OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS

3 FEBRUARY 2025 DHS-IA-IF-2025-02684

CYBERSECURITY

(U//FOUO) People's Republic of China: Exploitation of Internet-Connected Cameras Threatens US Critical Infrastructure

(U//FOUO) **The ability of People's Republic of China (PRC) cyber actors to access internet-connected cameras—especially those manufactured in the PRC—in the Homeland probably enables Beijing to conduct espionage or disrupt US critical infrastructure.**[a] These devices typically lack data encryption and security settings and have default settings to communicate with their manufacturer, which, for PRC-made cameras, could be in China. There are tens of thousands of PRC-made cameras on the networks of US critical infrastructure entities—including within the chemical and energy sectors—some of which are connected to operational technology (OT) networks, according to open-source and CISA reporting. Enforcing tighter restrictions on these cameras, such as by better identifying which have been re-branded or integrated into other systems, could help mitigate the threat.

- *(U//FOUO)* PRC cyber actors have previously exploited net-facing cameras. In September 2024, PRC cyber actors used internet-connected cameras as part of a botnet, according to an FBI and NSA joint cybersecurity advisory. In March 2024, a US oil and natural gas firm's PRC-made cameras communicated with China-based servers, including one possibly associated with a PRC state-sponsored cyber actor, according to reporting from ODNI's Commercial Cyber Threat Intelligence Program. PRC state-sponsored cyber actors have extensively targeted vulnerabilities associated with PRC-made cameras since at least 2020, according to CISA and commercial cyber threat reporting.

- *(U//FOUO)* Cameras connected to safety and industrial control systems (ICS) could be used by PRC cyber actors to gain access and manipulate systems, according to DOE technical analysis of multiple brands of PRC-manufactured cameras.[b] As of

[a] *(U//FOUO)* For more information on the PRC's assessed focus on US critical infrastructure sectors—including Energy, Water and Wastewater Systems, Communications, Transportation, and Financial Services—please see "People's Republic of China Disruptive Cyber Capabilities for Crisis or Conflict Likely Focus on Five Critical Infrastructure Sectors," DHS-IA-IF-2023-11775, dated 10 October 2023.
[b] *(U)* For further details on DOE's technical analysis, see Appendix.

December 2022, at least four US oil and gas entities had PRC-manufactured cameras networked to OT systems, according to a CISA report.

- *(U//FOUO)* PRC-manufactured, internet-connected cameras and devices could serve as additional vectors for cyber actors to gain and maintain stealthy, persistent access to US critical infrastructure. PRC state-sponsored cyber actors have compromised US critical infrastructure IT networks with the assessed goal of pre-positioning themselves for disruptive or destructive cyber attacks against US critical infrastructure in the event of a major crisis or conflict with the United States, according to Congressional testimony and joint cybersecurity advisories.

(U//FOUO) **The PRC is taking advantage of common commercial trade practices that hamper the ability of US regulators and industry to identify and block the use of PRC-manufactured, internet-connected cameras in US critical infrastructure.** Many of these cameras are imported after being packaged and sold by another company—a practice known as white labeling—sometimes as part of a package in which the cameras are integrated with other equipment. Broader dissemination of tools designed to help recognize PRC cameras, particularly white-labeled cameras, could tighten enforcement of the 2022 Federal Communication Commission (FCC) ban on the import of these cameras and help mitigate the threat of PRC cyber actors exploiting them for malicious purposes.

- *(U)* In early 2024, a US cybersecurity firm estimated that 12,000 PRC-manufactured, internet-connected cameras were in use at hundreds of US-based critical infrastructure entities. It was further estimated that, despite the FCC ban on their import, the number of cameras installed in US networks grew by up to 40 percent between 2023 to 2024, possibly due to white labeling.
- *(U//FOUO)* In 2022, CISA identified likely white-labeled, PRC-manufactured, internet-connected cameras at over 100 US-based federal, state, local, tribal, and territorial government and critical infrastructure entities.
- *(U)* CISA has published two manuals to help entities identify PRC-manufactured cameras of concern, even if they have been white-labeled: the “Hikvision Device Identification Playbook” and “Dahua Device Identification Playbook.”

(U//FOUO) **Appendix: Potential Camera-Enabled Cyber Attack Scenarios**

(U//FOUO) An early 2024 DOE national laboratory technical analysis of internet-connected cameras identified a wide range of ways that a malicious cyber actor could exploit the cameras, ranging from nuisance-level disruptions to physical destruction of equipment and infrastructure.

- *(U//FOUO)* A cyber actor could use the camera's audio or video surveillance data to capture passwords or other credentials; identify vendor and device data; understand a facility's physical and network layout to help plan attacks; collect sensitive operational or system data, including on contingency or maintenance conditions; monitor an attack in real time; or manipulate process-monitoring information sent to operators.
- *(U//FOUO)* A cyber actor could leverage cameras placed on IT networks for initial access and pivot to other devices to exfiltrate sensitive process data that an actor could use for attack planning or disrupting business systems. An actor could also disrupt OT processes, resulting in service disruptions.
- *(U//FOUO)* A cyber actor could use cameras placed on OT networks for initial access and pivot to ICS devices. Potential impacts vary depending on the attacker's intent, level of sophistication, and the setup of the victim's system. Impacts could range from nuisance-level disruptions to physical destruction of equipment and infrastructure.
- *(U//FOUO)* A cyber actor could use cameras placed on safety systems to suppress alarms, trigger false alarms, or pivot to disable fail-safe mechanisms. Adversaries might suppress alarms to cover up a cyber attack or to prevent operators from addressing an unsafe situation.
- *(U//FOUO)* A cyber actor could use the cameras to conduct denial-of-service attacks, in which it bombards a target with web traffic to disrupt its operation. The camera could be integrated with other infected devices to create a botnet.
- *(U//FOUO)* A cyber actor could use geolocation data from a camera to inform, support, or refine kinetic strikes.

Reference and Dissemination Information

Feedback

(U//FOUO) Customers may submit feedback on DHS I&A Analytic products via the DHS I&A Evaluation Form located at the following addresses:

- Unclassified: https://forms.office.com/g/FKkyksC3eg
- SIPR / HSDN: https://go.sgov.gov/IAFeedback
- JWICS / CLAN: https://go.intelink.ic.gov/IAFeedback

Definitions

(U) **Botnet:** A network of compromised computers and other internet-connected equipment, such as routers or internet of things (IoT) devices, under unified command and control.

(U) **Denial-of-Service (DoS):** A type of cyber attack designed to prevent users from accessing a network-connected service by sending illegitimate requests from one source.

(U) **Industrial Control System (ICS):** A computer or network that controls physical processes for industrial facilities and infrastructure.

(U) **Internet of Things (IoT):** A concept that describes everyday physical objects being connected to the internet and identifying themselves to other devices.

(U) **Operational Technology (OT):** General term that encompasses multiple types of hardware and software, the common theme of which is using electronic processes to monitor and process operational data or effect a physical change. Types of OT include ICS; supervisory control and data acquisition (SCADA) systems; distributed control systems (DCS); and other individual devices, such as programmable logic controllers (PLCs) and human-machine interfaces.

Reporting Suspicious Activity

(U) **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi.

(U) **To report a computer security incident, please contact CISA at 888-282-0870; or go to IRF Index - IRF. Please contact CISA for all network defense needs and complete the CISA Incident Reporting System form.** The CISA Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to CISA. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.

(U) **To report this incident to the Intelligence Community, please contact your DHS I&A Field Intelligence Officer at your state or major urban area fusion center, or e-mail DHS.INTEL.FOD.HQ@hq.dhs.gov.** DHS I&A Field Intelligence Officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.

Warning Notices & Handling Caveats	*(U)* **Warning:** This information is provided only for intelligence purposes. It cannot be used in connection with any foreign or domestic court proceedings or for any other legal, judicial, or administrative purposes. *(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. *(U)* US person information has been minimized. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.

Homeland Security

Office of Intelligence and Analysis

Customer Feedback Form

Product Title: (U//FOUO) People's Republic of China: Exploitation of Internet-Connected Cameras Threatens US Critical I

All survey responses are completely anonymous. No personally identifiable information is captured unless you voluntarily offer personal or contact information in any of the comment fields. Additionally, your responses are combined with those of many others and summarized in a report to further protect your anonymity.

1. Please select partner type: Select One **and function:** Select One

2. What is the highest level of intelligence information that you receive? Select One

3. Please complete the following sentence: "I focus most of my time on:" Select One

4. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Neither Satisfied nor Dissatisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Product's overall usefulness	○	○	○	○	○	○
Product's relevance to your mission	○	○	○	○	○	○
Product's timeliness	○	○	○	○	○	○
Product's responsiveness to your intelligence needs	○	○	○	○	○	○

5. How do you plan to use this product in support of your mission? ***(Check all that apply.)***

□ Drive planning and preparedness efforts, training, and/or emergency response operations

□ Observe, identify, and/or disrupt threats

□ Share with partners

□ Allocate resources (e.g. equipment and personnel)

□ Reprioritize organizational focus

□ Author or adjust policies and guidelines

□ Initiate a law enforcement investigation

□ Intiate your own regional-specific analysis

□ Intiate your own topic-specific analysis

□ Develop long-term homeland security strategies

□ Do not plan to use

□ Other:

6. To further understand your response to question #5, please provide specific details about situations in which you might use this product.

7. What did this product *not* address that you anticipated it would?

8. To what extent do you agree with the following two statements?

	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree	N/A
This product will enable me to make better decisions regarding this topic.	○	○	○	○	○	○
This product provided me with intelligence information I did not find elsewhere.	○	○	○	○	○	○

9. How did you obtain this product? Select One

10. Would you be willing to participate in a follow-up conversation about your feedback? Yes

To help us understand more about your organization so we can better tailor future products, please provide:

Name:

Organization:

Contact Number:

Position:

State:

Email:

Submit Feedback

Privacy Act Statement