October
2024

TECHNICAL SURVEILLANCE AWARENESS FOR INSIDERS

JOB AID

INTRODUCTION

What Is Surveillance?

Surveillance is the act of monitoring or observing individuals, groups, or environments, often with the intention of gathering information to conduct or prevent criminal activity. Surveillance takes many forms, including physical observation, electronic monitoring, video recording, data collection, and analysis. Law enforcement and private investigators use surveillance to maintain security, enforce laws and regulations, protect against threats, and investigate criminal activity.

What Is Technical Surveillance?

Technical surveillance encompasses all active and passive surveillance activities that involve tools, such as audio, video, or any other technical method for capturing and recording information. This includes monitoring a person or group's online activity, mobile devices, home and office networks, social media accounts, online activities, or any other publicly available online or digital activity.

Why Is an Understanding of Technical Surveillance So Important?

There are a wide range of technical surveillance devices and software available. Some are small, inexpensive, easily obtained, and easily installed on devices. Some are bespoke devices and techniques created by professional foreign intelligence services (FIS). The opportunities to compromise privacy are numerous, and always evolving. The technical components of surveillance are ever evolving both for and against you. Technical surveillance countermeasure specialists must continuously research emerging threats and develop counter measures to reduce the threat.

For Whom Was This Job Aid Created?

This job aid is designed to give individuals a better understanding of technical surveillance. This job aid will provide individuals with a baseline understanding and provide information that can be used to become better versed in the threat actors, tactics, tools, and procedures used to compromise your systems and devices.

How Should This Job Aid Be Used?

This job aid is not all-inclusive – use it as a tool to develop additional understanding of technical surveillance and for guidance on how organizations can protect their missions and priorities. Utilize it also as a reminder of the exceptional duty of care vested in those with access to information and critical infrastructure systems.

LEARN MORE: Readers should further consult applicable and controlling laws, regulations, policies, and procedures. Visit CDSE for additional training and resources.

NOTE: If the URLs in this document do not open upon clicking, right-click on the hyperlinked text, copy link location, and paste into a browser. Alternatively, you can open the PDF in a browser.

WHO USES TECHNICAL SURVEILLANCE?

Technical surveillance is conducted by a range of persons and organizations:

- **ORGANIZED CRIME:** Targeting individuals or organizations for profit.
- **VOYEUR**: Acting on their own for either personal gratification or other opportunities.
- **BUSINESSES:** Looking to gain a competitive edge over their competition.
- **DISGRUNTLED EMPLOYEES:** Those current and former employees and staff collecting data to ruin a reputation or to collect and sell data to a competitor.
- **STATE-SPONSORED ACTOR:** Conducting operations on behalf of their nation.
- **EX OR CURRENT PARTNER:** Exhibiting "stalker"-type behavior.

LEARN MORE: When it concerns national security, threats are not limited to only cyber, insider, foreign intelligence, and/or criminal activities. The 2023 Annual Threat Assessment of the U.S. Intelligence Community (IC) identified a growing number of foreign intelligence entities (FIE), state actors, and non-state actors targeting the United States Government (USG) and the private sector: Enterprise Risk Mitigation Blueprint for Non-Intelligence Agencies

Examples of Technical Surveillance as a Constantly Evolving Threat

June 22, 2022: Man Who Acted as a Russian Agent

Hector Fuentes, a Mexican citizen who lived in Miami, began to target and surveil a U.S. person on the behalf of a Russian official. Hector took photos of the U.S. person's car and communicated with the Russian official regarding the U.S. person's travel.

Man Who Acted as Russian Agent Sentenced to Federal Prison Term | United States Department of Justice

October 24, 2022: Four Chinese Nationals Charged with Conspiring to Act

Between 2008 to 2018, Wang Lin, Bi Hongwei, Dong Ting (aka Chelsea Dong), Wang Qiang, and others engaged in a wide-ranging and systematic effort to target and recruit individuals to act on behalf of the PRC in the United States. They requested information, materials, equipment, and assistance to the Chinese government to further China's intelligence objectives. These recruitment efforts targeted professors at universities, a former federal law enforcement and state homeland security official, and others to act as agents on behalf of the Chinese government.

Chinese Intelligence Officers Charged with Using Academic Cover to Target Individuals in United States | United States Department of Justice

January 8, 2024: Man Who Acted as Agent for China

Between August 2021 and at least May 2023, Petty Officer Wenheng Zhao secretly collected and transmitted sensitive, non-public information regarding U.S. Navy operational security, military trainings and exercises, and critical infrastructure. Zhao entered restricted military and naval installations to collect and record this information for China.

U.S. Navy Sailor Sentenced to 27 Months in Prison for Transmitting Sensitive U.S. Military Information to Chinese Intelligence | United States Department of Justice

TYPES OF SURVEILLANCE

Covert vs. Overt Surveillance

COVERT SURVEILLANCE refers to techniques that are hidden or disguised so that the subject does not know they are being monitored or watched. **OVERT SURVEILLANCE** refers to the use of devices that are visible and recognizable, such as a signposted CCTV system. Below are some of the most common ways intelligence and information operations are conducted.

- **PHYSICAL SURVEILLANCE:** Sometimes referred to as direct surveillance, physical surveillance involves observing people or places in person. With physical surveillance, investigators can either follow suspects around a location (commonly referred to as moving surveillance) or from a stationary position, also known as a "stakeout."
- **ELECTRONIC SURVEILLANCE:** Electronic surveillance relies on electronic devices such as cameras, microphones, GPS trackers, and other monitoring tools to gather information. Electronic surveillance is typically used by security personnel to monitor individuals within public and private establishments, but it's also used to capture and record covert conversations or activities.
- **CAMERA/VIDEO**: Systems put in place at home to protect personal property, business assets, government and public spaces, and critical infrastructure. They are often connected to a recording device or IP network. Cameras can be used 24/7 in all-weather situations, are smaller, have a high quality, and are more accessible on the open market. The smallest cameras now deliver HD quality video at only a few millimeters in size.
- **AUDIO:** Listening devices at their core consist of a microphone and receiver but also include an RF radio transmitter and receiver as well as low cost but highly effective Global System and Mobile (GSM) bugs, which can utilize cellular networks. While modern mobile phones are harder to monitor due to encoded and compressed transmission, a "man in the middle" attack is possible using an International Mobile Subscriber Identity (IMSI)-catcher.
- **SATELLITE SURVEILLANCE:** Satellite-based systems can be used by both government and private organizations to perform reconnaissance operations domestically and globally.
- **COMPUTER SURVEILLANCE:** Computer/cyber surveillance allows an individual or organization to track, monitor, and surveil subjects from anywhere in the world. This method consists of monitoring an individual's computer usage, including their internet history, emails, and online activities, and injecting software that can allow for increased surveillance.
- **SOCIAL MEDIA SURVEILLANCE:** Information shared on social media is not protected by a reasonable expectation of privacy; therefore, investigators can monitor a suspect's social media activity to gather information about their activities, interests, and contacts.
- **FINANCIAL SURVEILLANCE:** Financial surveillance involves monitoring financial transactions and activities to detect and prevent financial crimes such as money laundering. Financial surveillance can be done on an individual or a corporate level.
- **BIOMETRIC SURVEILLANCE:** Biometric surveillance uses various forms of technology to identify individuals based on physical characteristics such as fingerprints, facial recognition, or iris scans. CCTV is a common tool used in biometric surveillance.

LEARN MORE: An individual's office, position, or security clearance alone may not reduce the likelihood of being the target of cyber espionage. It is recommended that personnel regularly attend training for better situational awareness. The CDSE offers a Counterintelligence Awareness and Security Brief training (CI112.16).

TOOLS USED FOR SURVEILLANCE

- **DRONES:** Drones are expanding their use as a surveillance tool because they are cost-effective, portable, and easy to use. They have been used in a wide range of covert surveillance situations as well as to carry direct action.
- **CAMERAS:** Smartphones are incredibly advanced and have cameras that are capable of taking high-quality photos and videos. Professional cameras provide extremely high-quality photos and have long range capabilities. A high-quality camera with powerful zoom and night vision capabilities can capture clear images and videos of your subject in nearly every situation.
- **CELL PHONE HARDWARE/TOWERS:** Rogue cell towers are false base stations that hijack nearby mobile device connections. These false towers trick the mobile device into thinking it is connected to an authorized cell tower, leaving it vulnerable to man-in-the-middle attacks and increasing threats to privacy.
- **FACIAL RECOGNITION SOFTWARE:** Facial recognition software uses images of human faces to create biometric templates and compares these images with real-time populations to identify and track persons of interest.
- **PC DEVICES AND WEBCAMS:** Web cameras allow a PC user to incorporate video into their computer or mobile device. Software can be used to exploit these devices, allowing unauthorized persons to gain access.
- **MOBILE DEVICES:** Mobile devices pose perhaps an even greater risk than a PC device does. Your device's camera can be used against you, software can be installed for malicious reasons, and mobile devices can be tracked. Most people have a mobile device for personal use, banking, social media, and more, which creates a valuable target.
- **SMART DEVICES AND GAMING CONSOLES:** Video game consoles have network connectivity, system and TV integration capabilities, and a potentially greater range of applications than many devices combined.
- **SOCIAL MEDIA:** An individual's social media account can be accessed and surveilled using either open-source collection or phishing techniques.
- **GPS TRACKING:** GPS tracking devices are used to track the geolocation of persons or property.
- **VIDEO RECORDING DEVICES:** This is a network of cameras, monitors/display units, and recorders. These systems can be analog or digital and can be used with other technologies to assist in monitoring information collected.
- **AUDIO RECORDER:** Is used to capture conversations or other audio information.
- **CYBER:** This involves data gathering through technological tools and surveillance software programs. Cyber leverages malware, spyware, and phishing attacks to exploit vulnerabilities in computer systems and networks. Some methods include social engineering, malware distribution, advanced persistent threat (APT), watering hole attacks, and spear phishing.
- **HUMAN:** Human surveillance has long been a tool for the private investigator or spy. In most cases, the surveillance is covert, using techniques to monitor an individual or group or even infiltrate an organization without their knowledge.

LEARN MORE: Reporting is the first step in countering surveillance activities. Additional resources can be found in the Counterintelligence Awareness Toolkit (cdse.edu).

INSIDER THREAT: POTENTIAL RISK INDICATORS

What Is an Insider Threat?

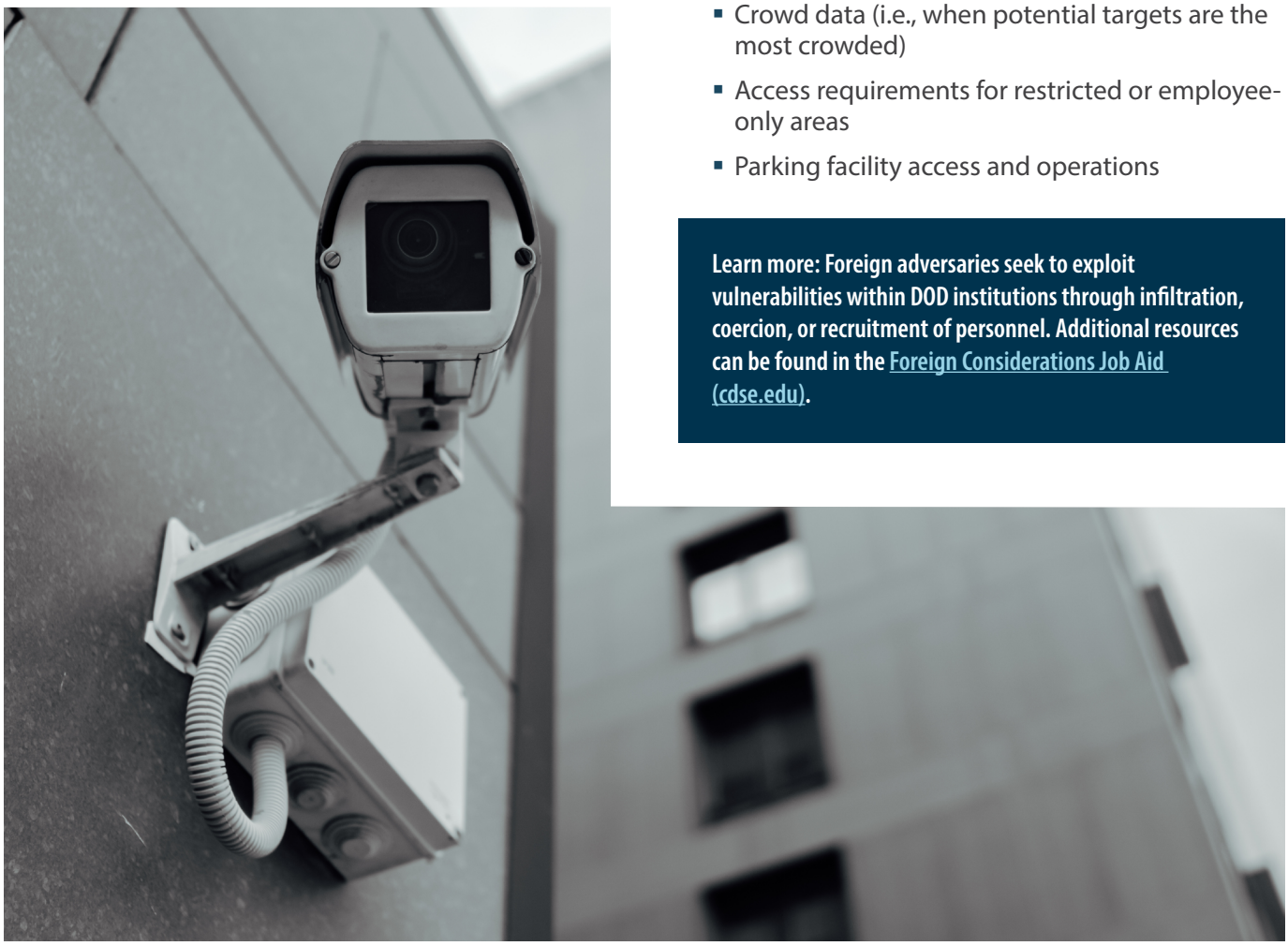
An insider threat is anyone with authorized access who uses that access to wittingly or unwittingly harm the organization and its resources. Insiders can be employees, vendors, partners, suppliers, etc.

Potential Risk Indicators (PRIs)

Most insider threats exhibit risky behavior prior to committing negative workplace events.

Spotting and Reporting PRI

Not all of these PRIs will be evident in every insider threat, and not everyone who exhibits these behaviors is doing something wrong. However, most insider threats have displayed at least some PRIs.



Information Collected through Surveillance

The following types of information have been collected through adversarial surveillance:

- Locations
- Numbers of security personnel and cameras
- Information on key personnel
- Facility layout, including access and egress routes
- Timing of routine events
- Event-specific data (relating to special events)
- Security/visitor processes and procedures
- Security equipment, including badges and uniforms
- Information about maintenance and cleaning personnel or procedures
- Crowd data (i.e., when potential targets are the most crowded)
- Access requirements for restricted or employee-only areas
- Parking facility access and operations

Learn more: Foreign adversaries seek to exploit vulnerabilities within DOD institutions through infiltration, coercion, or recruitment of personnel. Additional resources can be found in the Foreign Considerations Job Aid (cdse.edu).

METHODS USED BY FOREIGN INTELLIGENCE SERVICES

State threats exist online and offline. While a wide range of hostile actors use the internet to target people in the U.S., state actors are well equipped to conduct the most damaging online operations. State and other hostile actors may look to steal information remotely. Stealing information remotely enables them to do so on an industrial scale, with relatively little risk to their intelligence officers or overseas agents, and at little cost. They may also use malicious software, also known as malware, to disrupt and damage infrastructure. This can range from taking a website offline to manipulating industrial systems.

- **ELICITATION:** An effort in which a seemingly normal conversation is contrived to extract information about individuals, their work, and their colleagues.
- **EAVESDROPPING:** Gathering information in social environments by listening in on private conversations.
- **BAG OPERATIONS:** Efforts to steal, photograph, or photocopy documents, magnetic media, or laptop computers. This could occur in your hotel room, in an airport, in a conference room, or in any other situation where the opportunity presents itself and your materials are vulnerable.
- **ELECTRONIC INTERCEPTION:** Use of devices to electronically monitor an individual's use of modern telecommunications, office, hotel, portable telephones, faxes, and computers.
- **TECHNICAL EAVESDROPPING:** Use of audio and video devices, usually concealed in hotel rooms, restaurants, offices, cars, airplanes.

LEARN MORE: Foreign intelligence services may use an individual's (insider's) digital footprint data to understand their pattern of life, preferences, and susceptibilities. This Foreign Intelligence Entity Targeting Recruitment Methodology Job Aid (cdse.edu) offers additional information and insight.

UNUSUAL AND SUSPICIOUS ACTIVITIES

Other examples of surveillance-related activities that are suspicious if they are conducted in an unusual manner include:

- Taking photographs or videos.
- Using image-enhancing devices such as binoculars.
- Making notes, diagrams, or maps.
- Measuring distances in strides or timing events.
- Watching, visiting, or passing by a location repeatedly over time by the same person or vehicle.

Evaluating Unusual Activities

An unusual surveillance-related activity by itself may not necessarily be an indicator of adversarial surveillance. It is important to assess and evaluate the totality of observed actions and behaviors as well as other relevant circumstances.

For example, a person may be interested indoors or entrances for a variety of innocent reasons. However, the person's behavior is suspicious and should be reported if the person displays additional unusual behaviors, such as:

- Making repeated visits to the same location to record or document something about the doors or entrances.
- Attempting to disguise an interest in the doors or entrances.
- Displaying more of an interest in alarm and security features or in restricted or employee-only entrances.
- Questioning employees about security personnel, processes, procedures, and equipment.
- Security tests, attempts to access employee-only or non-public areas, or an increase in alarms or events that require a security or law enforcement response.
- Systems access attempts.
- Thefts or attempted thefts of IDs, badges, or uniforms; smart phones, laptops, or other equipment; or vehicles.

LEARN MORE: The CDSE eLearning course Phishing and Social Engineering: Virtual Communication Awareness Training DS-IA103.06 offers historical examples and insight. This interactive training provides an explanation of various types of social engineering, including phishing, spear-phishing, whaling, smis` hing, and vishing.

PROTECTING AGAINST TECHNICAL SURVEILLANCE

Given these threats, organizations must take proactive steps to protect themselves.

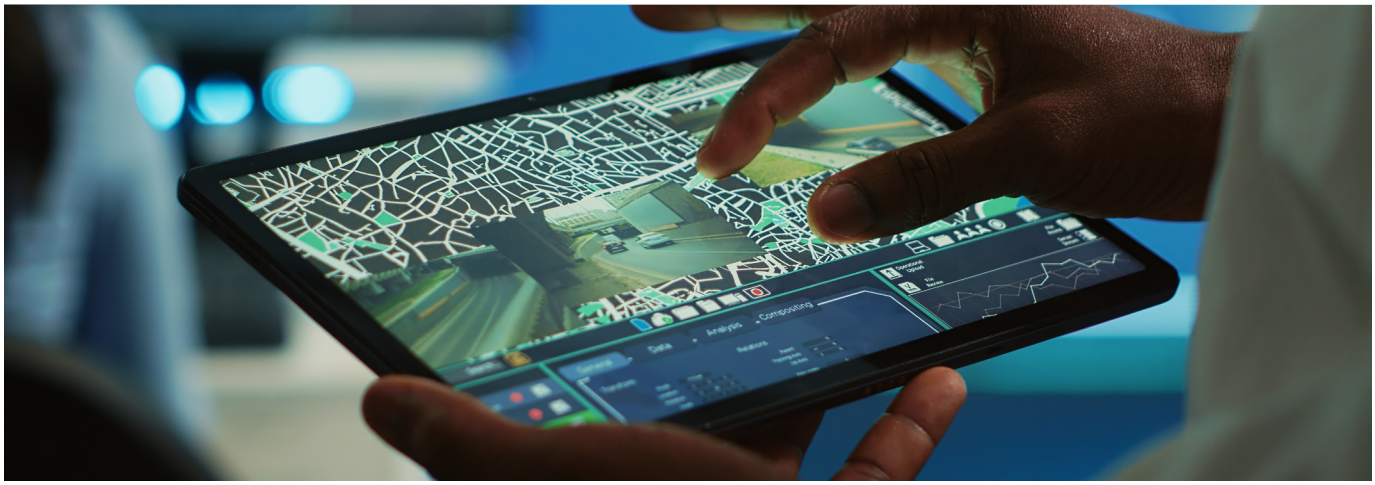
- **EDUCATION AND TRAINING:** Organizations should educate personnel about the types of surveillance technologies that exist and how they can be deployed. Training in digital security practices is crucial.
- **SECURE COMMUNICATIONS:** Use encrypted communication tools approved by your organization. Avoid using unsecured Wi-Fi without an organization-approved VPN.
- **PHYSICAL SECURITY MEASURES:** Be aware of the physical environment. Organizations should regularly check for unauthorized devices in offices and meeting spaces. Use secure, shielded rooms for highly sensitive discussions.
- **DIGITAL HYGIENE:** Maintain strong, unique passwords for all accounts. Regularly update software to protect against vulnerabilities. Use VPNs to secure internet connections, especially when working remotely.
- **DEVICE MANAGEMENT:** Keep personal and professional devices separate. Use anti-virus and anti-spyware software, and regularly check for unusual behavior on devices, such as unexpected battery drain or data usage spikes.
- **INFORMATION PROTECTION:** Educate staff on secure communication methods and be mindful of this when in person and working remotely. Desk and device screens should not be visible from entryways or windows.

Building a Culture of Security

Security awareness should be an integral part of every organization and employee. Organizations must prioritize the safety of their reporters by:

- **IMPLEMENTING SECURITY PROTOCOLS:** Develop and enforce comprehensive security protocols for both digital and physical security.
- **PROVIDING RESOURCES:** Offer tools and resources to help journalists stay secure, such as access to secure communication apps and training sessions.
- **FOSTERING A SECURITY-CONSCIOUS CULTURE:** Encourage open discussions about security threats and best practices. Share knowledge and experiences to collectively enhance security awareness.

Learn more: DoDI 5240.05: Technical Surveillance Countermeasures (TSCM) will be conducted to detect, neutralize, and exploit technical surveillance and associated devices, technologies, and hazards that facilitate the unauthorized or inadvertent access to, or removal of, DOD information.



ADDITIONAL RESOURCES

FEMA Emergency Management Institute (EMI)

IS-914: Surveillance Awareness: What You Can Do

United States Department of State

Guiding Principles on Government Use of Surveillance Technologies

Cybersecurity and Infrastructure Security Agency (CISA)

Cybersecurity Best Practices to Protect Yourself from Tracking Technologies and Spyware

Surveillance Detection Principles (AWR-940)

How to Protect the Data that is Stored on Your Devices

Cyber Security Best Practices

Center for Development of Security Excellence (CDSE)

INT280.16: Cyber Insider Threat (eLearning course)

Cybersecurity Attacks: The Insider Threat (short)

Potential Risk Indicators: Insider Threat (job aid)

Facebook Smartcard

LinkedIn Smartcard

Twitter Smartcard

An Alternative View of Preventing Insider Threats: Taking Culture Seriously (webinar)