Security Analysis of CCTV Surveillance Infrastructure: Technical and Geopolitical Implications of India's Restrictions on Chinese CCTV Ecosystems

Anmol Bose[1], Anup Singh Kushwaha[2], Meena Chaudhary[3], Ashish Sharma[4]
[1,2,3,4]*Department of Computer Science and Technology, Manav Rachna University*

***Abstract*—In light of the development of networked CCTV surveillance systems, concerns arise regarding cybersecurity risks, digital sovereignty, and geopolitical consequences. In India, prohibitions of Chinese surveillance equipment have prompted debate on such topics as supply chain security, firmware issues, and critical infrastructure vulnerable to attacks. Nevertheless, there is a lack of studies which explore both cybersecurity and geopolitical issues in terms of the restrictions imposed on China without analyzing the connection between those issues. In this regard, a comparative analysis of the cybersecurity and geopolitical impacts of India's restrictions on Chinese surveillance equipment on the basis of scholarly works, CVEs, government documents, policies, and cyber alerts was carried out through thematic comparison. As a result, vulnerabilities in Chinese CCTV systems due to firmware obscurity, poor firmware updating procedures, dependence on cloud service providers, and routing of data flows via channels located outside India were discovered. At the same time, the similar cybersecurity issues were found among non-Chinese surveillance systems because of problems with authentication and update mechanisms, as well as exposed network services. Moreover, certain procurement and cybersecurity policy vulnerabilities were revealed in India. The research referred to CCTV infrastructures as interdependent techno-political infrastructures that are based on cyber security resilience, dependence and sovereignty concerns. It further called for more robust procurement systems, cybersecurity assessments, good handling of firmware and establishment of local surveillance infrastructure.**

***Index Terms*—Cybersecurity governance, CCTV surveillance, firmware security, geopolitical risks, digital sovereignty.**

I. INTRODUCTION

The emergence of digital surveillance technology has turned CCTV cameras into a cyber-physical network with the incorporation of AI, cloud computing, and smart cities. CCTV cameras serve a significant purpose in policing, traffic, and critical infrastructure in the country of India. However, the increasing use of surveillance technology developed by countries abroad, especially those from China, have created issues of cybersecurity, supply chain, and digital sovereignty in India. The companies that dominate the market for surveillance technologies include Hikvision and Dahua because they are relatively cheap and integrate other technologies. Several countries have restricted the use of such surveillance cameras because of concerns about the supply chain and security issues [4], [15].

In theory, surveillance structures need to guarantee cyber-resilience, transparency of governance, and strategic independence. But in reality, the fast proliferation of CCTV cameras in India has focused on deploying them inexpensively at the cost of cyber-resilience. The majority of foreign technologies work on the basis of poorly audited firmware, cloud computing, and external communications architecture [3], [10], [12].

The existing literature is quite disjointed in its approach. On one hand, papers on surveillance capitalism and algorithmic governance examine the relationship between surveillance technologies and state power [2]; on the other hand, studies in cybersecurity focus on the shortcomings associated with inadequate encryption, insecure firmware, and vulnerabilities to cyberattacks via IoT-driven surveillance technologies [3]. There have been other

studies dealing with geopolitics of technology export and digital dependency from China [4]. However, in most cases, these aspects are examined in isolation, resulting in little understanding about the intersection between cybersecurity challenges and geopolitical dependency concerns.

This paper will contribute to the existing knowledge in that regard, conducting a holistic examination of India's CCTV surveillance infrastructure. Specifically, the objective will be to identify cybersecurity weaknesses in CCTV technology, geopolitics behind restricted use of surveillance devices from China, current laws and procurement procedures, as well as develop approaches for resilience, supply chain protection, and digital sovereignty.

The novel contribution of this paper lies in the connection made between the cybersecurity analytical techniques and the geopolitical approach towards surveillance infrastructures. In essence, this paper argues that surveillance security can be approached in two ways; it can either be done from a perspective based on technical aspects, or from perspectives that include governance issues, dependency considerations, and management issues. This paper places emphasis on CCTV surveillance, lack of a multidisciplinary perspective in prior literature, and addresses this problem through a multidisciplinary approach in studying China's CCTV in India.

CCTV Surveillance Ecosystem
↓
Technical Vulnerabilities
(Firmware, RTSP, Cloud Exposure)
↓
Supply-Chain Dependency
↓
Geopolitical Risk
↓
Digital Sovereignty Concerns
↓
Regulatory & Procurement Response
↓
Cybersecurity Resilience

Figure 1. Integrated Framework for CCTV Surveillance Security Analysis

II. LITERATURE REVIEW

The use of CCTV systems has proved essential for smart city applications, IoT technology, and also for a country's national security architecture [8], [3]. Modern-day surveillance cameras include features such as internet connectivity, firmware, remote control ability, and AI-based analysis [8], [10]. Even though all the above features play a pivotal role in improving their efficiency and storage capacity [4], these make them highly vulnerable against cyber threats as well. It was found that several cameras using IP addresses continue to employ protocols of HTTP/RTSP, thereby enabling video theft as well as unauthorized access [10]. More than one million of such surveillance cameras have been found to be exposed, with the lack of use of any HTTPS encryption despite keeping the Telnet and SSH ports open [10].

The analysis of already known weaknesses of the CCTV system usually involves a number of vulnerable categories, including firmware, authentication, default credentials, and open channels [3], [10]. Many researches have revealed numerous security weaknesses for the Hikvision and Dahua cameras. For example, exploitation of the CVE-2017-7921 weakness in the Hikvision firmware has allowed the attacker to fully control the device without any authorization [9]. In addition, a set of vulnerabilities for Dahua ONVIF cameras (CVE-2025-31700/31701) has caused unauthenticated remote code execution through malicious RTSP/ONVIF messages [11]. Moreover, the absence of the automatic firmware update feature results in numerous cases when surveillance cameras are still running on outdated firmware [2][11].

One can also see the problem of insecure implementation at the protocol level. Namely, the combination of insecure configuration settings and non-encrypted RTSP stream increases risks of eavesdropping, injection attacks, and illegal access to the data transmitted [10], [8]. Although HTTPS and DTLS protocols for securing communication between devices have been developed, there are still not many of them employed nowadays.

Another important subject is firmware safety and the security of the supply chain. Researchers have reported critical vulnerabilities and insecure firmware management practices in some Chinese surveillance products[9], [11]. These researchers claim that it is

risky to use insecure firmware management and foreign components to assemble surveillance systems [12], [3]. This problem is directly linked with the previously mentioned problems of digital sovereignty and technological dependence. For instance, new requirements for component traceability and testing processes were recently adopted in India [13], [16].

The modern surveillance systems of a smart city also represent an issue due to the use of the cloud and edge computing technologies as storage facilities and means of video analysis [8], [3]. While cloud-based surveillance improves scalability and enables using artificial intelligence solutions, it brings up the question whether foreign companies would be able to control the video and transport it to their countries [3], [5]. Officials in India are concerned about the potential of Chinese surveillance technologies to send sensitive information abroad [15]. This is why the current regulatory framework in India focuses on firmware management and communication security [16].

Geopolitical aspects of China's surveillance system technology have become more pronounced around the world. In this regard, the US, the UK, and other countries have introduced restrictions for companies such as Hikvision and Dahua because of their role in national security problems [15]. To address cybersecurity problems, India has adopted its "Essential Requirements" and compulsory certification process. It comprises testing and verification of security equipment [16]. Thus, only since April 2026, surveillance systems, which passed STQC/BIS certification and met these requirements, can be sold in India [16]. Therefore, this situation forced India to restrict China's surveillance technologies. Moreover, it facilitated the process of manufacturing of non-Chinese chips in the country [13], [14].

Other aspects that have been covered in the literature include some of the drastic changes that have taken place in the surveillance market in India. The Indian companies such as CP Plus, Prama, Matrix, and Sparsh have grown because there are restrictions on Chinese-based firms [14], [13]. Furthermore, some companies have even resorted to using the Taiwanese chips and locally made firmware because of the certification issue [14]. Additionally, many Indian firms have invested heavily in AI-vision and semiconductor surveillance [17], [18]. However, most of the information is industry-based.

The review of existing literature reveals multiple gaps within the field. While technical literature focuses on such risks as vulnerability of firmware, risks related to protocols and authentication processes [10], [3], policy-oriented literature is primarily engaged with such concepts as digital sovereignty, techno-nationalism, and supply chain dependencies [15], [14]. It is obvious that these matters have a common denominator, which is insufficiently addressed by only a handful of researchers and contributes to the complexities of procuring and geopolitical issues.

To conclude, it should be noted that contemporary literature reveals cyber threats and geopolitical aspects, which pose risks for modern CCTV systems. However, contemporary research addresses these matters separately. The main purpose of this paper is to address this gap and incorporate both elements into a single analysis of the CCTV system in India.

Table 1. Summary of Key Studies on CCTV Cybersecurity and Geopolitical Risks

Author	Focus Area	Key Findings	Research Gap
Sicari et al. (2015)	IoT security	Weak IoT security architecture	No geopolitical analysis
Feldstein (2021)	Digital surveillance	Surveillance as strategic control	Limited technical analysis
Greitens (2020)	Chinese surveillance exports	Strategic dependency concerns	No firmware-level discussion
Bernot et al. (2025)	CCTV vulnerabilities	Firmware vulnerabilities and outdated firmware	Limited India-focused analysis

III. METHODS

Qualitative review-based comparative research design was used as research methodology in the current study to examine the effects of India's ban on Chinese surveillance ecosystem on cybersecurity and geopolitics. The current research relied purely on secondary sources including scholarly journals, cybersecurity reports, vulnerability databases from open source, government alerts, advisories, cyber policy documents, and technical studies in industry about surveillance infrastructure security. The comparative analysis was conducted to evaluate the

vulnerabilities of cybersecurity as well as other strategic concerns associated with the security of surveillance infrastructure in India.

The literature review and data collection process were conducted between January 2025 and March 2026. Networked CCTV systems in smart cities, transportation systems, public surveillance systems, and critical infrastructures in India were taken into account. Specifically, special focus was put on the surveillance infrastructure built by China in India. At the same time, comparative analysis included non-Chinese surveillance infrastructures to find out whether there were cybersecurity vulnerabilities peculiar to China or to all countries.

Sources pertinent to this topic were collected through searches on different databases such as IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar. Also, other sources include cybersecurity consulting services, Common Vulnerabilities and Exposures listing, Indian government bulletins, and a variety of security-related documents. Some of the keywords used in the search process were "CCTV cybersecurity", "IoT Surveillance Security", "Surveillance Infrastructure in China", "Digital Sovereignty", and "Firmware Security".

Some of the main inclusion criteria considered during source selection were related to topics such as CCTV cybersecurity, surveillance governance, supply chain management, IoT firmware, and Indian cybersecurity policy regulations. Peer-reviewed academic papers, government bulletins, and technical publications from 2015 to 2026 have been selected while others are not considered.

Data analysis was done using comparative thematic synthesis as a methodology. The technical literature review consisted of analyzing themes such as the vulnerabilities associated with firmware, lack of proper authentication mechanisms, unencrypted communication protocol, cloud routing, and vulnerable update system in the literature. In contrast, the analysis of the policy literature and geopolitics included the themes of digital sovereignty, technonationalism, surveillance governance, and strategic infrastructure resilience.

A comparative methodology was developed in order to be able to link cybersecurity literature to geopolitics or regulatory literatures. This enabled an assessment of the various CCTV technology systems as technopolitical infrastructures that were exposed to several cyber threats, purchasing policies, and dependencies. Ethical approval was not required as the study used secondary literature only without any human subjects being tested on vulnerabilities or pen-testing.

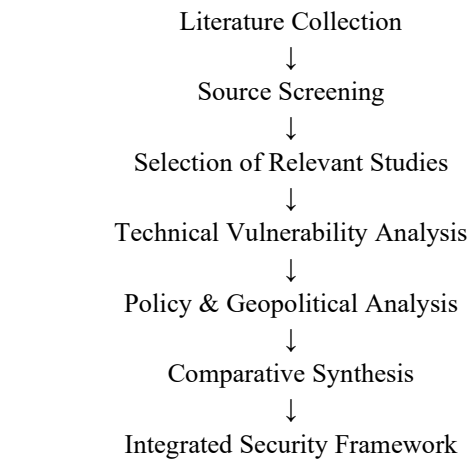

Figure 2. Review-Based Research Methodology Workflow

IV. RESULTS

In view of the literature review, the following types of cybersecurity vulnerabilities have been identified in the IP cameras' systems, particularly those produced in China. These included vulnerabilities in firmware architectures, secure connection and authentication, among others. Some of the cybersecurity vulnerabilities include insecure firmwares, bad authentication, administrative interface, insecure protocols for communication and security issues with remote connections in the CCTV system. It is worth noting that some of the firmwares are outdated in spite of the existence of CVEs.

According to the literature review, IP-based CCTV systems were differentiated according to their origin and found that Chinese origin systems raised more security concerns than non-Chinese ones [9], [11], [15]. It is because the Chinese systems were less open when it came to updating and patching. However, according to the literature review, it appears that other non-Chinese systems were less secure in terms of insecure configuration, exposure to the cloud service, and improper update of firmware.

In addition, insecure communication protocols in the communication infrastructure of CCTV systems were pointed out. For example, use of HTTP and RTSP

protocols is one of such cases. Also, it appeared from the literature that CVEs usually revealed authentication bypass, remote code execution, and insecure ONVIF protocol implementations.

When it comes to the policy analysis, it became apparent that although the use of foreign surveillance equipment had been restricted in India, the surveillance governance framework in India was rather fragmented. This is due to inconsistencies with regard to cybersecurity audit, transparency of firmware updates, and verification of secure procurement. Moreover, import dependencies and exposures related to surveillance systems were among the other problems pointed out in the literature analysis.

It is evident from the market analysis that the banning of the importation of surveillance products from China by India resulted in adopting strategies for manufacturing domestically, using domestically manufactured firmware, and employing different chipsets. However, it is apparent from the analyzed data that while limiting imports might be helpful in dealing with the problem of surveillance-security, better cyber security governance needs to be put into practice.

Table 2. Comparative Cybersecurity Risks in CCTV Ecosystems

Security Dimension	Chinese-Origin Systems	Non-Chinese Systems	Observed Risk Level
Firmware Transparency	Limited	Moderate	High
Cloud Dependency	Frequent	Moderate	High
Encryption Practices	Inconsistent	Better but variable	Medium
Patch Management	Weak in many reports	More structured	Medium
Default Credential Risks	Frequently reported	Occasionally reported	Medium
Regulatory Scrutiny	High	Moderate	High

Source: Compiled from [9], [11], [13], [15], [16]

V. DISCUSSION

The conclusions drawn from the review of the scientific literature proved that the CCTV surveillance infrastructures can be viewed as technopolitical structures and not mere technologies. Problems arising from issues of firmwares' opaqueness, using routing via clouds, employing insecure protocols, and applying external infrastructures pointed at more profound problems linked to notions of digital sovereignty and technological dependencies. The conclusions corresponded with critical infrastructure protection theory; whereby digital system vulnerabilities could give rise to national security threats [19].

An important conclusion was made that problems relating to the insecurity of surveillance infrastructures produced in China did not depend only on geopolitical factors. The technical analysis proved that there were certain vulnerabilities due to such issues as opaqueness of firmwares, insecure software updates, problems of authentication, and cloud services. It helped confirm that earlier research was correct in its findings regarding surveillance technologies' role as instruments of strategic influence and technological dependencies [4],[8].

In contrast, conclusions drawn from the literature review revealed that replacing Chinese vendors by others could not guarantee the security of CCTV cameras. There was an insecure protocol, out-of-date firmware, and poor software update practices discovered in both types of products. Hence, it should be noted that the problem with surveillance-security relates to the globalized nature of IoT infrastructure.

It is important to mention that there were restrictions in governance in the case of India's surveillance-security. In spite of the fact that the recent procurement policy and certification showed increased awareness concerning digital sovereignty, there was huge discrepancy among different surveillance systems in terms of their governance. Several academic studies revealed that the previous procurement policy paid little attention to the cybersecurity aspect and focused on efficiency and rapid implementation [13], [15], [16].

Significance of the study involves the capability of incorporating cybersecurity issues within the context of geopolitics and governance. The use of an analysis framework that considers vulnerabilities in cybersecurity, coupled with supply chain dependency, procurement governance, and digital sovereignty, highlights their combined role in national surveillance resilience.

VI. LIMITATIONS

Secondary sources were employed for collecting information for this research and include research papers related to cybersecurity issues, policies implemented by governments, and vulnerability databases that mentioned potential threats to CCTV systems. No testing processes like firmware extraction and penetration testing had to be conducted since there was no need for testing at all. Some results obtained in the course of this research depend on the reliability of past research; moreover, proprietary environments of firmware and classified procurement databases are not accessible to public access. Technological advancements and new laws on cybersecurity can be viewed as threats to the validity of the research findings in the long run.

VII. CONCLUSION

In this research, the consequences of India's restriction of Chinese CCTV systems concerning cybersecurity and geopolitics were investigated using a comparative review method. According to the findings of the study, the surveillance systems provided by Chinese companies had been frequently associated with problems such as lack of transparency about the firmware, dependence on cloud routing, poor updating methods, and reliance on external networks for communication. However, the findings of the study demonstrated that cybersecurity problems did not only concern Chinese suppliers as other non-Chinese surveillance systems have experienced security concerns, too.

Additionally, the surveillance procurement procedure and regulations used by India turned out to be vulnerable due to auditing and cybersecurity considerations. The implications derived from the study suggest that restricting suppliers cannot ensure the sustainability of the surveillance systems in the absence of appropriate procurement policies, firmware management, and cybersecurity audits.

Nevertheless, the research contributes greatly to the body of knowledge on the subject of cyber governance and digital sovereignty through the inclusion of cybersecurity analysis and the geopolitical dimension of surveillance technology. Although the research is confined by secondary sources only, it demonstrates a more comprehensive approach to the analysis of CCTV technology not only through the prism of technology but also geopolitics. Finally, the research has proved that surveillance technology operates within a context wherein cybersecurity, geopolitical dependence, and digital sovereignty converge.

REFERENCES

[1] S. Feldstein, The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance. Oxford, U.K.: Oxford University Press, 2021.

[2] S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York, NY, USA: PublicAffairs, 2019.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[4] S. C. Greitens, "Dealing with Demand for China's Global Surveillance Exports," Brookings Institution Report, Washington, DC, USA, 2020.

[5] V. Braun and V. Clarke, "Using Thematic Analysis in Psychology," Qualitative Research in Psychology, vol. 3, no. 2, pp. 77–101, 2006.

[6] J. W. Creswell and V. L. Plano Clark, Designing and Conducting Mixed Methods Research, 3rd ed. Thousand Oaks, CA, USA: Sage Publications, 2018.

[7] R. K. Yin, Case Study Research and Applications: Design and Methods, 6th ed. Thousand Oaks, CA, USA: Sage Publications, 2018.

[8] MP-IDSA, "The Weaponisation of Surveillance Infrastructure." [Online]. Available: https://idsa.in/publisher/issuebrief/the-weaponisation-of-surveillance-infrastructure

[9] Cyber Unit, "Your Security Cameras May Be Your Biggest Security Risk." [Online]. Available: https://cyberunit.com/insights/hikvision-iot-security-cameras-business-risk/

[10] "Large-Scale Analysis of the Security of Embedded Firmware," arXiv. [Online]. Available: https://arxiv.org/pdf/1910.10749

[11] The Hacker News, "Critical Dahua Camera Flaws Enable Remote Hijack via ONVIF and

File Upload Exploits," 2025. [Online]. Available: https://thehackernews.com/2025/07/critical-dahua-camera-flaws-enable.html

[12] Oxford Academic, "Cybersecurity Risks in Smart Surveillance Systems." [Online]. Available: https://oup.silverchair-cdn.com/article-minimal/8345066

[13] Mint, "India to Ban Sales of Chinese CCTV Brands Hikvision and Dahua from 1 April." [Online]. Available: https://www.livemint.com/technology/tech-news/india-to-ban-sales-of-chinese-cctv-brands-hikvision-tp-link-and-dahua-from-1-april-report-11774863069285.html

[14] ET BrandEquity, "Market Reset: India Pulls the Plug on Chinese CCTV Makers." [Online]. Available: https://brandequity.economictimes.indiatimes.com/news/marketing/market-reset-india-pulls-the-plug-on-chinese-cctv-makers/129890645

[15] India Today, "Why India Is Banning Hikvision, Dahua, TP-Link CCTV Cameras," Apr. 2026. [Online]. Available: https://www.indiatoday.in/technology/news/story/why-india-is-banning-hikvision-dahua-tp-link-cctv-cameras-from-today-all-you-need-to-know-2889858-2026-04-01

[16] Matrix Comsec, "STQC Certification & ER Compliance Mandate for CCTV Cameras." [Online]. Available: https://www.matrixcomsec.com/stqc-certification-er-compliance-for-cctv-cameras/

[17] Honeywell, "Honeywell Launches Its First-Ever CCTV Camera Portfolio Made in India," 2025. [Online]. Available: https://www.honeywell.com/in/en/press/2025/06/honeywell-launches-its-first-ever-cctv-camera-portfolio-made-in-india

[18] The Economic Times, "BigEndian Semiconductors Bags $6 Million Funding to Scale Indigenous VisionAI Chips," 2025. [Online]. Available: https://economictimes.indiatimes.com/tech/funding/bigendian-semiconductors-bags-6-million-funding-to-scale-indigenous-visionai-chips/articleshow/130842533.cms

[19] J. A. Lewis, Cybersecurity and Critical Infrastructure Protection. Washington, DC, USA: Center for Strategic and International Studies (CSIS), 2019.