ARMIS LABS

WHITE PAPER

Securing Critical Infrastructure: Addressing Espionage Threats from Chinese Surveillance Cameras

By Andrew Grealy, Head of Armis Labs

Executive Summary

The Department of Homeland Security (DHS) recently issued a bulletin warning that Chinese-made internet-connected video surveillance cameras pose a serious espionage and sabotage threat to U.S. critical infrastructure. These cameras, often found in sectors like energy and chemicals, frequently lack robust security (such as data encryption) and, by default, communicate with servers run by their manufacturers in China. The DHS assessment – echoed by cybersecurity experts – is that China's Ministry of State Security (MSS) could exploit such devices to conduct espionage or even disrupt industrial systems on American soil. U.S. authorities have responded with regulations banning or restricting Chinese-made cameras in federal networks. Still, many devices remain in use, including under third-party brands that obscure their Chinese origin.

This report reviews the identified camera brands and models of concern, outlines relevant U.S. government policies addressing the threat, and provides an overview of Armis Centrix™, the Armis Cyber Exposure Management Platform and its capabilities in monitoring, detecting, and mitigating risks from these cameras. We then detail mitigation strategies for organizations, starting with basic protective measures (like not exposing cameras directly to the internet), and outline how Armis can be leveraged to continuously monitor and secure these devices. **In summary, Chinese-manufactured cameras present a clear cybersecurity risk,** but with a combination of prudent network controls and advanced asset intelligence from Armis, the threat can be significantly reduced.

Background

It is important to understand PRC Law to understand how far-reaching the MSS capability is.

China's National Intelligence Law of 2017 creates a legal framework that forces all companies and organizations operating in China—even private tech firms—to cooperate with the government's intelligence services. Here's what that means:

1. Mandatory Cooperation:

- Every Chinese company must help the government's intelligence work.
- This includes providing any data they collect, whether it's gathered in China or abroad.

2. Secrecy Requirement:

> Article 7 of the law requires that companies and individuals keep any details about government intelligence work secret, ensuring that sensitive information doesn't leak to the public.

3. Reporting Vulnerabilities:

> An additional law requires that any security weaknesses (or vulnerabilities) discovered in technology must be reported to the government.

> This means that if a Chinese tech firm finds a flaw in its system, it must notify the authorities.

4. Implications for Technology:

> Because all Chinese technology is subject to these laws, the Chinese government has the legal right to access and potentially exploit any data or security flaws in technology products made in China.

Implications for the U.S.:

Data Security Risks:

If U.S. companies use technology developed by Chinese firms or if U.S. data flows through Chinese networks, there is a risk that this information could be handed over to the Chinese government, potentially compromising sensitive or proprietary information.

Potential for Exploitation:

The government's access to security vulnerabilities means that Chinese intelligence (through agencies like the Ministry of State Security) could exploit these weaknesses. This raises concerns about the integrity and security of products used by U.S. businesses or government agencies.

Broader National Security Concerns:

There is an underlying risk that Chinese technology could be used to undermine U.S. interests, whether through espionage, cyber-attacks, or other means of intelligence gathering.

In short, the law gives the **Chinese government a legal pathway to access and potentially exploit technology and data produced by Chinese companies,** which poses serious security and privacy challenges for the US.

Threat Overview: Exploitation of Chinese Video Cameras in Critical Infrastructure

Nation-State Cyber Threat via IoT Cameras: Internet-connected cameras made by Chinese manufacturers have been identified as potential tools for espionage and disruption. According to a DHS bulletin obtained by the media, these devices could allow the Chinese government to "conduct espionage or disrupt U.S. critical infrastructure" if exploited. Intelligence reporting notes that tens of thousands of such cameras are deployed across U.S. critical infrastructure networks – including in the chemical and energy sectors – often installed with default configurations that lack encryption and basic security hardening. Because many of these cameras automatically communicate with their manufacturers' servers, a compromised camera could feed sensitive video/data back to China or receive malicious commands from state-sponsored actors without the owner's knowledge.

Attack Scenarios: Chinese MSS-affiliated hackers have a track record of targeting vulnerable IP cameras. In prior incidents, cyber operatives gained unauthorized access through camera vulnerabilities. Then, they pivoted deeper into victim networks. For example, an attacker who takes over an IP camera on an enterprise IT network could use that foothold for initial access, then move laterally to other systems to exfiltrate sensitive data or plan further attacks. Even more alarming, if cameras are connected to safety or industrial control systems, an attacker could manipulate them to suppress or trigger false alarms and potentially disable fail-safe mechanisms, hampering an organization's ability to respond to real emergencies. These scenarios illustrate how a seemingly innocuous security camera can become an entry point for sabotage of industrial processes or espionage on confidential activities.

Vulnerable Brands and Models: Several Chinese camera manufacturers have been specifically linked to security concerns:

> **Hangzhou Hikvision Digital Technology (Hikvision):** One of the world's largest CCTV camera producers (42% owned by the Chinese government), Hikvision cameras have been implicated in multiple security issues. U.S. authorities have banned Hikvision products from being used by the government due to espionage fears. Technical analyses have revealed serious firmware vulnerabilities – for instance, an improper authentication flaw (CVE-2017-7921) in many Hikvision models (e.g., DS-2CD and DS-2DF series IP cameras) that allows attackers to bypass login controls (). As of late 2024, Hikvision had not fully remediated this issue in all affected models (), leaving many devices exploitable if not manually patched. These weaknesses could enable remote takeover of Hikvision cameras for spying or network intrusion.

Zhejiang Dahua Technology (Dahua): Another major PRC-based surveillance camera provider banned in U.S. federal systems, Dahua has faced revelations of backdoors and hardcoded credentials in its devices. In 2017, for example, Dahua IP cameras and DVRs (models IPC-HDW, IPC-HFW, and others) were found to contain vulnerabilities that allowed unauthorized retrieval of user passwords and complete admin access. An attacker exploiting these flaws could intercept video feeds or repurpose the device as a jumping-off point into the network. Dahua released firmware fixes, but any unpatched units remain at risk.

Other Chinese OEM Brands (and "White Label" rebrands): Beyond the two largest vendors above, other Chinese firms like Huawei and ZTE (more known for telecommunications gear) and Hytera (radio systems, including some surveillance products) have been flagged by U.S. agencies for security risks (). In the video surveillance market, Chinese manufacturers often sell their hardware through OEM or rebranding agreements, known as "white labeling." This means a camera might carry an American or third-party brand name while a banned Chinese company makes the underlying hardware and software. The DHS bulletin notes that Beijing has leveraged white-labeling to evade U.S. restrictions, importing cameras that are repackaged under different brands to mask their origin. Examples in recent years include brands like Lorex (a retail camera brand formerly owned by Dahua) and equipment sold by resellers that source from Hikvision/Dahua. Buyers may be unaware that such products are Chinese-made. This complicates the threat landscape – many organizations might unknowingly have high-risk cameras on their networks. In summary, Hikvision and Dahua (and their numerous subsidiaries or OEM partners) represent the primary concern, with multiple camera models across their product lines known to have serious vulnerabilities or built-in communications that China's MSS could exploit.

U.S. Government Regulations and Policies Addressing the Threat

U.S. authorities have recognized the risk posed by Chinese-made surveillance equipment and taken steps to limit their deployment, especially in government and critical networks. Key regulations and policies include:

Federal Acquisition Bans (NDAA §889): The John S. McCain National Defense Authorization Act for FY2019, Section 889, prohibits federal agencies (and contractors) from procuring or using telecommunications or video surveillance equipment from certain Chinese companies. Specifically, federal entities may not buy from or even do business with vendors that use equipment by Huawei, ZTE, Hytera, Hikvision, or Dahua (including any subsidiaries or affiliates). This ban, implemented via Federal Acquisition Regulation (FAR) rules in 2019-2020, effectively blacklists Hikvision and Dahua cameras (among others) from U.S. government contracts due to national security concerns. Contractors must report and remove any such equipment if found in their systems. This was a direct response to warnings that these devices could be used for espionage.

Zhejiang Dahua Technology (Dahua): Another major PRC-based surveillance camera provider banned in U.S. federal systems, Dahua has faced revelations of backdoors and hardcoded credentials in its devices. In 2017, for example, Dahua IP cameras and DVRs (models IPC-HDW, IPC-HFW, and others) were found to contain vulnerabilities that allowed unauthorized retrieval of user passwords and complete admin access. An attacker exploiting these flaws could intercept video feeds or repurpose the device as a jumping-off point into the network. Dahua released firmware fixes, but any unpatched units remain at risk.

FCC "Covered List" and Import/Sales Ban: The Federal Communications Commission maintains a "Covered List" of communications equipment deemed a threat to national security under the Secure and Trusted Communications Networks Act of 2019. In November 2022, the FCC adopted new rules banning the authorization (importation or sale) of covered equipment in the U.S. market () (). Notably, the FCC's Covered List explicitly includes video surveillance and communications gear from Huawei, ZTE, Hytera, Hikvision, and Dahua (). As a result, these companies can no longer receive approval for new FCC equipment, preventing most of their new products from being legally sold in the United States. This was the first time the U.S. government blocked commercial sales of electronics on national security grounds, signaling the seriousness of the threat. (Existing installed devices are not automatically removed by this rule, however.)

Other Policies and Guidance: U.S. agencies have also issued less formal guidance to address this risk. For example, the Cybersecurity and Infrastructure Security Agency (CISA) regularly publishes advisories on vulnerabilities in IoT and industrial devices (including cameras), urging operators to apply patches or remove risky devices. In October 2022, CISA, NSA, and FBI jointly highlighted a critical Hikvision camera vulnerability (CVE-2021-36260) as one of the top exploits used by Chinese state hackers. This kind of guidance reinforces policy by alerting the private sector and state/local entities to the need for vigilance with Chinese-made equipment. Additionally, some state governments and U.S. allies have imposed their own bans on Chinese surveillance cameras in government facilities (for instance, the U.K. and Australia moved to bar Hikvision/Dahua on official sites). While not uniform, the trend in policy is clear: Chinese camera technology is treated as a high-risk supply chain element, and organizations are expected to identify and mitigate or eliminate its presence to protect national security.

Despite these measures, enforcement is an ongoing challenge. Many critical infrastructure sites are owned by private companies or local agencies not strictly bound by federal procurement rules. The DHS bulletin observed that Chinese firms had used loopholes like rebranding to **avoid detection by regulators.** Thus, even with strong policies on paper, the onus is on individual organizations to proactively find and secure (or replace) any cameras of Chinese origin in their environments.

Preventing Video Surveillance Compromise

Organizations should implement a multi-layered mitigation strategy to protect critical infrastructure and enterprise networks from the threats associated with Chinese-made (or otherwise vulnerable) cameras. Below are detailed recommendations, starting with basic security hygiene and progressing to advanced monitoring measures.

1. Restrict Exposure and Network Access:

Do not expose security cameras directly to the public internet. One of the top recommendations from both government and industry experts is to minimize network exposure for all cameras and ensure they are not accessible from external networks (). Place cameras behind firewalls and segmented networks – ideally on a separate VLAN or subnet isolated from critical business or control system networks. This way, the attacker cannot directly reach sensitive systems even if a camera is compromised. Disable any peer-to-peer cloud connectivity on the camera if it's not explicitly required, or use VPN access for remote viewing instead of open ports. Treat cameras as untrusted devices: give them only the minimum network access they require (e.g., to a central video management system) and block all other outbound communications. This containment strategy prevents an outside adversary from reaching the cameras and equally prevents a compromised camera from reaching out to the internet or moving laterally into secure zones.

2. Change Default Credentials and Hardening:

Immediately change all default passwords on cameras during installation. Many IP cameras come with factory-default login credentials (often publicly documented) that are trivial for attackers to guess. Use strong, unique passwords for each device, and disable or rename default admin accounts. Additionally, where supported, features like two-factor authentication or certificate-based authentication for camera access are enabled. It is also prudent to disable any unused services or open ports on the cameras (for example, telnet or HTTP if not needed) and enforce encryption for video feeds and management sessions (use HTTPS or SSH). These hardening steps reduce the "low-hanging fruit" opportunities for adversaries. Both DHS and FBI warnings emphasize that weak or default credentials are a common weakness exploited in these cameras (). A robust password policy and device hardening can deter opportunistic attacks.

3. Keep Firmware Updated (or Replace Unsupported Devices):

Regularly apply firmware updates and security patches provided by the camera manufacturers (). Many vulnerabilities that Chinese state hackers have exploited (such as the Hikvision and Dahua flaws mentioned earlier) have patches available – but those patches only protect you if installed. Develop a maintenance plan to check for new firmware on a routine schedule (e.g., monthly or quarterly per vendor advisories). If the manufacturer no longer supports a camera model and isn't receiving updates, strongly consider replacing it.

Running outdated, unpatchable equipment is an unacceptable risk, especially for devices facing critical networks. Inventory your camera fleet and identify any end-of-life models – these should be prioritized for retirement. In environments covered by regulations (e.g., federal contractors), simply having certain banned devices, even if not actively exploited, can violate policy. So, replacement is both a security and compliance mandate in those cases.

4. Monitor Network Traffic and Device Behavior:

Implement continuous monitoring to detect signs of compromise or abnormal behavior in camera devices. Traditional security tools may not inspect IoT device traffic closely, so consider specialized solutions. The FBI recommends explicitly using security monitoring tools that log network traffic to establish a baseline of normal activity and detect deviations, including lateral movement.

5. Incident Response and Isolation:

Even with preventive measures, organizations must be prepared to respond quickly if a camera is compromised. Automated or one-click isolation of affected devices can play a pivotal role in response. Policies can be set to automatically cut off a camera that exhibits malicious behavior. At a minimum, teams can manually quarantine the device when an issue is suspected. This stops an attacker from doing further harm – for instance, blocking a camera that's been taken over prevents the hacker from using it to traverse into more critical systems or from exfiltrating footage. After isolation, teams should also check the device for compromise – this might involve inspecting the firmware integrity or logs. While externally observable indicators can be monitored, a deeper forensic check can confirm if malware exists on the camera's firmware. In practice, one can swap out the suspected device with a clean spare to restore camera coverage and then analyze the compromised unit offline.

6. Ongoing Asset Management and Policy Enforcement:

Mitigation is not a one-time task but an ongoing process. Use asset management tools to maintain an up-to-date inventory of all cameras and IoT devices on your networks. Tag or label devices that are critical or that originate from high-risk manufacturers. Regularly review this inventory against the latest government ban lists and internal security policies. If new devices are added, ensure they meet security standards (avoiding prohibited brands and properly configured). Alert systems can be set to notify if any new device from a banned vendor connects to the network – effectively providing an early warning if, say, someone inadvertently installs a disallowed Hikvision camera. This continuous visibility is key to enforcing compliance with policies like NDAA §889. Furthermore, checks for these cameras should be incorporated into vendor risk management and procurement processes. For example, procurement checklists should be updated to avoid white-labeled Chinese cameras.

Collectively, the above steps form a defense-in-depth approach. Start by **reducing the attack surface** (no internet exposure, strong credentials, updated firmware), then **monitor aggressively** for any intrusion. Be ready to **respond and contain** quickly if an incident occurs. It is particularly important to heed official guidance: DHS, CISA, and FBI have **consistently advised isolating these devices and monitoring them closely** as essential defenses (). Organizations should also educate their IT and security personnel about the risks – a camera should not be treated as a simple appliance but as a potential network computer that needs oversight.

How Armis Can Help

Armis Centrix™, the Armis Cyber Exposure Management Platform, detects known and unknown attacks by continuously analyzing the network traffic, source, destination, and identifying malicious and suspicious threats including signature-based known attacks such as Log4j and SQL Injection, IOCs using behavioral patterns analysis including Brute Force, Port Scan and Malicious Hosts Connections, and abnormal asset behavior.

Armis Centrix™ has a cloud-based threat detection engine, using machine learning and artificial intelligence to detect when a device is operating outside of its “known good” baseline. Our multi-detection technology supports both anomaly detection and policy-based detection for more comprehensive protection. Monitor any device’s communication in your environment and respond quickly and effectively to suspicious deviations.

Armis Centrix™, is powered by the Armis AI-driven Asset Intelligence Engine that monitors billions of assets world-wide in order to identify cyber risk patterns and behaviors. It delivers unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

Armis Centrix™ provides organizations with the ability to build a comprehensive cybersecurity program focused on: asset management and security, vulnerability and security finding, prioritization and remediation, OT/ICS security, medical device security, and early warning.

Solution, At-a-glance:

Armis can be deployed to watch over all network communications involving your cameras – it will learn typical patterns (e.g., a camera sending video to an internal server) and immediately alert on anomalies (e.g., a camera suddenly sending data to an unknown IP, or a camera scanning other devices on the network).

Armis helps catch an intrusion in its early stages by monitoring it in real-time. For example, if China's MSS attempted to activate a dormant backdoor in a camera, Armis would detect the unexpected command & control traffic. Security teams should integrate such monitoring with their incident response process: if an alert indicates a camera acting suspiciously, treat it as a potential breach, investigate promptly, and remove or isolate the device.

Armis can play a pivotal role in incident response and isolation by enabling automated or one-click isolation of affected devices. Policies can be set so that Armis will automatically cut off a camera that exhibits malicious behavior. At a minimum, administrators can use the Armis console to quarantine the device when an issue is suspected manually. This stops an attacker from doing further harm – for instance, blocking a camera that's been taken over prevents the hacker from using it to traverse into more critical systems or from exfiltrating footage. After isolation, IT staff should also check the device for compromise – this might involve inspecting the firmware integrity or logs. While Armis monitors externally observable indicators, a deeper forensic check can confirm if malware exists on the camera's firmware.

Leverage Armis and other asset management tools to maintain an up-to-date inventory of all cameras and IoT devices on your networks. Tag or label devices that are critical or that originate from high-risk manufacturers. Regularly review this inventory against the latest government ban lists and internal security policies. If new devices are added, ensure they meet security standards (avoiding prohibited brands and properly configured).

Armis can be set to alert if any new device from a banned vendor connects to the network – effectively providing an early warning if, say, someone inadvertently installs a disallowed Hikvision camera. This continuous visibility is key to enforcing compliance with policies like NDAA §889. Furthermore, checks for these cameras should be incorporated into vendor risk management and procurement processes. For example, procurement checklists should be updated to avoid white-labeled Chinese cameras.

Conclusion

The recent DHS warning about China's MSS exploiting Chinese-made video cameras highlights a sobering reality: seemingly benign devices installed in our offices, factories, and power plants can be turned into tools of state-sponsored espionage or sabotage. **Chinese-manufactured cameras (notably those from Hikvision and Dahua and their offshoots) have well-documented security weaknesses** and a direct line back to a geopolitical adversary. U.S. government actions, from federal procurement bans to FCC import restrictions, underscore the seriousness of the threat and aim to stem the influx of these devices. However, many such cameras persist across critical infrastructure, often unknowingly via third-party rebranding. This report has identified the major brands and models of concern and reviewed the policies in place to address them.

Organizations can take specific measures to reduce the risk of these devices, but this is no easy task – strategies involve isolating cameras from networks, changing default passwords and minimizing exposure, restricting cloud connectivity and ports. Effective monitoring (and incident response) also requires specialized tools that can inspect camera traffic for anomalies or known attacks. Armis Centrix™ provides such capabilities with multi-detection technology, AI-driven asset intelligence and asset management and security to monitor your entire attack surface – including all IoT devices like Chinese video cameras. If you operate a critical infrastructure environment where these banned Chinese-made cameras are present, **addressing them should be a top security priority**. Don't delay in assessing your risks, patching vulnerable equipment, and upgrading to more secure alternatives – do it now to keep your organization safe from China's state hackers.

Sources

- Internet-connected cameras made in China may be used to spy on US infrastructure: DHS | **Everett Post**
- Dahua Technology Co., Ltd Digital Video Recorders and IP Cameras | **CISA**
- Interim Rule Implements Section 889 Ban on Contractors Using Certain Telecoms Equipment | **Armis**
- Chinese-Made Cameras Pose a Threat to National Security | **Armis**
- Top CVEs Actively Exploited By the People's Republic of China State-Sponsored Cyber Actors | **CISA**
- Armis Partners with ECS to Deliver the Next Generation of CDM Data Services for U.S. Department of Homeland Security (DHS) | **Armis**
- Hikvision Cameras | **CISA**
- The PRC Laws

ARMIS LABS

About Armis Labs

Armis Labs, a division of Armis, is a team of seasoned security professionals dedicated to staying ahead of the ever-evolving cybersecurity landscape. With a deep understanding of emerging threats and cutting-edge methodologies, Armis Labs empowers organizations with unparalleled visibility and expertise to protect against the threats that matter most, right now.

At the heart of Armis Labs lies a formidable research powerhouse, where experts investigate the latest trends and tactics employed by cyber adversaries. Armed with access to over 5 billion profiled assets and state-of-the-art tools and methodologies, the team at Armis Labs conducts in-depth analyses of evolving threats both in the pre-emergence stage and “in the wild” stage of an attack.

+5 Billion

Core to Armis Labs is our Asset Intelligence Engine. It is a giant, crowdsourced, cloud-based knowledge base—the largest in the world, tracking over five billion assets—and growing. It powers Armis Labs with unique, actionable cyber intelligence to detect and address real-time threats across the entire attack surface.

Armis Labs security practitioners are utilizing cutting edge tools that include deception technology, incident forensics, reverse engineering, dark web monitoring, and human intelligence to proactively identify and mitigate threats before they manifest. Leveraging advanced AI/ML technologies, Armis Labs’ proactive threat detection capabilities enable organizations to stay one step ahead of cyber adversaries, minimizing the risk of potential breaches while stopping potential damage before it occurs.

Armis Labs is dedicated to providing organizations with the tools and expertise they need to defend against the threats that matter most, right now. With comprehensive threat intelligence, proactive threat detection capabilities, and seamless integration into existing security workflows, Armis Labs empowers organizations to stay ahead of cyber adversaries and protect their most critical assets.

ABOUT THE AUTHOR

Andrew Grealy

Head of Armis Labs

Andrew Grealy is Head of Armis Labs, the dedicated research practice at Armis. Equipped with state-of-the-art tools and methodologies that leverage one of the largest data sets in the world, Armis Labs conducts in-depth analyses of evolving threats, both in the pre-emergence stage and “in the wild” stage of an attack. Andrew has a vast background in AI, threat detection and threat intelligence. He was most recently the CEO and Co-Founder of CTCI, which was acquired by Armis in February 2024. Andrew is also an advisor to multiple AI and cybersecurity companies.

ARMIS

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization’s cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011