TLP:CLEAR

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

General Intelligence and Security Service (AIVD)
Military Intelligence and Security Service (MIVD)

july 2026

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

Key points

- Russian state actors are systematically conducting **digital espionage operations via IP cameras**, which are cameras with internet access.
- At least one **Russian intelligence and security service** is conducting digital espionage operations via IP cameras **in the Netherlands**, as well as various **other EU and NATO member states and Ukraine**.
- This actor performs automated analysis of imagery through image recognition software to conduct targeted searches for military vehicles and the military cargo they are transporting.
- This provides the actor with, among other things, **relevant military data**, such as EU and NATO military transport routes, weapon deliveries to Ukraine, and the locations of Ukrainian military personnel.
- The information from IP cameras in Ukraine is used in attempts to **neutralise Ukrainian military personnel and to destroy their military materiel**.
- Furthermore, the Russian service is using the access to IP cameras to acquire relevant military intelligence in European member states, including information that is not directly relevant to the war in Ukraine.
- Intelligence reveals a systematic increase in the number of digital espionage operations by Russian state actors to support military operations during the war in Ukraine.
- People and organisations in the Netherlands and Europe can **reduce the risks of espionage by implementing measures** for the use of IP cameras, such as:
  - Limiting direct access to the IP camera from the internet;
  - Limiting the field of vision of the IP camera;
  - Managing the access and authentication of IP camera users;
  - Ensuring the firmware and software of the IP camera is up to date.

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

Context

Russian digital espionage operations via IP cameras

Intelligence from the Netherlands General Intelligence and Security Service (AIVD) and the Netherlands Defence Intelligence and Security Service (MIVD) – the Dutch services – illustrates that Russian state actors are systematically conducting digital espionage operations via IP cameras (cameras with internet access). At least one Russian intelligence and security service is responsible for these operations that are taking place in the Netherlands, various other EU and NATO member states and Ukraine. This cybersecurity advisory concludes with actionable recommendations to mitigate the risks of espionage via IP cameras.

The information obtained by the Russian state actor via digital espionage operations targeting IP cameras provides insight into relevant military data, such as EU and NATO military transport routes and weapon deliveries to Ukraine. The Russian state actor uses image recognition software to conduct targeted searches for military vehicles and the military cargo they are transporting.

In some cases, the access to IP cameras gained by the Russian state actor in Ukraine is used to identify the locations of Ukrainian military personnel. Intelligence reveals that this information is subsequently used to neutralise Ukrainian military personnel and military materiel in use by the Ukrainian armed forces. Furthermore, the Dutch services have determined that the Russian service is using the access to IP cameras to acquire relevant military intelligence in EU and NATO member states, including information that is not directly relevant to the war in Ukraine.

To date, the Dutch services have not observed the Russian state actor using such information for military attacks outside Ukraine. However, it does demonstrate that the Russian service is capable of acquiring relevant intelligence from IP cameras and that the same tactics could possibly be implemented by Russian military units in a future conflict.

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

Digital espionage supporting the Russian war in Ukraine

The Dutch services assess that there has been a systematic increase in the number of digital espionage operations by Russian state actors to support military operations since the start of the war in Ukraine. The digital activities that target IP cameras form only a small part of their operations. The Russian authorities derive significant tactical and strategic advantages from the deployment of cyber operations, from both defensive and offensive perspectives. For example, the MIVD has previously issued a warning about exploratory activities by Russian state actors targeting logistical routes, including routes in the Netherlands.[1] [2]

In recent years, the Dutch services have observed numerous activities in which Russian state actors have deployed cyber operations to identify and neutralise Ukrainian military personnel and Ukrainian armed forces' materiel. The Dutch services further deem it highly probable that the threat posed by Russian cyber operations to the Ukrainian armed forces will increase throughout almost the whole of Ukraine. Furthermore, these cyber operations possibly provide an early warning of Ukrainian operations and troop movements, which potentially leaves them exposed to disruption or rendered less effective.

How Russian actors gain access to IP cameras

The internet offers various services that facilitate easy, swift and targeted scanning of the environment for devices. IP cameras can subsequently be identified based on device characteristics, such as brand names.[3]

Once an IP camera has been identified, the malicious actor can attempt to gain access to the IP camera via the internet. This is often a relatively simple process, since many IP cameras that are connected to the internet lack adequate security measures. For example, they often have default passwords, obsolete firmware and factory configurations.

[1] MIVD, Russian GRU Targeting Western Logistics Entities and Technology Companies, https://www.defensie.nl/documenten/2025/05/21/russian-gru-targeting-western-logistics-entities-and-technology-companies 13 May 2025.

[2] Cybersecurity and Infrastructure Security Agency (CISA), Russian GRU Targeting Western Logistics Entities and Technology Companies, https://www.defensie.nl/documenten/2025/05/21/russian-gru-targeting-western-logistics-entities-and-technology-companies 17 April 2026.

[3] NCSC, The internet is being scanned, https://www.ncsc.nl/edge-devices/het-internet-wordt-gescand.

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

Recommendations

Public and private entities can implement measures to mitigate the risk of espionage as far as possible. The most important factors in this process are the field of vision and the accessibility of the IP camera from the internet.

Limit direct access to IP cameras from the internet

- Ensure that live streams are not publicly accessible via the internet, unless these live streams serve an essential purpose.
- Avoid using port forwarding[4]-functionalities on the network router to expose the IP camera to external access.
- Disable Universal Plug and Play (UPnP) on the IP camera. This setting enables automated port forwarding.
- Configure the local network to allow for the use of a Virtual Private Network (VPN) connection to establish remote access to the local network via the internet. The IP camera can then be accessed via the VPN connection.
- Disable any protocols that are not required for the use of the IP camera, for example SSH, Bonjour, FTP, UPnP and Telnet. If possible, use only secured protocols such as HTTPS and RTSPS.[5]

Limit the field of vision of the IP camera

- Position the IP camera to match its intended use, and keep irrelevant objects out of view as much as possible.
- Internet-connected IP cameras should ideally be aimed at locations and objects that do not form part of logistical flows or public infrastructure. This reduces the risk of digital espionage on critical routes, harbours or loading zones.
- Mask sensitive zones within the field of view, for example by blurring them. The software of some IP cameras allows for specific parts of the image to be masked.
- Limit visible details, such as GPS location, on the images of the stream.

[4] Port forwarding is a technique used to direct incoming internet traffic through a specific port directly to a pre-configured device.

[5] Consult the device or supplier manual for an overview of the available settings and how these can be configured.

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

Access control and authentication

- Immediately change the default passwords when installing a new IP camera. Use complex, unique passwords that have not been published in databases of breached passwords.[6]
- Isolate IP cameras within a dedicated Virtual Local Area Network (VLAN), separate from the main network.
- Use the admin account exclusively for admin matters and not to access the IP camera's live stream. Only user accounts with limited rights should be used to access the live stream.
- Use multi-factor authentication (MFA) for all access to the IP camera stream.

Ensure the firmware and software of the IP camera is up to date

- Choose an IP camera that offers several years of security support for both firmware and software.
- Periodically check for new security updates for the IP camera's firmware and software.

Origin of the IP camera

- Be aware of the origin of the IP camera. A number of countries, such as China, Russia and Iran, are actively conducting offensive cyber programmes targeting Dutch interests.[7]

Unknown IP cameras

- Be wary of unknown IP cameras on or directed at your premises, which may have been deployed by external actors.

[6] Use services such as https://haveibeenpwned.com/passwords to verify that a password is not listed in a database of breached passwords.

[7] AIVD, What is an offensive cyber programme?, https://www.aivd.nl/vraag-en-antwoord/cyberdreiging/wat-is-een-offensief-cyberprogramma.

Cybersecurity advisory

Russian state actors are compromising IP cameras in Europe for military purposes

Additional reading

Consult the following resources for more in-depth information:

- AIVD, What is an offensive cyber programme?, https://www.aivd.nl/vraag-en-antwoord/cyberdreiging/wat-is-een-offensief-cyberprogramma.
- AIVD, Offensive cyber programmes: an ideal business model for states, https://www.aivd.nl/documenten/2019/06/27/offensief-cyberprogramma-een-ideaal-businessmodel-voor-staten, 27 June 2019.
- NCSC, The internet is being scanned, https://www.ncsc.nl/edge-devices/het-internet-wordt-gescand, 13 November 2025.
- NCSC, What is a VPN?, https://www.ncsc.nl/databeveiliging/wat-is-een-vpn, 18 November 2025.
- NCSC, Security tips for Internet of Things (IoT), https://www.ncsc.nl/edge-devices/beveiligingstips-voor-internet-of-things-iot, 29 May 2026.
- NCSC, Asset management, https://www.ncsc.nl/asset-management, 16 December 2025.
- NCSC UK, 'Smart' security cameras: Using them safely in your home, https://www.ncsc.gov.uk/guidance/smart-security-cameras-using-them-safely-in-your-home, 3 March 2020.

About this Cybersecurity Advisory

The Dutch services regularly publish advisories derived from intelligence investigations conducted by both agencies. These publications can be accessed via the AIVD website, english.aivd.nl/cyberadvisories. A cybersecurity advisory is intended to give users actionable recommendations in the form of security measures, in order to increase resilience against state actors. The Dutch services issue these recommendations based on assessed intelligence, knowledge and expertise. The primary focus is on European security.

Distribution of the Cybersecurity Advisory

This document is marked **TLP:CLEAR**

Subject to copyright laws and the applicable regulations and procedures for the disclosure of information, TLP:CLEAR information may be distributed without restriction.

General Intelligence and Security Service (AIVD)
P.O. Box 20010 | 2500 EA the Hague
english.aivd.nl

Military Intelligence and Security Service (MIVD)
english.defensie.nl

july 2026