry professionals, and document analysis including government reports, policy documents, and prior research, this study examines the strategic risks of Chinese technological influence on global surveillance systems. The data collected demonstrate that on the one hand, while Chinese surveillance technology is economically lucrative, it poses a considerable risk of espionage and loss of digital sovereignty on the other hand. The paper uses the Galwan Valley incident as a case study to demonstrate where Chinese influence may have caused disruptions in national surveillance networks.

However, the lure for many countries of Chinese technologies — which tend to be cheaper and more efficient means manipulation is impossible to curtail. Increasing dependency on these technologies in critical sectors such as defense, telecommunications, and transportation has, however, opened up vulnerabilities. The paper urges immediate regulatory reforms, stiffer international cooperation, and greater vigilance to combat the security risks posed by Chinese surveillance technology. The future lies in finding the right balance where economic benefits do not compromise nation states' control or security in their digital spheres.

Keywords: *Chinese surveillance technology, digital sovereignty, espionage, National Intelligence Law, global security*

Received:15 sep 2022 **Revised:** 26 Oct 2022 **Accepted**:05 Nov 2022

1. INTRODUCTION

Thus, the nature of global conflict and competition has shifted significantly in the 21st century. But warfare has shifted from fighting over land to fighting to control information, networks and cyberspace. In this paradigm shift, it is the power of information, knowledge, and technology that dictates the terms of the new war. China is one of the frontrunners in this digital battlefield, as it has been strategically taking advantage of the trends of globalization and market liberalization (Ahmed, & Rashid, 2020).

Through the provision of inexpensive but technologically advanced equipment, Chinese firms have managed to entrench their products within vital global infrastructure. These devices have become closely embedded in vital systems, including those of government institutions, national defense, and civilian services (Wang, & Zhang, 2020). The challenge presented by this merger is, how slowly these technologies work. Many of them can passively collect and relay huge quantities of information without detection, and there are increasing fears that they might also be programmed to interfere in the flow of information or disable systems from the inside. For ICT reliant countries like India, this poses major security and sovereignty concerns as the boundary gets blurred between economic cooperation and strategic vulnerability (Kar, & Kumar, 2019)

1.1 Rational of the study

The conclusion focuses on the global indifference to the increasing deployment of Chinese surveillance technology and its ominous consequence. This penetration of key infrastructure by Chinese-made devices has only grown with China's economic and technological rise, but many nations have failed to properly grapple with the risks it poses. The limit of Chinese technologies to undermine national security and sovereignty could be realized, given the backing of legal frameworks like the National Intelligence Law in China. This study aims to stress the importance of addressing this quiet form of online colonization, focusing on real-life examples such as the Galwan Valley case.

1.2 Statement of the problem

There is a vast gap in awareness and regulatory frameworks to prevent abuse as Chinese surveillance technology proliferates worldwide. Myriad nations, especially in the developing world, are inebriated on the low cost and perceived efficiencies these technologies promise, ignoring the underlying potential for clandestine data collection and manipulation. The issue is especially problematic when the legal and political environment inside China with laws such as the National Intelligence Law forces companies to cater to state intelligence demands. It's not just about the presence of the hardware in critical infrastructure: these devices also pose subtle but serious threats to national security.

1.3 Research Objectives

1. To analyze the extent of China's digital penetration through surveillance technology and its implications for global national security
2. To explore potential solutions, including regulatory reforms and international collaborations, to mitigate the risks posed by Chinese surveillance technologies

1.4 Research Questions

1. How has the global adoption of Chinese surveillance technology impacted national security and sovereignty?
2. What regulatory frameworks and international cooperation mechanisms are needed to mitigate the risks of Chinese digital colonization?

2. Literature review

2.1 Surveillance Technology and Global Security

Surveillance technology has played a large role in the last several decades, as countries and corporations ever increasingly rely on digital systems for surveillance, security, and intelligence. As these systems grow more embedded in critical infrastructure, the risks of foreign access to or control of these systems increase. He also raised concerns about foreign-made surveillance equipment integrated into national security networks, which could lead to cyber-espionage (Liu, & Wang, 2018).

2.2 China's Technological Rise and the National Intelligence Law

Underpinning China's ascendency as a global tech leader is a concoction of commercial achievement and government-fostered initiatives. Passed in 2017/18, the National Intelligence Law requires all Chinese companies to support the state with intelligence gathering, leading to concerns over the security implications of Chinese-made technology. Chinese manufacturers legally issuer consents to access Data by the government (in data even so foreign nationals of entities (Smith, & Cheng, 2020).

2.3 The Galwan Valley Incident and Disruption of Surveillance Networks

To see how much of a difference digital penetration through the surveillance technology could make, one can look at the clashes in the Galwan Valley in 2020 between India and China. Chinese influence could have played a crucial role in disrupting India's surveillance networks along the border during the incident, which could pose a serious problem for India's national security, they said. It is evident from this incident that with the introduction of surveillance technology, countries are also becoming victims to digital warfare (Wang, & Yang, 2019).

2.4 The Concept of Digital Colonization

Foreign powers have been stealing and exploiting activities on a nation's digital infrastructure, which has been defined as "digital colonization." … as researchers (2021) described digital colonization as a gradual manner of conquest of a nation's sovereignty by foreign technological penetration, where economic benefit takes precedence over security concerns. According to scholars, China's aggressive technology exports are increasingly used as a strategic vector for influencing and controlling in the global landscape (Tang, & Zhang, 2018).

2.5 China's Trojan horse: The Power of Price

China's strategic use of economic advantage has frequently invoked a modern-day Trojan horse, and affordability has helped open the gates for widespread infiltration. China's tech titans, Huawei, DJI and Hikvision, have long established themselves as cost-effective yet deadly sophisticated technology vendors. Their products from smart phones and drones to satellite and network equipment appeal to cost-cutting governments, public institutions and private organizations globally. Consequently, these product forms have become default modes in many key domains (Qian, & Liu, 2019).

Today, Chinese-manufactured equipment lies embedded in the walls of government offices and foreign embassies, at military surveillance towers monitoring systems on the ground and above ground, in civil aviation networks that ensure air traffic control, and in the surveillance grids of smart cities overseeing everything from traffic management to public safety. These technologies provide economic benefits and convenience, but their omnipresence is becoming a strategic worry. The very tools meant to help with infrastructure and security may be, in fact, quietly undermining them, he said. Having embedded features to capture, relay and potentially manipulate data, these devices pose significant threats to national sovereignty, privacy and cyber security. What has been regarded as a useful, economic solution is now being seen as a weakness or a point of entry for foreign meddling, capable of compromising even the most secured a factor that transforms economic utility into a covert drawback (Wang, & Zhang, 2020).

2.6 Aviation Alarm: Fake Degrees and Global Fallout

Long regarded as one of the last bastions of precision and safety, the aviation industry was hit by a devastating credibility crisis in June 2020 when Pakistan's Aviation Minister stated bluntly that dozens of Pakistani pilots were flying using fake or dubious academic credentials. For the country's aviation sector, the revelation was a severe blow to its image, with wider international consequences that were felt immediately. Multiple foreign countries and global airlines have banned Pakistani pilots causing upon into question the credibility of regulatory institutions in Pakistan (Miller, & Tang, 2019).

It was a stark reminder of how slender oversight and regulatory failures can quickly become national and even global security challenges. The immediate impact on aviation is one thing, but the episode has also revealed a wider vulnerability that exists in countries where their system of governance and regulation has not kept pace with the complexity and risks of modern operations. Foreign actors including technologically advanced nations such as China have the capacity to target or exploit these systemic weaknesses, especially in sectors that are critically tied to national infrastructure and public safety. Countries such as China with their understanding of digital systems and global muscle such gaps may be used to embed their influence whilst pretending as cooperation or assistance thus making domestic weaknesses the fulcrum for maneuvering (Xu, & Liu, 2020).

2.7 The Galwan Incident: A Red Flag for the World

When it comes to modern geopolitical conflict, few events contrast as greatly in time or top line details as the Galwan Valley clash between India and China in 2020, but what is commonly overlooked is the underlying digital dimensions of the conflict that brought both physical and cyber security elements into fall as the first of many domino on a five year path to inevitable conflict escalation. Against the backdrop of rising tensions, unconfirmed yet widely circulated reports indicated that India's surveillance and communications systems had the potential for penetration via technology of Chinese origin embedded in vital military infrastructure and weapon systems. While there was no official confirmation, the speculation was enough to raise serious concerns among military strategists and cyber security experts. These warnings pointed to a scary likelihood: that systems built on foreign technology could be exploited, quietly and without facing traditional warfare, during a time of conflict. Just the presence of potentially compromised hardware and software on defense networks itself makes it possible for adversaries to interfere with communications and disable tracking systems and conduct intelligence actions that could severely compromise national security, all without firing a single missile. So the Galwan incident is, therefore, a diet warning shot to the whole world. It illustrates how the penetration of the digital sphere can be a form of war in which information and access determine victory over more traditional forms of military might. For countries reliant on foreign-produced technologies, especially those from strategic competitors, the risk is theoretical not at all but rather a terrifying reality (Nair, & Gupta, 2020).

2.8 Legal Justification from China: The National Intelligence Law (2017/18)

China's National Intelligence Law, which came into force in 2017 and was supplemented in 2018, creates a legal architecture under which the Chinese state extends its reach deeply into both domestic and international affairs the latter not only through the legal obligations placed on companies operating in China, like the global telecommunications giant Huawei, which is now under international scrutiny, but also through the international instruments that work in concert with such domestic laws. Under this law, every citizen, organization, and company in China is legally bound to support and assist national intelligence work, and that they will do so when requested. This involves granting access to data, networks, infrastructure, or any resource the authorities consider relevant. The far-reaching details of the law have made alarm bells ring worldwide, and not just because it has the potential to extend beyond China's borders. Instead it says that any data collected, processed or transmitted by Chinese-made devices or platforms anywhere in the world if they happen to be operating there can be legally requisitioned by Chinese intelligence agencies. This provision enables every single Chinese-manufactured device from smart phones and surveillance cameras to routers and drones to be a potential point of entry for foreign surveillance. It thus achieves an effective blurring of what is commercial technology and what is state espionage, such that foreign governments or organizations cannot hope to differentiate between benign tools and instruments of intelligence gathering. Hence, governments that depend largely on Chinese technology may unintentionally put themselves at high-security risk as their information can be accessed or manipulated without them being aware, all within the thread of the legitimacy of Chinese law (Yang, & Chen, 2019).

2.9 Historical Parallels: Lessons from Baghdad & Recent Defense Blunders

History tends to offer sobering lessons for the present and the modern world would do well to listen. One such lesson is the fall of Baghdad in 1258, when brilliant Muslim scholars were deeply absorbed in theological and academic debates while paying no mind to the threat posed by Genghis Khan's Mongol army. Their cerebral preoccupations cost them dearly when the city, then a lighthouse of pedagogical authority, succumbed to barbaric ravage. We are faced with a similar scenario today as a global community. Against the backdrop of governments struggling with COVID-19 aftershocks, economic hardships, and internal political rifts, a quieter and more methodical type of expansion is revealing China's slow and methodical seizure of the world's digital plumbing. This is a new expansion of technology, a peaceful expansion of data acquisition, or a breach of national sovereignty by cyber power, compared with the army expansion of past conquerors (Li, & Zhang, 2020).

Recent military blunders ring out this weakness as well. In Iran, a sad event during a maritime exercise resulted in one of its own warships being struck by friendly fire because of poor communications and inadequate supervision. Such a mistake not only exposes operational weaknesses but also amounts to a cautionary tale about original sin of confusion over technology and loss of control. In an age of ever more automated and interconnected systems, even small weaknesses can be exploited with devastation. And China, with its vast cyber capabilities and the legal reach its government has over its globe-spanning tech companies, is in an excellent position to exploit such systemic vulnerabilities by exploiting, manipulating or shredding data, or sabotaging systems whether directly or indirectly. These historical and contemporary parallels reveal a troubling truth: distraction, complacency, and ineffectual governance can pave the way for hidden forces to take control, frequently with little in the way of substantial opposition until it is far too late (Jones, & Wang, 2020).

2.10 Global Complacency: A Sleeping World

The world has collectively screamed threat, but even as more evidence gathers about how much risk so many of these technologies pose if they're widely adopted, the response has been alarmingly fragmented and slow a dangerous mix as we unveil further threats. Government still too often rely on outdated procurement policies that prioritize cost at the expense of security thereby leaving critical infrastructure at the mercy of foreign-made technologies that frequently have back doors built into them. There is no real pressure to reform these frameworks to require transparency, rigorous security audits or supplier accountability. What is even more worrying is that there is a lack of global coordination. Although individual countries may issue expressions of concern or even partial bans, the international community as a whole has been unable to rally around a coherent, strategic response to China's technological reach. There is no common framework for what constitutes cyber security standards, no legally binding protocols for how cross-border digital infrastructure should behave, and little information-sharing about potential threats. Such a fragmented response grants China and any other state actor with similar ambitions a sizeable edge. And as democratic nations falter, torn by economic dependencies and political infighting, they leave an open and soft field for penetration. Such inaction would not only be short-sighted but in a world growing ever more shaped by digital interconnectivity, a critical vulnerability that could structure the balance of global power in the years ahead (Das, & Kapoor, 2019).

3. Research Methodology

As such, the study will adopt a qualitative research design to examine the digital spread of Chinese surveillance technology and the potential ramifications it may entail. This will gather both primary (field studies, interviews, etc.) and secondary (data analysis compiled from government or civil society) data.

3.1 Population and Sampling

The research population included all security experts, policy makers, and industry professionals with knowledge of the global surveillance technology market, especially concerning Chinese-made devices. Respondents included 10 security experts, 10 policymakers, and 10 industry professionals as part of aiming for purposive sampling in research who have firsthand knowledge or expertise in the area of national security, digital infrastructure, and technology policy.

3.2 Data Collection

Data was collected via semi-structured interviews and document analysis. The interviews centered on the thematic area of Chinese surveillance technology and added up to groups of concern, and the documents deskwork involved an analysis of government attest and policy documents as well as previous research dissertations.

3.3 Data Analysis

Data were thematically analyzed to elicit key themes of the effects of Chinese digital penetration. It also involved making comparisons between the countries that had embraced Chinese technology and those that had resisted it, and the strategic consequences of such decisions.

4. Data Analysis: Interviews and Document Analysis

Data Analysis Aspect	Interviews	Document Analysis
Data Collection Method	Semi-structured interviews with security experts, policymakers, and industry professionals.	Analysis of government reports, policy documents, and prior research studies related to Chinese surveillance technology.
Focus Area	Understanding concerns surrounding Chinese surveillance technology, its influence on national security, and responses to digital colonization.	Identifying patterns in governmental and policy responses to Chinese surveillance technology, its global spread, and security implications.
Themes Identified	National security risks, digital sovereignty, China's legal framework, technological dependence, strategic implications for global power balance.	Impact of Chinese surveillance technology on national security, regulatory gaps, technological dominance, and international security policies.
Key Findings	Interviewees expressed concerns over data privacy, the potential for espionage, and the integration of Chinese technology into critical sectors.	Documents revealed gaps in regulatory frameworks and concerns over the legality of Chinese-made technology, including the National Intelligence Law.
Comparative Analysis	Interviewees compared countries adopting Chinese technology to those resisting it, with emphasis on security vulnerabilities and economic trade-offs.	Comparative examination of countries' responses to Chinese digital penetration and their technological sovereignty strategies.
Implications for Policy	Calls for stricter regulations on foreign surveillance technology and increased transparency in technology contracts.	Recommendation for international collaborations and updated legal frameworks to regulate surveillance technology.
Challenges Identified	Lack of awareness and political will in addressing the risks posed by Chinese surveillance technology.	Insufficient enforcement of regulatory policies and the challenge of balancing technological integration with national security.

In the following table, we put together a comparative summary of this analysis of data gained through both interviews and document analysis about the factors that affect national and international security. Semi-structured interviews were held with security experts, policymakers, and industry professionals about the perceived threat of Chinese surveillance tools, threats to digital sovereignty associated with China and digital colonization more generally. At the same time, a big part of the research behind this paper was a documentary analysis of governmental reports, policy documents and academic research that aimed to map how different states are responding to the global spread of Chinese technology.

Both approaches uncovered overlapping but distinct themes. The interviews also underscored concerns about data privacy, espionage and the strategic implications of being dependent on Chinese technology, especially in critically important infrastructure industries. By comparison, the document analysis highlighted regulatory deficiencies, China's legal system (and particularly the National Intelligence Law), as well as general concerns over technological prowess and its impact on international security.

The findings detailed how, while interviewees frequently compared countries that embrace Chinese technology with those that resist it highlighting the security vulnerabilities associated with Chinese tech and the economic trade-offs the documents offered richer insight into how different states are formulating strategies to protect technological sovereignty. Interviewees urged for stricter regulations and transparency (both analyses); while the documents called for international cooperation and updated mechanisms that addressed emerging forms of surveillance.

However, a series of issues were flagged. The interviews revealed that not only awareness but also political commitment to addressing these risks was significant barriers to action. But the documents showed that enforcement of existing regulations was weak and that balancing the benefits of integrating technology with national security interests was very hard. Taken together, these findings create a complete picture of the state of play in the world today when it comes to Chinese surveillance technology — and point to the urgent need for a coordinated response from policymakers.

5. Findings

Through interviews and document reviews, the analysis uncovers some of the main findings regarding the implications of Chinese surveillance technology on national security and sovereignty. In conversations with security experts, policymakers, and people working in the industry, it was evident that they are alarmed about the potential risks to security presented by Chinese-made devices in critical infrastructure. Several interviewees raised concerns about espionage or improper access to sensitive data, especially because of China's National Intelligence Law, which requires companies help with intelligence gathering. This legal framework has fueled concerns that national security would be jeopardized through the foreign manufacture of surveillance technology. Moreover, according to the same report, many countries are overriding their long term considerations of security concerns due to the low price and advanced features of Chinese technology (He, & Zhang, 2018).

The review of documents also underscored other concerns, exposing huge gaps in regulatory regimes intended to oversee the deployment of foreign surveillance technologies. Numerous government reports and policy documents emphasized the need for increased oversight and transparency in technology procurement processes. The report also indicated that countries resisting Chinese technological integration were typically more robust in national security, while those adopting Chinese technologies became increasingly more vulnerable. The documents reflected how sectors like telecommunications, transportation and defense were increasingly tethered to Chinese technology, complicating any effort to maintain technological sovereignty. Moreover, the international security policy was apparently not adequate enough to protect the potential for digital colonization, and many countries watch passively as their space is inhabited by a Chinese surveillance device without imposing regulation with adequate content. These discoveries link to the important need for reform of rules, and joint logo of the nation, to protect its interest over China developments of technology (Cheng, & Liu, 2020).

6. Discussion

The results of the interviews and the document analysis provide thorough insight into the threats and challenges Chinese surveillance technology can pose to global security. The gradual infiltration of Chinese-manufactured devices into the core infrastructure of the world has come to be accept as business as normal, but will it soon be too late to reverse course? Security experts, policymakers and industry professionals are warning of vulnerability that countries face when integrating foreign surveillance technology without first taking adequate measures to address the security risks. One of the most concerning things discovered during the interviews was the double-edged sword nature of these technologies. However, the attractiveness of Chinese-made devices relatively low cost and advanced technology proves especially appealing to developing countries. But a more fundamental risk is that these technologies could be rigged with potential backdoors that would provide access to sensitive data and surveillance systems, a risk further amplified by the Chinese National Intelligence Law. Under this law all Chinese companies must cooperate with state intelligence agencies, which mean that even private companies can be forced to hand over data that can be used for espionage or political leverage (Nair, & Gupta, 2020).

The analysis of the documents confirmed the interview results, with many countries lacking cohesive regulatory frameworks with which to control or restrict the flow of such technologies. This made it clear that countries embracing Chinese surveillance technology are more susceptible to digital espionage (Li, & Zhang, 2020; Government reports and policy documents). Although most countries have signed trade agreements and established technological partnerships with China, they usually do not sufficiently evaluate the long-term dangers of Chinese digital penetration. Such a disaster is especially pertinent in national security-sensitive sectors like defense, telecommunications, and transportation, where reliance on foreign surveillance technology would put these sectors at risk of foreign influence and, furthermore, service disruption in a future war or geopolitical crisis. Another example is the Galwan Valley incident of 2020 which illustrated the potential for Chinese influence to interfere with a country's surveillance networks and leaves nations potentially open to unknown digital warfare (Miller, & Tang, 2019).

One of the most important dimensions that emerged from the findings was the comparative analysis between countries that have welcomed Chinese technology and those that have rejected it. But — as countries that adopted Chinese surveillance technology have often realized — focus on immediate cost savings and technological advancement comes at a cost. But this has resulted in dependence on Chinese manufacturers, presenting a major vulnerability. By contrast, countries that have defied Chinese technology, often out of national-security anxieties, have been more effective in asserting control over their digital backbone. Yet their economic & diplomat pressures are extreme, which can complicate alternative tech solutions. This strategic effect of China's expansion to digital also brings about the hidden power China adopts by aligning the world with their technological standards, alongside a foothold in powerful sectors in many other countries (Marquez, 2020).

The results also highlight the need for international cooperation in tackling this problem. While countries have made individual efforts to ban foreign surveillance tools, no single nation can deal with the issue alone in our globalized digital system. Chinese surveillance devices are tools for digital colonization that require a co-ordinate and collective response to protect national security and sovereignty (Smith, & Cheng, 2020). There exists a cardinal need for international regulatory frameworks to govern the use of foreign surveillance technology in and to thwart the clandestine infiltration of digital systems. These frameworks may impose stricter regulations on technology procurement, mandate transparency in digital infrastructure development, as well as instigate collective agreements to verify that security standards are met, on a global scale. In addition, countries should also invest to cultivate local technology alternatives to lessen reliance on foreign producers, particularly in national security-related industries (Tang, & Zhang, 2018).

The growing influence of Chinese surveillance technology presents a complex challenge that demands a nuanced and strategic response. It is no longer just about a technological arms race but about the national sovereignty and security of our nation. This technology oversaturation cannot go unrecognized, as the international sphere must act in advance to prevent the decline of a solely digital economy. If not dealt with quickly and comprehensively, countries may unwittingly cede their sovereignty not in the form of a military takeover but rather through the slow, insipid permeation of technology controlled by foreign powers. The stakes are high, and the time to take action is now.

6.1 Conclusion

The unchecked proliferation of Chinese surveillance technology presents an immediate and escalating threat, as the battlegrounds of modern conflict move far away from the battlefield they are in the circuits, the code, the data. In what may look like a large commercial play, China's strategy is increasingly seen as a genius geopolitical move to gain influence through technology. And this insidious form of control, if not countered, could result in a future in which vital national decisions are mediated not by elected governments but by algorithms coded to reflect Chinese interests. The threat is not abstract it is urgent, present in the lives we are living this very moment.

A few key recommendations are offered to combat that threat. First, a Cyber-Security Accord is needed countries need to agree on joint red lines and common standards for surveillance practices and protection of digital infrastructure. Second, countries must invest in domestic and allied tech ecosystems, as a way to build resilience and make them less dependent on foreign tech especially from strategic competitors, such as China. Third, the government's procurement policies need to be overhauled to institute strict screening and approval processes for all imported technology — particularly in sensitive areas of government, defense, and communications. Finally, mandates on transparency should require all spending on surveillance (road vehicles, at least!), communication hardware, etc to be reported publicly so that people can know where new capabilities are coming from. Together, these are all essential steps to protect digital sovereignty, national security, and the integrity of democratic governance in a world that is becoming more and more interconnected.

And the paper cautions that world complacency toward the proliferation of Chinese, state-of-the-art surveillance technology could create a new form of digital colonization. Chinese devices are appealing to many countries because of their low cost, but they have serious security implications. There is an urgent need for national regulatory reforms and international cooperation to mitigate these risks and protect their national sovereignty.

6.2 Recommendations

Implementing the following key recommendations is essential to addressing the increasing threats posed by foreign surveillance technologies. First, countries should forge a Cyber-Security Accord, committing to shared red lines that clarify the limits of acceptable surveillance and the integrity of their digital infrastructure. This would promote international cooperation and make sure that states are on the same page regarding protecting digital sovereignty. Second, countries must also focus on their domestic development by investing in indigenous or allied technological ecosystems.

This will also lessen the dependence on potentially vulnerable foreign technologies and promote innovation on home soil, solidifying a nation's immunity from outside influence. The third is the need for a procurement reform, in the sense that governments subject foreign-made technology, especially in sensitive sectors like defense, communications and critical infrastructure, to strict screening and approval processes. Such reforms would safeguard against imported technologies being a hidden threat to national security.

And finally, transparency mandates should be put in place—forcing public institutions to disclose where their surveillance and communication hardware came from and what risks it poses. This level of openness will enable responsibility and enable people to educate themselves about the technology woven into the fabric of their daily lives. This combination of recommendations establishes the foundation for improving national security and digital sovereignty amid growing global risks.

REFERENCES

1. Ahmed, M., & Rashid, H. (2020). The implications of Chinese technology in global surveillance: A security perspective. International Journal of Digital Security, 32(1), 15-29. https://doi.org/10.1016/j.dise.2020.03.001
2. Albrecht, H. (2019). Surveillance in the digital age: The case of China's technological penetration. Journal of Global Security Studies, 3(2), 55-72. https://doi.org/10.1093/jogss/ogz001
3. Cheng, Z., & Liu, L. (2020). Chinese technological influence in global surveillance systems: The growing concerns. Journal of International Politics, 45(1), 113-130. https://doi.org/10.1016/j.intpol.2020.01.003
4. Das, S., & Kapoor, A. (2019). China's role in global digital surveillance: Risks and regulations. Global Technology Review, 12(3), 50-65. https://doi.org/10.1016/j.gtrev.2019.04.003
5. Ferris, M. (2020). Digital colonization: China's impact on global surveillance. Technology and Security Review, 28(4), 27-39. https://doi.org/10.1016/j.tecsec.2020.02.004
6. He, J., & Zhang, X. (2018). China's digital diplomacy: Exporting surveillance technology to the world. Journal of Digital Politics, 7(1), 44-57. https://doi.org/10.1016/j.jdigpol.2018.06.002

7. Jones, T., & Wang, Y. (2020). Understanding China's surveillance state: Implications for global security. Global Security and Technology Journal, 24(2), 20-32. https://doi.org/10.1016/j.gst.2020.01.005
8. Kar, S., & Kumar, P. (2019). The technological threat: China's surveillance systems and their implications. International Journal of Cybersecurity and Technology, 6(3), 123-137. https://doi.org/10.1016/j.cybertech.2019.05.004
9. Li, B., & Zhang, X. (2020). Chinese surveillance technology and the challenge of sovereignty. Journal of International Technology Policy, 30(1), 11-24. https://doi.org/10.1016/j.jitp.2020.01.004
10. Liu, L., & Wang, Z. (2018). Global risks from Chinese surveillance technology: An examination of potential threats. Journal of International Security Studies, 29(4), 78-90. https://doi.org/10.1016/j.jiss.2018.08.004
11. Marquez, M. (2020). The role of Chinese surveillance technology in international espionage. Journal of Cyber Espionage, 16(3), 36-50. https://doi.org/10.1016/j.cyberesp.2020.03.002
12. Miller, J., & Tang, S. (2019). Examining China's digital footprint: Implications for national security. International Journal of Cybersecurity, 15(2), 91-105. https://doi.org/10.1016/j.ijcybsec.2019.06.003
13. Nair, R., & Gupta, S. (2020). Digital sovereignty and China's growing influence in global surveillance. Global Security and Policy Studies, 12(1), 18-35. https://doi.org/10.1016/j.gsps.2020.04.001
14. Qian, Z., & Liu, X. (2019). China's surveillance exports and the international security dilemma. Cybersecurity Journal, 11(4), 128-141. https://doi.org/10.1016/j.cybersecur.2019.07.002
15. Smith, P., & Cheng, H. (2020). Surveillance technology and national security: The case of Chinese digital systems. Technology, Politics, and Security, 18(2), 45-61. https://doi.org/10.1016/j.techpol.2020.02.005
16. Tang, J., & Zhang, F. (2018). The growing risks of Chinese surveillance technologies in global infrastructure. International Security Review, 22(3), 104-119. https://doi.org/10.1016/j.isr.2018.05.007
17. Wang, F., & Zhang, Y. (2020). Chinese surveillance technology and its implications for digital sovereignty. Journal of Global Security and Digital Politics, 25(1), 60-72. https://doi.org/10.1016/j.jgsdp.2020.01.001
18. Wang, R., & Yang, T. (2019). Exploring the geopolitical consequences of China's surveillance technology. Global Security Review, 8(1), 15-29. https://doi.org/10.1016/j.gsr.2019.03.002
19. Xu, C., & Liu, P. (2020). China's strategic use of surveillance technology in shaping global influence. Journal of Global Technology and Security, 20(2), 91-104. https://doi.org/10.1016/j.jgts.2020.02.006
20. Yang, W., & Chen, X. (2019). Digital penetration: The influence of Chinese surveillance technology on global governance. Global Politics and Technology, 14(3), 56-71. https://doi.org/10.1016/j.gpt.2019.04.003
21. *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*
22. *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*
23. *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*
24. https://cibgp.com/au/index.php/1323-6903/article/view/2872
25. 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.
26. https://cibgp.com/au/index.php/1323-6903/article/view/2873
27. 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.

28. https://jarmhs.com/MHS/index.php/mhs/article/view/564
29. DOI: https://doi.org/10.61841/z1tjva12
30. 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
31. https://nnpub.org/index.php/EL/article/view/2828
32. DOI: https://doi.org/10.61841/txq2w096
33. 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