DEPARTMENT OF HOMELAND SECURITY
OFFICE of INTELLIGENCE and ANALYSIS

# THREAT PULSE

**JULY 2025 | HOMELAND THREAT PULSE**

We, at the Department of Homeland Security's Office of Intelligence & Analysis (DHS I&A), continually track threats to the Homeland that we are addressing in collaboration with our federal, state, local, tribal, territorial, and private sector partners.

This is the first in a series DHS I&A is publishing to help raise awareness of several threats to the nation DHS I&A is tracking. Welcome to the July 2025 Homeland Threat Pulse!

## Counterterrorism Brief

### Israel-Hamas conflict drives terrorism activity in the Homeland.

Since the October 7, 2023 attack by HAMAS, the Israel-HAMAS conflict has continued to inspire violence against targets in the Homeland, including Jewish or Israeli institutions and persons or targets perceived as supporting Israel. The perpetrators of many of these attacks used firearms or improvised incendiary devices, such as Molotov cocktails, and they often expressed grievances related to anti-Semitism or US foreign policy regarding the Israel-HAMAS conflict. These attacks have included the June 1 use of improvised incendiary devices to attack individuals attending a Boulder, Colorado, march in solidarity with Israeli hostages in Gaza and the May 21 shooting that killed two Israeli embassy staff members at an event in Washington, DC.

### Israel-Iran relations causing heightened threat environment.

Over the last month, we highlighted for federal, state, and local partners the likely Homeland threat implications of Israel and Iran's June conflict, US military involvement in this conflict, and recent rulings issued by Iranian religious leaders, which called for violence against Iran's alleged enemies in the United States and Israel. DHS I&A worked with our DHS partners to release the National Terrorism Advisory System (NTAS) Bulletin to provide the public with additional information about this evolving threat and resources to stay safe.

### Immigration enforcement grievances contributing to recent attacks and threats of violence.

Since January, individuals likely with immigration enforcement-related grievances have engaged in or threatened violence against DHS personnel, law enforcement partners, and organizations involved in or seen as supporting immigration enforcement efforts. In July, a group of individuals—with radios, tactical gear, shields, weapons and wearing all black—launched fireworks toward the Immigration and Customs Enforcement's (ICE) Prairieland Detention Center in Alvarado, Texas, vandalized vehicles located at the facility, and shot at ICE detention center personnel and responding law enforcement officers injuring one of the first responders. The same month a lone offender fired shots at law enforcement personnel and the entry doors of the US Border Patrol Rio Grande Valley Sector Annex in McAllen, Texas, but the attacker was unable to enter the facility before he was engaged by responding U.S. Border Patrol agents. Also, in April law enforcement arrested an individual in Texas who allegedly threatened on social media to shoot ICE agents and engage in violence against the Secretary of DHS, and in March there was an arson attack against a political party's building in New Mexico in which the alleged perpetrator also spraypainted "ICE=KKK" on an exterior wall.

## China Brief

**We are concerned with China's attempts to dominate the global critical minerals trade.**

China's investments in US mining operations could potentially threaten the independent supply of these minerals in the United States with possible long-term implications for our economic resilience and military readiness. The concentration of these minerals in select regions of our nation could make them attractive targets for China's exploitative trade practices. DHS reviews of transactions involving foreign investment in the United States could offer opportunities to disrupt these actions.

**DHS I&A is monitoring the threat of China-based technology firms that have stepped up their illicit export of signal jammers to the United States in recent years,** heightening the threat of criminal or terrorist use of these devices against US law enforcement or critical infrastructure. Since October 2020, CBP has seized over 2,300 jammers, 98 percent of which originated in China. Signal jammers are inexpensive, ranging from $50 to $5,000, and can be used to disrupt a range of radio frequency signals. Jamming can target any communications system that uses wireless radio frequency signals.

**China is an enduring threat to state and local critical infrastructure.**

China's cyber operations targeting US critical infrastructure pose an enduring threat to the IT networks of state, local, tribal, and territorial governments—many of which own or operate public utilities, particularly in the Energy and Water Wasterwater Systems Sectors. Of particular concern are China's cyber actors, publicly tracked as Volt Typhoon, who have been preparing for potential cyber attacks on these and other critical infrastructure networks in the event of a major crisis or conflict with the United States.

## Cyber Brief

**Ideologically motivated "hacktivists" generally pose persistent but low-level threats** to US critical infrastructure networks and websites. DHS I&A is concerned they may pursue minimally disruptive distributed denial-of-service attacks, website defacements, or other low-level activity in response to developments in the Middle East conflict. Other malicious cyber actors could also take advantage of regional developments, prompting the need for vigilance of US networks and adherence to the federal government's guidance on cyber hygiene and patching vulnerabilities.

## Cyber Brief (Continued)


**While ransomware attacks on the US Financial Services Sector, which includes banks, investment firms, and insurance firms, are fairly routine, attacks on US credit unions and other small monetary institutions tend to have outsized impacts** because of these institutions' limited budgets and reliance on third-party vendors for a range of IT services. Small monetary institutions serve over one in three Americans, and ransomware attacks on these entities frequently disrupt their services and expose the sensitive data of citizens across the country.


**Some ransomware actors are focused on stealing data rather than just extorting victims, complicating remediation efforts.**

Data theft has significant additional impacts for both the targeted organization and its customers, whose stolen data is frequently leveraged for identity theft, follow-on extortion, and other criminal activities. Organizations can better position themselves to mitigate the risk of data theft during ransomware attacks by using network defense solutions that rapidly identify network compromises and leverage help from US government cybersecurity and law enforcement agencies.

## Additional Briefs

**Foreign nationals smuggling hazardous biological materials into the United States threaten public safety and health.**

There have been several instances in the past year of Chinese nationals being charged for smuggling harmful biological materials into the United States. In some cases, the smuggled materials are classified in scientific literature as potential agroterrorism weapons. We continue to work alongside partners and Customs and Border Protection to mitigate risks associated with the illicit flow of hazardous biological materials into the Homeland.

**Threat actors target special events.**

In collaboration with our Intelligence Community and law enforcement partners, DHS I&A continues to assist in preparations for possible physical, cyber, and counterintelligence threats targeting special events and holidays. January 2025's New Year's Day vehicle-ramming terrorist attack in New Orleans is evidence that high-profile public events continue to be enduring terrorist targets.

## Stay Tuned

*Stay tuned for next quarter's edition.*