The DART Board May 2025

RED DART ALLIANCE

This product is intended to educate readers on events and items of interest relating to technology protection and counterintelligence throughout the United States.

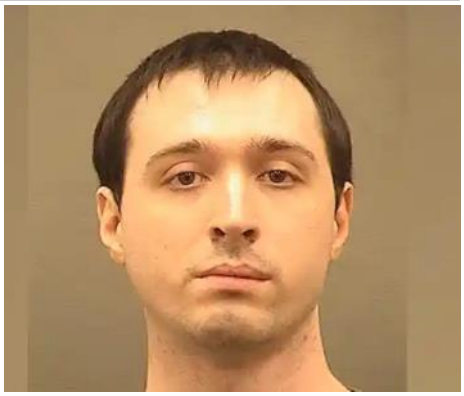
Distribution of this document is Authorized within your agency or company

The information contained in this product was collected through open sources.

The Dart Board is NOT an official endorsement of any of the cited articles

Intelligence Agency IT Specialist Charged with Attempting to Provide Classified Information to Foreign Government

Source: ABC News by Alexander Mallin, 30 May 2025



In communications with an undercover agent with the FBI, posing as an emissary of the foreign country, Laatsch is alleged to have transcribed classified information into a notepad at his desk over a three-day period that he told the agent he was ready to provide.

Video from inside the DIA facility where Laatsch worked showed him writing multiple pages of notes, which he folded into squares and hid in his socks, according to an affidavit filed in U.S. District Court for the Eastern District of Virginia.

Another DIA employee saw Laatsch placing multiple notebook pages in the bottom of his lunchbox, according to the affidavit.

The FBI then conducted an operation on May 1 in which Laatsch agreed to drop the classified information via thumb drive at a designated spot in a public park in northern Virginia, according to the charging documents.

The drive allegedly contained information that was designated at both the Secret and Top Secret classification levels. Laatsch contacted the agent roughly a week later and said he was interested in citizenship to the unnamed country because he did not "expect things here to improve in the long term," according to the documents.

Laatsch again then allegedly attempted to prepare classified information to provide to the agent and in an operation earlier Thursday, he arrived at a location in northern Virginia where he was taken into custody, according to the documents.

Laatsch's arrest comes amid broader concern among current and former intelligence officials that individuals with access to high-value classified information may use the current moment of disarray and consternation in the intel community to try and sell information to foreign governments for profit.

Laatsch, who was hired by the Defense Intelligence Agency in August 2019, most recently worked as a data scientist and IT specialist for information security in the agency's Insider Threat Division, according to court documents.

FBI Warns of Ongoing Scam That Uses Deepfake Audio to Impersonate Government Officials

Source: Arstechnica by Dan Goodin 15 May 2025

The FBI is warning people to be vigilant of an ongoing malicious messaging campaign that uses AI-generated voice audio to impersonate government officials in an attempt to trick recipients into clicking on links that can infect their computers.

"Since April 2025, malicious actors have impersonated senior US officials to target individuals, many of whom are current or former senior US federal or state government officials and their contacts," Thursday's advisory from the bureau's Internet Crime Complaint Center said. "If you receive a message claiming to be from a senior US official, do not assume it is authentic."

Think you can't be fooled? Think again

The campaign's creators are sending AI-generated voice messages—better known as deepfakes—along with text messages "in an effort to establish rapport before gaining access to personal accounts," FBI officials said. Deepfakes use AI to mimic the voice and speaking characteristics of a specific individual. The differences between the authentic and simulated speakers are often indistinguishable without trained analysis. Deepfake videos work similarly.

One way to gain access to targets' devices is for the attacker to ask if the conversation can be continued on a separate messaging platform and then successfully convince the target to click on a malicious link under the guise that it will enable the alternate platform. The advisory provided no additional details about the campaign.

The advisory comes amid a rise in reports of deepfaked audio and sometimes video used in fraud and espionage campaigns. Last year, password manager LastPass warned that it had been targeted in a sophisticated phishing campaign that used a combination of email, text messages, and voice calls to trick targets into divulging their master passwords. One part of the campaign included targeting a LastPass employee with a deepfake audio call that impersonated company CEO Karim Toubba.

In a separate incident last year, a robocall campaign that encouraged New Hampshire Democrats to sit out the coming election used a deepfake of then-President Joe Biden's voice. A Democratic consultant was later indicted in connection with the calls. The telco that transmitted the spoofed robocalls also agreed to pay a $1 million civil penalty for not authenticating the caller as required by FCC rules.

Continued on Page 3

FBI Warns of Ongoing Scam That Uses Deepfake Audio to Impersonate Government Officials

Continued from previous page

Thursday's advisory provided steps people can take to better detect these sorts of malicious messaging campaigns. They include:

Verify the identity of the person calling you or sending text or voice messages. Before responding, research the originating number, organization, and/or person purporting to contact you. Then independently identify a phone number for the person and call to verify their authenticity.

Carefully examine the email address; messaging contact information, including phone numbers; URLs; and spelling used in any correspondence or communications. Scammers often use slight differences to deceive you and gain your trust. For instance, actors can incorporate publicly available photographs in text messages, use minor alterations in names and contact information, or use AI-generated voices to masquerade as a known contact.

Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic facial features, indistinct or irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, watermarks, voice call lag time, voice matching, and unnatural movements.

Listen closely to the tone and word choice to distinguish between a legitimate phone call or voice message from a known contact and AI-generated voice cloning, as they can sound nearly identical.

AI-generated content has advanced to the point that it is often difficult to identify. When in doubt about the authenticity of someone wishing to communicate with you, contact your relevant security officials or the FBI for help.

The guidance is helpful, but it doesn't take into account some of the challenges targets of such scams face. Often, the senders create a sense of urgency by claiming there is some sort of ongoing emergency that requires an immediate response. It's also not clear how people can reliably confirm that phone numbers, email addresses, or URLs are authentic.

The bottom line is that there is no magic bullet to ward off these sorts of scams. Admitting that no one is immune to being fooled is key to defending against them.

Man Attacks Colorado Crowd with Firebombs, 8 People Injured

Source: Reuters by Jasper Ward, Kristina Cooke, and Mark Makela, 02 June 2025

Eight people were injured on Sunday when a 45-year-old man yelled "Free Palestine" and threw incendiary devices into a crowd in Boulder, Colorado where a demonstration to remember the Israeli hostages who remain in Gaza was taking place, authorities said.

Four women and four men between 52 and 88 years old were transported to hospitals, Boulder police said. Authorities had earlier put the count of the injured at six and said at least one of them was in a critical condition.

"As a result of these preliminary facts, it is clear that this is a targeted act of violence and the FBI is investigating this as an act of terrorism," the FBI special agent in charge of the Denver Field Office, Mark Michalek, said. Michalek named the suspect as Mohamed Soliman, who was hospitalized shortly after the attack. Reuters could not immediately locate contact information for him or his family.

"As a result of these preliminary facts, it is clear that this is a targeted act of violence and the FBI is investigating this as an act of terrorism,"

FBI Director Kash Patel also described the incident as a "targeted terror attack," and Colorado Attorney General Phil Weiser said it appeared to be "a hate crime given the group that was targeted." Boulder Police Chief Stephen Redfearn said he did not believe anyone else was involved. "We're fairly confident we have the lone suspect in custody," he said.

The attack took place on the Pearl Street Mall, a popular pedestrian shopping district in the shadow of the University of Colorado, during an event organized by Run for Their Lives, an organization devoted to drawing attention to the hostages seized in the aftermath of Hamas's 2023 attack on Israel.

In a statement, the group said the walks have been held every week since then for the hostages, "without any violent incidents until today." Israeli Prime Minister Benjamin Netanyahu said in a statement that the victims were attacked "simply because they were Jews" and that he trusted U.S. authorities would prosecute "the cold blood perpetrator to the fullest extent of the law".

"The antisemitic attacks around the world are a direct result of blood libels against the Jewish state and people, and this must be stopped," he said. The incident comes amid heightened tensions in the United States over Israel's war in Gaza, which has spurred both an increase in antisemitic hate crime as well as moves by conservative supporters of Israel, led by President Donald Trump, to brand pro-Palestinian protests as antisemitic. His administration has detained protesters of the war without charge and cut off funding to elite U.S. universities that have permitted such demonstrations.

Tip of the Month

CDSE
Center for Development of Security Excellence

SOCIAL MEDIA SAFETY SMART CARD

SOCIAL MEDIA
CONNECTS US GLOBALLY

Maximize social media security by:

- Using secure browsing (https)
- Reviewing your history to identify unauthorized access
- Using multi-factor authentication (MFA) to secure logins

DO

- Secure your accounts with complex passwords/passphrases and a password manager.
- Keep anti-virus software up to date. Only download known or trusted apps.
- Report scammers, spammers, and fake accounts. Doing that helps keep the site safer for everyone.
- Review permissions to your account and data access in your security settings periodically.
- Encourage your family and friends to take similar precautions with their accounts; their privacy and sharing settings can expose your personal data.
- "Opt Out" to prevent companies from collecting your personal information and data based on your activity on websites, devices, or apps for the purpose of advertising.
- Restrict privacy settings to who can view your profile, posts, and photos to friends only.

DO NOT

- Do not connect with or message strangers. Generic photographs? Incomplete profile?Odd wording in message? Be on the lookout for fake profiles.
- Do not assume your posts, photos, direct messages, location, and activities are private. Privacy settings are not a complete solution.
- Do not reveal sensitive job information.
- Do not share personal information in online quizzes; this could be used to get into your account.
- Do not click links in unsolicited chats or direct messages.
- Do not enable location sharing on social media sites.
- Do not post Personally Identifiable Information (PII), such as birthdays, bank account numbers, credit card, or Social Security information.
- Do not post or share photos that let people know you're on vacation. Be vigilant.

WARNING SIGNS
OF A SCAM

- A sense of urgency
- Money, bitcoin, or gift cards
- Deliveries that can't be delivered
- Strange activity on your accounts
- Impersonated accounts of family, friends, businesses, or well-known people
- Invoices from companies you don't recognize
- Generic text messages from numbers you don't know
- Calendar invitations from strangers

WHEN IN DOUBT, REPORT IT!

REDDART
When In Doubt, Report It Out!

Longer but Worthwhile Reads

We've Got a F--king Spy in This Place: Inside America's Greatest Espionage Mystery

On the night of March 10, 1986, Michael Sellers parked his car on a dark Moscow street and peeled off his disguise: a Mission Impossible-style prosthetic mask that made him look like a Black colleague who worked at the embassy. He'd used it to slip past the guards watching the diplomatic compound where he lived. But he'd still have to be careful. On paper, Sellers was an ordinary American diplomat, but the KGB had identified him as a CIA officer and kept him under heavy surveillance.

Sellers quickly changed into another disguise — a typical Soviet overcoat, glasses and a fur-lined Russian chapka hat with built-in hair extensions — before ditching the car to blend into the crowd. He took a circuitous route to shake anyone who might be following him. His mission was to meet a valuable asset the agency had cultivated inside the KGB.

Link: https://www.politico.com/news/magazine/2025/05/16/cia-fbi-spy-russia-mystery-00317973

Uncovering Chinese Academic Espionage at Stanford

This summer, a CCP agent impersonated a Stanford student. Under the alias Charles Chen, he approached several students through social media. Anna*, a Stanford student conducting sensitive research on China, began receiving unexpected messages from Charles Chen. At first, Charles's outreach seemed benign: he asked about networking opportunities. But soon, his messages took a strange turn.

Charles inquired whether Anna spoke Mandarin, then grew increasingly persistent and personal. He sent videos of Americans who had gained fame in China, encouraged Anna to visit Beijing, and offered to cover her travel expenses. He would send screenshots of a bank account balance to prove he could buy the plane tickets. Alarmingly, he referenced details about her that Anna had never disclosed to him.

Link: https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/

SUPPORTING *through* REPORTING

To whom should you report an INSIDER THREAT?

All military, federal, or contract personnel should report potential insider threat incidents to their **Component Insider Threat Hub/Program.**

If you are *not* affiliated with the government as an employee, military member, or contractor, you should contact your **local law enforcement or Federal Bureau of Investigations (FBI.gov).**

Scan the QR code to learn more:

CDSE Center for Development of Security Excellence

www.cdse.edu

LEARN. PERFORM. PROTECT.

How China Recruits it's Spies in the U.S.

Source: CBS News, By Brit McCandless Farmer, 18 May 2025

China's main spy agency, the Ministry of State Security – or MSS – is now the largest and most active spy agency in the world. Its top target is not a foreign power, although the United States ranks number two. Instead, the priority for the MSS is China's own people, including those living abroad in the U.S.

According to Jim Lewis, a former U.S. diplomat whose direct experience with China's intelligence agencies spans more than 30 years, Chinese nationals on foreign soil pose a unique risk to Chinese President Xi Jinping's regime.

"The ability to blackmail people into being agents because of threats to their family is very powerful"

"They could be plotting. It's happened before," Lewis said. "They could be agents of the evil foreign power. They could be learning something that Xi doesn't want them to learn. And so, they are seen as a risk, not as a threat, but as a risk."

According to Lewis, the MSS spies on Chinese nationals living abroad in a few ways. First, it surveils WeChat, a Chinese instant messaging and social media app used by more than 1 billion people worldwide.

"It's hard to do things in China without access to it," Lewis said. "And it's completely monitored with the cooperation of the owner by the Chinese state."

In addition to monitoring online activity, Lewis told 60 Minutes that Chinese intelligence agents have also infiltrated college campuses in the U.S. This corroborates a report this month from the Stanford Review, which alleges that spies from the Chinese Communist Party are recruiting students at the California campus.

"I've had Chinese students tell me, 'I couldn't talk in class because the fellow sitting over there in the corner would report back.'"

According to Lewis, China's MSS uses many of the same techniques as other spy agencies: sex, money, and revenge. "You're a disgruntled employee. You haven't been recognized, and someone comes along and flatters you and says you can pay them back," Lewis explained.

He also said the "honeypot" or "honey trap" strategy is common. A mainstay in spy activity for centuries, a honey trap is when an undercover operative, typically a woman, establishes a romantic or sexual relationship with someone to extract confidential information from them.

If those do not work, there is always a monetary incentive. "Money works like a charm," Lewis said. The MSS last year released a propaganda

Continued on Page 9

How China Recruits it's Spies in the U.S.

Continued from previous page

video on China's largest social network, boasting that the agency "fights against evil." The video served as both propaganda and as a recruiting commercial.

"It's both an advertisement to recruit people and it's an advertisement to warn people that if you fall afoul of us, we will come after you," Lewis explained. "The Chinese want to give this perception they are largely present everywhere anymore."

China's MSS is not the only agency sending a message through flashy videos. The CIA this month released its own videos to encourage Chinese nationals to spy for the U.S. Last year, the CIA also published a text-based video in Chinese that provided detailed, step-by-step guidance on how to safely get in touch with the agency online.

A U.S. official told the New York Times that the agency released this month's videos because the instructional video was successful. The recent, highly produced videos tap into the fear of the Chinese Communist Party, especially for those who still have family living in China.

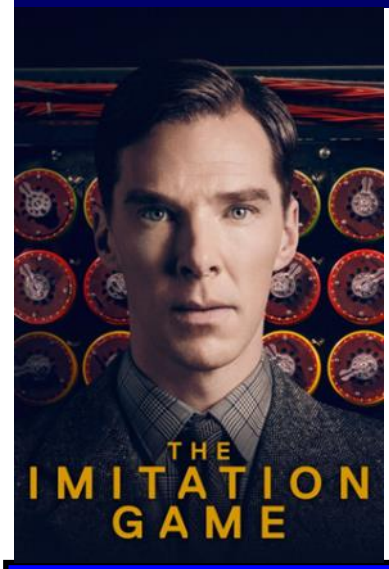
Lewis told 60 Minutes that Chinese intelligence agents coerce Chinese nationals abroad by threatening to harm their family members back home in China.

"The ability to blackmail people into being agents because of threats to their family is very powerful, and it's a tool denied to the West," he said. "But it's a tool that the Chinese are not at all bashful about using."

Lewis told 60 Minutes that people with ties to China are not the only ones who should care about Beijing's coercion abroad.

"One of the precedents that I thought we had learned in the 1940s is that countries that don't respect their own citizens, don't respect their neighbors," he said. "Fundamental rights are the basis of international security... Because when they mistreat their own citizens, you're next."

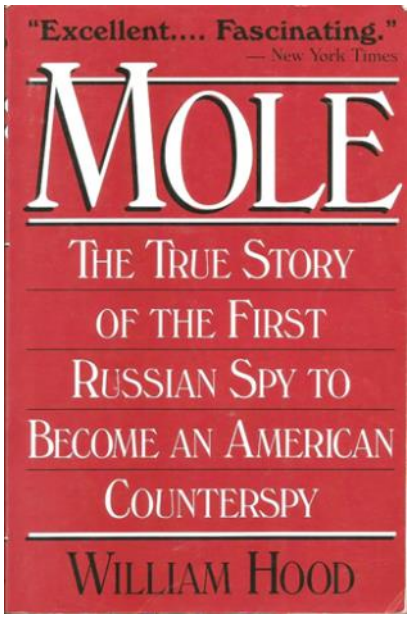
CI CINEMA



The Imitation Game

During World War II, the English mathematical genius Alan Turing tries to crack the German Enigma code with help from fellow mathematicians while attempting to come to terms with his troubled private life.

Watch on Hulu, YouTube and Sling



Mole

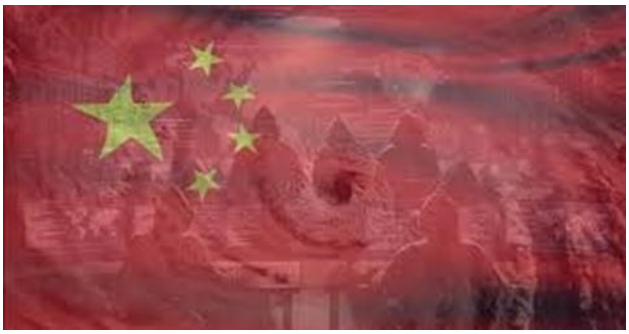
By William Hood

At the heart of all secret operations is the penetration agent—or mole—the lonely man in the enemy camp.

The true story about GRU Lieutenant Colonel Pyotr Semyonovich Popov, CIA's first successful penetration of Soviet intelligence. Between 1952 and 1958, Popov provided the CIA with large amounts of information concerning Soviet military capabilities and espionage operations, including the names of

FBI Asks for Help Tracking Chinese Salt Typhoon Actors

Source: Infosecurity By Phil Muncaster 28 April 2025



The FBI has appealed to the public for information which might help it to unmask the threat actors behind a notorious Chinese APT group.

Salt Typhoon (aka FamousSparrow, GhostEmperor, Earth Estries and UNC2286) is thought to be the work of China's vast Ministry of State Security (MSS), and has been active since at least 2020.

It leapt to fame in November last year after a major intelligence gathering operation targeting US telecommunications companies was revealed by the authorities.

Any actionable information could qualify for a $10m reward from the US Department of State

"Investigation into these actors and their activity revealed a broad and significant cyber campaign to leverage access into these networks to target victims on a global scale," the FBI said in its Public Service Announcement (PSA).

"This activity resulted in the theft of call data logs, a limited number of private communications involving identified victims, and the copying of select information subject to court-ordered US law enforcement requests."

In October, Donald Trump's presidential campaign was told that the phones of Trump and VP JD Vance, as well as staff members from Kamala Harris's 2024 presidential campaign, may have been compromised in the hack.

"FBI maintains its commitment to protecting the US telecommunications sector and the individuals and organizations targeted by Salt Typhoon by identifying, mitigating, and disrupting Salt Typhoon's malicious cyber activity," the PSA continued.

"If you have any information about the individuals who comprise Salt Typhoon or other Salt Typhoon activity, we would particularly like to hear from you."

Any actionable information could qualify for a $10m reward from the US Department of State's Rewards for Justice (RFJ) program. This offers cash in exchange for information on foreign state-linked threat actors who target US critical infrastructure, in violation of the Computer Fraud and Abuse Act (CFAA).

RED DART Agency Spotlight

NGA
NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

What We Do

Strategic Intelligence

NGA provides GEOINT that allows the president and national policymakers to make crucial decisions on counterterrorism, weapons of mass destruction, global political crises and more.

Warfighter Support

NGA enables the Department of Defense to plan missions, gain battlefield superiority, precisely target the adversary and protect our military forces.

Indications & Warning

NGA focuses on global hot spots and provides timely warnings to our military service members and national decision-makers by monitoring, analyzing and reporting imminent threats.

Safety of Navigation

NGA provides and maintains the maps, charts and publications for navigation in the air and on the seas with the most current information for U.S. military forces and global transport networks.

Foundation Data

Foundation data — including topographic, elevation and terrain, land cover, and geodetic information — helps us describe the world in which we live. NGA leads the Department of Defense and intelligence community in the production, procurement, assessment and cataloging of geospatial data.

Humanitarian and Disaster Relief

NGA supports federal agencies' — such as the Department of State and the Federal Emergency Management Agency — response to humanitarian and disaster relief missions.

Special Event Planning

When requested, NGA supports planning for special events such as presidential inaugurations, state visits by foreign leaders, international conferences and major public events (e.g., Olympics, Super Bowl).

Homeland Defense

NGA provides vital GEOINT that contributes to counterterrorism, counternarcotics, and border and transportation security efforts.

Our Mission

We provide GEOINT for our nation's security.

Our Vision

Know the Earth...Show the Way...Understand the World.

https://www.NGA.mil

REDDART
When In Doubt, Report It Out!

RED DART Alliance

Current RED DART Teams

* RED DART North Carolina * RED DART Southern Virginia * RED DART Huntsville * RED DART South Carolina * RED DART Central Virginia * RED DART Gulf Coast * RED DART Chicago * RED DART North Texas * RED DART North Mississippi * RED DART Indiana * RED DART Silicon Valley * RED DART South Florida * RED DART Tennessee * RED DART Sacramento * RED DART Greater Los Angeles * RED DART Colorado

- RED DART Southwest Ohio * RED DART Hawaii * RED DART San Diego * RED DART Japan * RED DART Portland * RED DART Seattle

The stated purpose of the RED DART program is to create a unified, cross-agency team of counterintelligence professionals dedicated to the protection of classified and sensitive technology research throughout a given area of responsibility (AOR). RED DART operates under a "shared leadership" principle, which allows each partner agency to own the program while being responsible and responsive to the other partner agencies.

New RED DART teams are forming regularly throughout the U.S. Contact your servicing Defense Counterintelligence and Security Agency (DCSA) CI agent or Federal Bureau of Investigation (FBI) CI agent to see if a team is being established in your area.