MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

The Weaponisation of Surveillance Infrastructure

Rohit Kumar Sharma

May 05, 2026

Summary

Cyber operations targeting cameras require relatively limited technical sophistication but offer significant intelligence gains once access to the device is obtained. Over the years, the Indian government has taken various measures to address concerns about imported CCTV surveillance systems. It is equally essential to ensure strong cyber hygiene practices.

Closed-Circuit Television (CCTV) cameras, once benign equipment used for workplace monitoring or crime prevention, have evolved into critical assets for national security and data sovereignty. Advancements in technology over the years have led to the proliferation of Internet of Things (IoT)-enabled cameras with embedded firmware, providing internet connectivity and cloud integration for remote access and control.

There are numerous advantages of using IoT cameras, including ease of access. Security exposure in such devices, due to a large attack surface and other factors, enables malicious actors to exploit them for nefarious objectives. Multiple cases have emerged in the recent past illustrating how these devices, once compromised, can become a strategic liability, particularly during an armed conflict.[1] In fact, compromised traffic cameras in Tehran were used to build a 'pattern of life' of senior Iranian leadership, which was later utilised for targeted strikes against them.[2]

Clearly, the trend of weaponising cameras is not going to stop, especially as technology evolves to integrate AI in this equipment. The brief assesses vulnerabilities in these systems, the potential consequences of these gaps, and the strategic consequences of failing to secure this equipment.

Increasing Attack Surface

Over the years, there has been a notable shift in consumers opting for IoT cameras over analog cameras. The shift illustrates consumers choosing internet-connected cameras for reasons ranging from better-quality video and cloud storage to remote-viewing and AI-based analytics.[3] However, these features also introduce vulnerabilities with significant consequences, as with any device connected to the internet. To understand the vulnerabilities (Table 1) that contribute to an expanding attack surface, it is essential first to examine the network environment that underpins IoT cameras.

The operation of an IoT camera involves several stages. The camera utilises image sensors to capture pictures, which are then stored in the memory module. The communication interface facilitates image transfer to other devices, while the

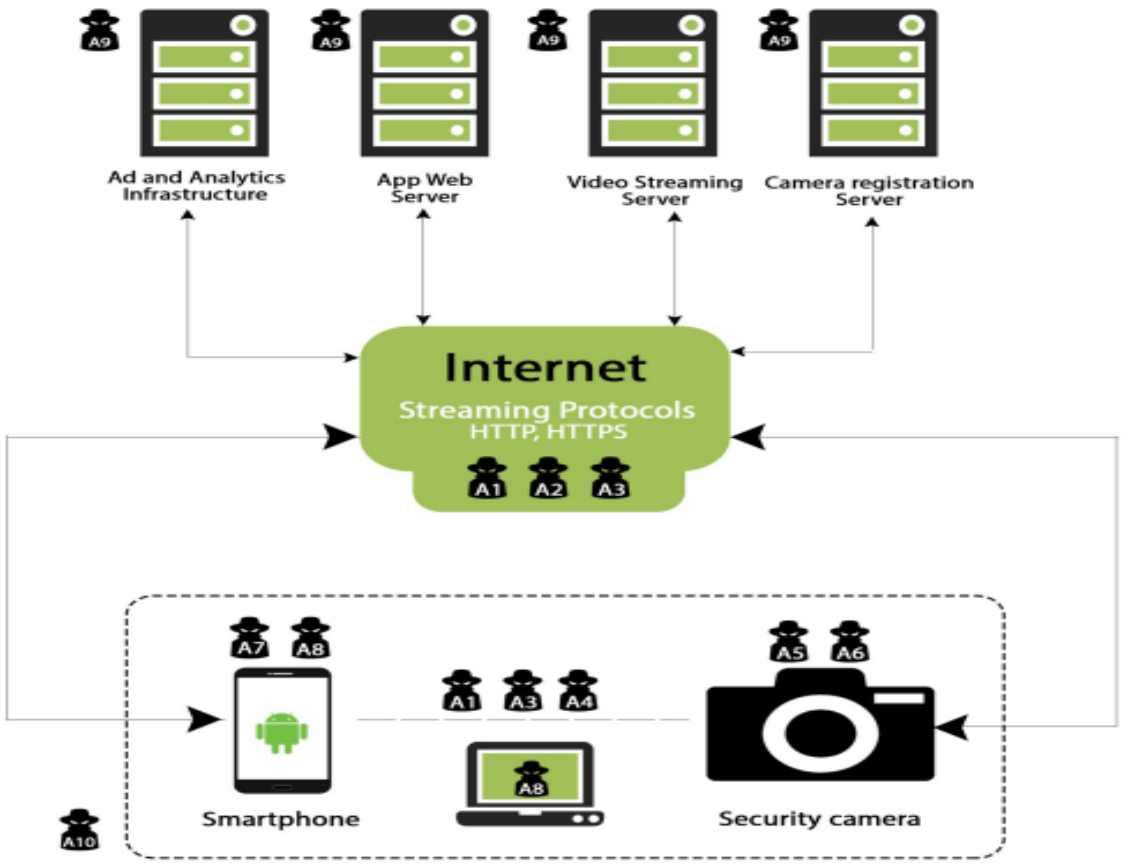
[1] Mehul Srivastava, James Shotter and Neri Zilber, **"Inside the Plan to Kill Ali Khamenei"**, *Financial Times*, 2 March 2026.

[2] Ibid.

[3] Jeremy White, **"What's the Difference Between IP vs. Analog CCTV Cameras?"**, Pro-vigil, 3 September 2025.

processor controls the camera's overall functionality.[4] However, it is not just the camera, but also other components that make up the environment. Figure 1 depicts the complex, interlinked environment of an IoT camera system: the camera, a smartphone with a camera-associated application installed, the camera's web interface, and the servers that enable communication within the system.[5] More nodes in a network increase vulnerability by expanding the attack surface and creating more potential entry points for threat actors.

Figure 1. The Smart Camera Environment



Source: Alharbi and Aspinall (2018)

Through these devices, threat actors aim to target video streams and personally identifiable information (PII) and gain authorised access to the camera itself, the primary physical asset. Once compromised, these cameras can be misused by actors for varying purposes. An attacker, by deploying various tools and techniques, can

[4] **"NCCS/ITSAR/Access Equipment/IoT End Devices/Smart Camera-V1.0.0"**, Ministry of Communications, Government of India, 21 April 2025.

[5] Rana Alharbi and David Aspinall, **"An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities"**, University of Edinburgh Research Explorer, 2018.

get unauthorised access to the network, where they can monitor and retrieve the unencrypted traffic.[6] Man-in-the-middle (MITM) is one such scenario where an attacker intercepts and potentially alters communication. Malware designed to target smart camera applications on mobile devices or access data stored in phone logs can also facilitate broader network compromise. Other attack vectors include Wi-Fi sniffing, in which an attacker obtains router credentials and gains access as a trusted network component.

Past incidents have shown that attackers can exploit tools such as search engines to identify and scan vulnerable networks and IoT devices, including cameras. The Shodan search engine is one such example. It uses a variety of filters to locate devices such as computers, routers and servers that are connected to the internet.[7] Conceived as a powerful tool for security professionals to identify vulnerable devices, Shodan has also gained infamy as the 'Google for hackers'.[8] It is infamous for being instrumental in black-hat hacking and for identifying IP addresses and, upon connection, collecting and recording their metadata.[9] This can lead threat actors to exposed devices, including cameras with no authentication and unpatched vulnerabilities. However, the existence of such tools is not inherently problematic; rather, it challenges the notion of 'security through obscurity' and reinforces the need for robust, proactive security measures.[10]

In the evolving threat landscape of IoT cameras, threat actors have increasingly recognised the potential of compromised devices. While attacks on these systems are not always momentous, some breaches can have strategic consequences, particularly in the context of armed conflicts between states.

Table 1. Categorisation of CCTV Vulnerabilities*

Vulnerability Type	Examples	Impact
Authentication & Access	Default credentials, lack of Multi-factor authentication (MFA), weak password enforcement	Enables easy, large-scale unauthorised access

[6] Ibid.

[7] **"Check Point Threat Alert: Shodan"**, Check Point Research Team, 4 January 2016.

[8] Ibid.

[9] Robert O' Harrow Jr., **"Cyber Search Engine Shodan Exposes Industrial Control Systems to New Risks"**, *The Washington Post*, 3 June 2012.

[10] **"Shodan: The Search Engine For Hackers"**, bugcrowd, 18 March 2026.

Software & Firmware	Unpatched CVEs, lack of signed firmware	Provides a path for remote code execution (RCE)
Network Protocol	Unencrypted RTSP/HTTP	Facilitates data interception and man-in-the-middle (MITM) attacks
Hardware & Supply Chain	Hidden backdoors, compromised third-party libraries	Introduces persistent, hard-to-detect threats embedded at source

Source: Prepared by the author; * The list is not exhaustive

Strategic Consequences

In recent years, multiple incidents have highlighted how compromised cameras are being used for purposes ranging from sustained reconnaissance of political and military leadership to monitoring troop movements and strategic assets. In fact, cyber operations targeting cameras have become a standard tactic, as they require relatively limited technical sophistication while offering significant intelligence gains once access to the device is achieved. This is true in both peacetime and wartime contexts, as the table illustrates, where the strategic utility of compromising cameras ranges from conducting psychological operations and espionage to carrying out battle damage assessments following strikes during armed conflict.

Compromised street cameras in Tehran that enabled the military strikes against the Iranian supreme leader underline how such systems are used in wartime.[11] Advances in AI now enable agencies to process a vast cache of surveillance data, significantly improving target identification. This trend is not limited to Iran, as Iranian-affiliated groups have reportedly hacked parking and roadside cameras to track the movements of Israeli VIPs. In one instance, from the 2025 12-day war, before Iran's ballistic missile strike on the Weizmann Institute of Science, attackers had gained access to street cameras facing the facility, using them to monitor the target shortly before the strike.[12]

[11] Dake King and Sam Mednick, **"Iran Built a Vast Camera Network to Control Dissent. Israel Used It to Track Targets, AP Sources Say"**, *PBS News*, 23 March 2026.

[12] Yonah Jeremy Bob, **"Iran Has Attacked Every Israeli Citizen Multiple Times, New Cyber Chief Yossi Karadi Says"**, *The Jerusalem Post*, 9 December 2025.

Assessments by threat intelligence firms have repeatedly highlighted the Iranian strategy of leveraging hacked cameras for operational support and as a key component of ongoing battle damage assessments.[13] Moreover, as observed, the targeting of internet-connected cameras often aligns closely with geopolitical developments, including visits by American political and military leadership to West Asia.[14]

Similar activities targeting cameras have also been reported in the context of the Russia–Ukraine war (see Table 2). In the case of India, it was recently reported that Pakistan has been engaged in an espionage operation against India using Chinese-made CCTV systems.[15] The cameras were reportedly positioned near strategic Indian assets in border areas, which were being used by threat actors to monitor military and logistics movement.[16] These solar-powered CCTV cameras rely on 4G SIM cards for internet connectivity, with their data routed through servers based in China, making live feed accessible there.[17] The live footage was then relayed to Pakistan-based actors for potential use in an armed conflict scenario.

This is not the first time that Chinese-made surveillance equipment has been at the centre of espionage allegations. Similar issues concerning vulnerabilities that allowed videos to be transferred to servers in China were also raised in 2021.[18] It was also revealed that, according to estimates, around 1 million Chinese-made CCTV cameras were installed in government institutions alone, an alarming figure that raises serious questions about India's cybersecurity posture in relation to cyber threats from China.[19] Reports also suggest Chinese espionage activities in 2021 that leveraged compromised cameras to gather intelligence against India's power infrastructure.[20]

It is important to note that while CCTV cameras are not the only devices that can provide an initial access point for hackers in larger operations, they are particularly valuable for conducting reconnaissance and espionage activities. Through a CCTV

[13] **"Interplay between Iranian Targeting of IP Cameras and Physical Warfare in the Middle East"**, Check Point Research, 4 March 2026.

[14] Ibid.

[15] Dalip Singh, **"Pakistan Used Chinese CCTV Networks to Access Indian Assets for Potential Strikes"**, *The Hindu Business Line*, 12 April 2026.

[16] Ibid.

[17] Samridhi Tewari, **"ISI's Evil Eye? Spy Ring Bust in Delhi Points to China-made Solar CCTVs 'Sending Live Feed to Pakistan'"**, *The Print*, 23 April 2026.

[18] **"Lok Sabha Unstarred Question No. 3594"**, Ministry of Electronics and Information Technology (MeitY), Government of India, 17 March 2021.

[19] Ibid.

[20] Pradip R. Sagar, **"The War on Snooping Eyes | India's CCTV Security Crisis"**, *India Today*, 24 April 2026.

camera, a threat actor can access real-time video and audio feeds. As recent conflicts have demonstrated, these devices are no longer merely passive monitoring tools but can serve as active enablers in kinetic operations. It also illustrates a classic case of integrating physical surveillance tools with cyber tactics and AI to exfiltrate data from sensitive locations.

There have also been instances of cybercriminals selling hacked CCTV footage from hospitals, schools, and even private homes across India.[21] Compromised footage, including live feeds, is also circulated and sold on Telegram channels, often through paid subscriptions.[22]

Table 2. Weaponisation of Cameras and Strategic Utility

Context	Incident	Strategic utility	Targeted Infrastructure
Peace/Grey Zone	A DDoS attack by the Mirai botnet that used compromised IoT devices, including cameras[23]	Infrastructure weaponisation	Consumer IoT devices
Peace/Grey Zone	Evin prison data leak (2021)[24]	Psychological operations: exposing internal facility footage to undermine state legitimacy.	Institutional security
Peace/Grey Zone	Verkada System Breach (2021)	Vulnerability demonstration	Cloud management platform[25]
Grey Zone/Peace time	Over 5,000 cameras around Tehran were	Minor incident with no strategic outcomes.	Municipality CCTVs

[21] **"Mass CCTV Hack in India Exposes Maternity Ward Videos Sold on Telegram"**, *digwatch*, 18 November 2025.

[22] **"Indian Hackers Steal CCTV Footage from Maternity Ward, Sell It on Telegram"**, *ynet*, 17 November 2025.

[23] **"Inside the Infamous Mirai IoT Botnet: A Retrospective Analysis"**, Cloudflare, 14 December 2017.

[24] **"Iran Prisons Chief Apologises Over Leaked Videos of Evin Abuse"**, *BBC*, 24 August 2021.

[25] Chaim Gartenberg, **"Security Startup Verkada Hack Exposes 150,000 Security Cameras in Tesla Factories, Jails, and more"**, *The Verge*, 10 March 2021.

	hacked and deactivated.[26]		
Armed Conflict	Multiple cases in the Russia–Ukraine war[27]	Positioning and conditioning activity through compromised surveillance cameras for potential strikes. Strikes are then followed by battle damage assessments and/or target correction efforts.	CCTVs in residential buildings
Armed Conflict	Multiple cases in West Asia, particularly in Israel and Iran	Espionage and surveillance on political and military leaders[28] Battle damage assessments after strikes[29]	CCTVs in non-military areas
Grey Zone/Peace time	Reports emerging on Pakistan's surveillance using Chinese-made CCTVs.[30]	Espionage on strategic Indian assets in border states	CCTVs near sensitive defence establishments

Source: Prepared by the author based on media reports.

[26] **"Tehran's 5,000 Surveillance Cameras, 150 Sites Hacked"**, *Iran International*, 2 June 2022; **"Iran Exiles Claim Disrupting Tehran's Surveillance Cameras"**, *Arab News*, 3 June 2022.

[27] Silviu Stahie, **"Pro-Ukraine Hackers Take Over Surveillance Cameras in Russia and Transmit Zelensky's Speech"**, *Bitdefender*, 12 May 2023; Silviu Stahie, **"Ukrainian Authorities Shut Down a Couple of Residential Cameras Used to Coordinate the January 2 Attack on Capital"**, *Bitdefender*, 4 January 2024; Daryna Antoniuk, **"Ukraine Says Russia Hacked Web Cameras to Spy on Targets in Kyiv"**, *The Record*, 3 January 2024.

[28] Yonah Jeremy Bob, **"Iran Has Attacked Every Israeli Citizen Multiple Times, New Cyber Chief Yossi Karadi Says"**, *The Jerusalem Post*, 9 December 2025; Mehul Srivastava, James Shotter and Neri Zilber, **"Inside the Plan to Kill Ali Khamenei"**, *Financial Times*, 2 March 2026.

[29] **"Interplay between Iranian Targeting of IP Cameras and Physical Warfare in the Middle East"**, Check Point Research, 4 March 2026.

[30] Dalip Singh, **"Pakistan Used Chinese CCTV Networks to Access Indian Assets for Potential Strikes"**, no. 15.

Indian Government's Response

Over the years, the Indian government has taken various measures to address concerns about imported CCTV surveillance systems. In 2017, CCTV cameras/recorders were included in the list of products under the Bureau of Indian Standards (BIS) Compulsory Registration Scheme (CRS). Following this, every manufacturer of CCTV cameras was required to apply for registration with BIS after recognised labs tested their products.[31]

To restrict the import and sale of sub-standard electronic goods, the Indian government has also notified mandatory Essential Requirements for CCTVs in India.[32] These requirements essentially focus on all the layers that constitute a CCTV network: physical, access, network and software. Under the provisions, it is obligatory to document the origin of the critical components, like System-on-Chip or SoC,[33] a critical step to uncover and control the source of the 'intelligence-bearing layers'.[34] Devices also need to undergo testing against vulnerabilities at accredited labs. The key areas of testing would include: device communication protocols, network services, security of the firmware update process, data storage and encryption, among others.[35]

The essential requirements also seek to encourage the use of tamper-resistant camera enclosures to deter physical tampering.[36] Furthermore, the requirements emphasise role-based access to the network, ensure encrypted data transmission, and enforce strong password policies to support the overall security of the CCTV system. As part of a broader strategy to complement the 'Make in India' initiative and secure CCTV systems against potential adversaries, the government, through a March 2024 notification, has directed procuring entities to prioritise locally manufactured video surveillance systems.[37]

---

[31] **"What is Compulsory Registration Scheme (CRS)"**, Bureau of Indian Standards (BIS), Government of India.

[32] **"Government Has Strengthened the Legal Framework Pertaining to Network Security and Data Protection"**, Press Information Bureau, Ministry of Electronics & IT, Government of India, 25 March 2026.

[33] Ibid.

[34] Pradip R. Sagar, **"The War on Snooping Eyes | India's CCTV Security Crisis"**, *India Today*, 24 April 2026.

[35] **"Subject: Amendment to the "Electronics and Information Technology Goods (Requirement of Compulsory Registration) Order, 2021"**, Ministry of Electronics & IT, Government of India, 9 April 2024.

[36] Ibid.

[37] **"Centre Tightens Security Norms for CCTV Systems to Prevent Remote Unauthorised Access: Jitin Prasada"**, *ET Telecom*, 26 March 2026.

Manufacturers are also required to have their products tested by the Standardisation Testing and Quality Certification (STQC) Directorate and to secure registration from the BIS. The STQC confirms that the device complies with the government-notified essential requirements. It is also the manufacturer's obligation to communicate to the certifying body any minor or major changes post certification to ensure the continuity of the certificate.

All these government measures mean that the CCTVs are no longer operating in a loosely regulated environment; in fact, they are now part of a regulated product category which requires compulsory registration.[38] In response to regulatory measures and growing concerns over Chinese-made cameras, the Delhi government has also announced plans to phase them out for national security reasons.[39]

Conclusion

The usage of internet-connected CCTV cameras is inevitably going to rise, and so are the opportunities for threat actors to gain unauthorised access to these networks. As discussed above, if left unsecured and without adequate measures, compromised systems can be exploited for a range of malicious purposes: from disruptive activities such as DDoS attacks to more strategic uses by actors in both peacetime and wartime.

With the rise in such incidents and the government stepping up regulatory measures, there is a growing view among experts that CCTV systems in sensitive sectors should be treated as strategic infrastructure. While government measures, such as prioritising locally manufactured CCTV cameras to reduce reliance on Chinese equipment, are important, it is equally necessary to address vulnerabilities at the human layer, as without strong cyber hygiene practices, these efforts are unlikely to yield the desired outcomes.

[38] **"STQC Certification and ER Compliance for CCTV Cameras: The Mandate, the Deadline, and Why It Now Matters"**, Matrix Comsec.

[39] Abhinav Rajput, **"51% of CCTVs China-made, Delhi Plans Phased Removal Over Security Concerns"**, *The Times of India*, 2 April 2026.

About the Author

Mr. Rohit Kumar Sharma is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses