OFFICE *of* INTELLIGENCE *and* ANALYSIS

Homeland Threat Assessment

Homeland Security


EAST
20
E FRONT ST
LOUISIANA AVE


WITH HONOR AND INTEGRITY, WE WILL
SAFEGUARD THE AMERICAN PEOPLE,
OUR HOMELAND, AND OUR VALUES.

Table of Contents

PUBLIC SAFETY AND SECURITY 1

Terrorism 2

Illegal Drugs 6

Nation-States: Influence Operations and Transnational Repression 8

BORDER AND IMMIGRATION SECURITY 13

Migration and Watchlist Encounter Trends 14

Transnational Criminal Organizations 16

CRITICAL INFRASTRUCTURE SECURITY 21

Disruptive and Destructive Cyber Attacks Targeting Critical Infrastructure 22

Disruptive and Destructive Physical Attacks Targeting Critical Infrastructure 24

Intelligence Collection Against Critical Infrastructure Networks 25

THREATS TO ECONOMIC SECURITY 29

Economic Manipulation and Coercion 30

Economic Espionage and Influence 31

Definitions and Contextual Notes 33


WE STAND READY TO RISE AND FACE THE NEXT
CHALLENGE THAT THREATENS OUR HOMELAND.

Scope Note

The Office of Intelligence and Analysis of the Department of Homeland Security presents the 2025 Homeland Threat Assessment, which provides insights from across the Department and other homeland security stakeholders to identify the most direct, pressing threats to our Homeland during the next fiscal year (FY). This Assessment organizes evolving threats to homeland security missions arising from the dynamic terrorist threat, the increasing complexities straining the immigration system, transnational organized crime, proliferating cyber threats, and geopolitical strategic competition into four sections: Public Safety and Security, Border and Immigration Security, Critical Infrastructure Security, and Economic Security. This Assessment employs a traditional intelligence assessment format in which summary assessment paragraphs are followed by bullets with additional details that underpin the assessment.

We note that many of the threat actors and efforts addressed in this Assessment appear in multiple sections as they cut across mission areas and interact in complex and, at times, reinforcing ways. Throughout this Assessment, we also examine enduring issues, such as the development and proliferation of new technologies and climate change, which involve various mission areas and impact multiple threats. Definitions for terms and additional contextual notes are included at the end of this document.

Executive Summary

The Homeland faces a complex set of threats to our public safety, border security, critical infrastructure, and economy from violent extremists, transnational criminal organizations (TCOs), adversarial nation-states, and malicious cyber actors. These threats, while varied in scope and intended purpose, at times compound one another in unexpected ways, harming our communities and generating costly disruptions to the US economy. Meanwhile, technological advances, climate change, and natural disasters have the potential to exacerbate many of the aforementioned threats.

PUBLIC SAFETY AND SECURITY: Over the next year, the terrorism threat environment in the Homeland will remain high. We are particularly concerned about a confluence of factors this year, including violent extremist responses to domestic sociopolitical developments—especially the 2024 election cycle—and international events that domestic and foreign violent extremists likely will use to justify or encourage attacks in the Homeland. Lone offenders and small groups continue to pose the greatest threat of carrying out attacks with little to no warning. Meanwhile, foreign terrorist organizations (FTOs) and their supporters will maintain their enduring intent to conduct or inspire attacks in the Homeland.

In addition, the production, trafficking, and sale of illegal drugs by transnational and domestic criminal actors will continue to pose the most lethal threat to communities in the United States. Fentanyl and other synthetic opioids remain the most lethal of drugs trafficked into the country, but small increases in overdoses linked to cocaine and methamphetamine highlight the danger from other drug types.

We expect the Homeland also will face threats to public safety from state actors using subversive tactics in an effort to influence and divide the American public and undermine confidence in our institutions. Many of these actors—in particular, the People's Republic of China (PRC)—also target ethnic and religious minorities, political dissidents, and journalists in the United States to silence and harass critical voices, violating our sovereignty and the rule of law.

The 2024 election cycle will be an attractive target for many adversaries. Some domestic violent extremists (DVEs) likely view a wide range of targets indirectly and directly associated with elections as viable targets for violence with the intent of instilling fear among voters, candidates, and election workers, as well as disrupting election processes leading up to and after the November election. Nation-state-aligned foreign malign influence actors almost certainly will continue to target democratic processes with the aims of affecting US voter preferences, exacerbating social tensions, and undermining confidence in our democratic institutions and the integrity of the electoral process.

BORDER AND IMMIGRATION SECURITY: Migrant encounters at our border have declined over the last year, but migrants are still arriving in high numbers, complicating border and immigration security. As overall encounters have declined, so too have encounters with individuals in the Terrorist Screening Data Set, also known as the "terrorism watchlist," which includes individuals associated with information indicating they may be directly engaged in or supporting terrorist activities as well as known associates of watchlisted individuals, such as family members. For several years prior to this year's decline, terrorism watchlist encounters had increased, a trend consistent with the overall increase in migrant encounters at the southwest border.

CRITICAL INFRASTRUCTURE SECURITY: Domestic and foreign adversaries almost certainly will continue to threaten the integrity of our critical infrastructure with disruptive and destructive cyber and physical attacks, in part, because they perceive targeting these sectors will have cascading impacts on US industries and our standard of living. The PRC, Russia, and Iran will remain the most pressing foreign threats to our critical infrastructure. Most concerningly, we expect the PRC to continue its efforts to pre-position on US networks for potential cyber attacks in the event of a conflict with the United States. Nation-states, criminal hacktivists, and financially motivated criminals will likely hone their techniques to disrupt US services or to conduct espionage focused on gaining access to US networks, including critical infrastructure entities. We assess that domestic and foreign violent extremists will continue to call for physical attacks on critical infrastructure in furtherance of their ideological goals and, at times, in response to international conflicts and crises.

ECONOMIC SECURITY: Multifaceted and diverse economic threats—primarily from the PRC—will likely continue to harm US producers and consumers and degrade the competitiveness and future health of US companies and industries. The PRC likely will remain our greatest economic security threat because of its aggressive use of anticompetitive, coercive policies and theft of US intellectual property, technology, and trade secrets. Lastly, we expect our supply chains will remain vulnerable to foreign manipulation abroad, which could harm global productivity and consumer demand.

PUBLIC SAFETY AND SECURITY

Overview: *Within this section, we examine lethal threats to the Homeland from terrorism and illegal drugs, and national security threats from nation-state efforts to malignly influence US audiences and suppress critical voices.*

Over the next year, domestic and foreign violent extremist actors, the harmful effects of illegal drugs, and adversarial states seeking to exacerbate our divisions as well as silence criticism from diaspora communities will pose a threat to public safety and security in the Homeland. Specifically, we expect the terrorism threat environment in the United States over the next year will remain high due to a confluence of factors. These factors include violent extremist responses to domestic sociopolitical developments and the 2024 election cycle, the enduring intent of FTOs to conduct or inspire attacks in the Homeland, and the galvanizing effect that successful terrorist attacks abroad and the ongoing conflict in the Middle East have had on a range of violent actors.[1,2] Despite the lethal and destabilizing threat terrorism poses to our country, the production, trafficking, and sale of illegal drugs by transnational and domestic criminal actors remain the most lethal and persistent threats to US communities. Concurrently, adversarial states are intent on sowing distrust in our institutions, as well as confusion and division in our communities, through their malign influence campaigns, with some actors seeking to boost these efforts during the 2024 election cycle. These state actors also violate our rule of law and undermine freedom of speech in their efforts to suppress dissidents living in the United States. *(For more information on threats to the 2024 US election cycle, see page 10.)*

Terrorism

Looking into 2025, the threat of violence from US-based violent extremists—including DVEs who are motivated by various ideologies and FTO-inspired homegrown violent extremists (HVEs)—will remain high.[3,4] The threat will continue to be characterized primarily by lone offenders or small cells motivated to violence by a combination of racial, religious, gender, or anti-government grievances; conspiracy theories; and personalized factors.[5,6] We particularly are concerned about the likelihood of violence motivated by developing domestic and global events, including the 2024 election cycle and the ongoing Israel-HAMAS conflict. A number of violent extremists embrace multiple, sometimes competing motivations, challenging our ability to identify their potential targets in advance because their pre-attack statements online are often unrelated or only loosely related to the targets they ultimately choose.

- Between September 2023 and July 2024, DVEs driven by various anti-government, racial, or gender-related motivations have conducted at least four attacks in the Homeland, one of which resulted in a death.[7] US law enforcement disrupted at least seven additional DVE plots. Two HVE attacks, partially motivated by the Israel-HAMAS conflict, also occurred during this timeframe, and law enforcement disrupted at least three other HVE plots.
- Over the last year, DVE efforts have focused on a range of targets, including ethnic and religious minorities, government officials, and ideological opponents, while HVEs have mostly targeted faith-based organizations. Some of these incidents focused on less secure targets, like houses of worship, a store, and a university. DVEs motivated by various ideologies have also used online messaging to increasingly promote the swatting and doxxing of ideological opponents, including public and private officials at their residences.[8] Other DVE-related violent threats have targeted court officers associated with divisive sociopolitical cases; migrants and government officials linked to immigration grievances; and Jewish, Muslim, and Arab communities, partly in response to the Israel-HAMAS conflict.
- DVEs and HVEs will continue to be influenced by sociopolitical drivers emphasized in popular discourse, particularly those related to current events, which are used to amplify existing narratives and justify violence. HAMAS's terrorist attack against Israel on 7 October 2023 and the subsequent conflict between Israel and HAMAS and its regional allies have spurred violent extremists across the ideological spectrum to promote attacks against Jewish, Muslim, Christian, and Arab communities in the United States. These events will likely be referenced in FTOs' official and unofficial messaging and contribute to the radicalization and mobilization of US-based individuals to violence into at least 2025.[9]

Targeted Violence

In contrast to DVE and HVE attacks, most mass casualty attacks in the Homeland over the last year were not motivated by an ideology, but were rather associated with suspected or confirmed mental illness or driven by relationship grievances; however, these factors alone are not diagnostic indicators of likely violence.[10] Over the last year, at least eight mass casualty attacks primarily motivated by reasons other than an ideology have occurred in the United States, killing at least 38 and injuring 68. Individuals acting alone conducted most of these attacks while using firearms and targeting commercial and education facilities. At least one of these attackers cited the 1999 Columbine School shooting as inspiration, suggesting that tragic incident will continue inspiring threat actors in the years to come.

FTOs, like ISIS and al-Qa'ida, maintain the enduring intent to conduct or inspire attacks in the Homeland and have leveraged the conflict in the Middle East to reaffirm this intent. These organizations maintain worldwide networks of supporters that could target the Homeland. FTO media outlets promote violent rhetoric intended to inspire US persons to mobilize to violence, while foreign terrorists continue engaging online supporters to solicit funds; create and share media; and encourage followers to attack the Homeland, US interests, and what they perceive as the West. Additionally, individuals with terrorism connections are interested in using established travel routes and perceived permissive environments to facilitate their access to the United States. *(For more information on terrorist watchlist encounters at the US border, see page 15.)* Among state actors, we expect Iran to remain the primary sponsor of terrorism and continue its efforts to advance plots against individuals—including current and former US officials—in the United States.

- Following ISIS's loss of territorial control in the Middle East in 2019 and three of its most senior leaders in 2022, ISIS's branches have taken a greater role in conducting operations on behalf of the group. ISIS-Khorasan (ISIS-K)—ISIS's regional branch in Afghanistan and Pakistan—has been increasingly active outside of Afghanistan this year and will likely try to capitalize on its notable 2024 attacks in Iran and Russia to recruit followers in the Homeland and the West, as well as inspire individuals to mobilize to violence. These attacks, which killed more than 95 and 140 people, respectively, were the first major attacks conducted outside of the group's traditional operating area in several years, and were the most recent examples of ISIS-K's successful recruitment of Central Asian supporters for attacks abroad. ISIS-K's online media, particularly its multilingual *Voice of Khurasan* magazine, continues to emphasize the group's intent to reach global audiences and galvanize supporters among Central Asian communities, including diaspora populations in other countries. ISIS online media groups have also used the Israel-HAMAS conflict to encourage attacks against the West and Jewish and Christian communities, and ISIS media outlets have capitalized on recent attacks in Europe to inspire more violent action.

- Al-Qa‘ida remains committed to striking the Homeland and has reinvigorated its outreach to Western audiences. In December 2023, al-Qa‘ida’s affiliate in Yemen released its first *Inspire*-branded video and the first *Inspire* publication since 2021, which encouraged attacks against civil aviation and prominent individuals, urged retaliation against the West for supporting Israel, and provided bomb-making instructions. Al-Qa‘ida has also been inspired by the HAMAS attack against Israel and directed its supporters to conduct attacks against the Homeland, Jewish targets, and Israel.
- Iran maintains its intent to kill US government officials it deems responsible for the 2020 death of its Islamic Revolutionary Guards Corps (IRGC)-Qods Force Commander and designated foreign terrorist Qassem Soleimani. In August 2024, a Pakistani national with ties to Iran was indicted for a planned assassination of US government officials. In June 2023, the US Department of the Treasury designated six IRGC members for their role in assassination plots targeting former US government officials, dual US and Iranian nationals, and Iranian dissidents.

Chemical, Biological, Radiological, and Nuclear (CBRN) Threats To Endure

We expect predominantly aspirational and rudimentary interest in CBRN attacks will continue in 2025. Among foreign and domestic threat actors, we assess that DVEs and criminals will remain the most likely perpetrators of deliberate CBRN-related attacks. Over the last year, there were 18 known deliberate chemical- or biological-related incidents in the Homeland, four of which were linked to political or ideological motives while the rest were criminal in nature. All of the incidents employed simple methods, and one incident caused at least one death. Two of the 18 incidents involved the alleged use of ricin, while 14 of the incidents employed easily obtainable chemicals—including a range of pesticides, chlorine, bear spray, and other chemical irritants. Fentanyl was weaponized in two instances. Foreign and domestic threat actors maintain aspirational interest in radiological and nuclear attacks, but these attacks remain unlikely.

We expect threat actors will continue to explore emerging and advanced technologies to aid their efforts in developing and carrying out chemical and biological attacks. Over the last year, foreign and domestic extremists online expressed interest in using DNA modification to develop biological weapons to target specific groups. We remain concerned about the potential exploitation of advances in artificial intelligence (AI) and machine learning to proliferate knowledge that supports the development of novel chemical or biological agents. *(For more information on AI and threat actors, see pages 26–27.)* Such advances could be exploited by state and state-sponsored adversaries, but the necessary expertise for such exploitation most likely exceeds that of most nonstate actors. We also remain concerned about the potential for threat actors to use unmanned aircraft systems (UAS) in chemical or biological attacks due to the continued advancement of UAS technology and the growing availability of UAS.

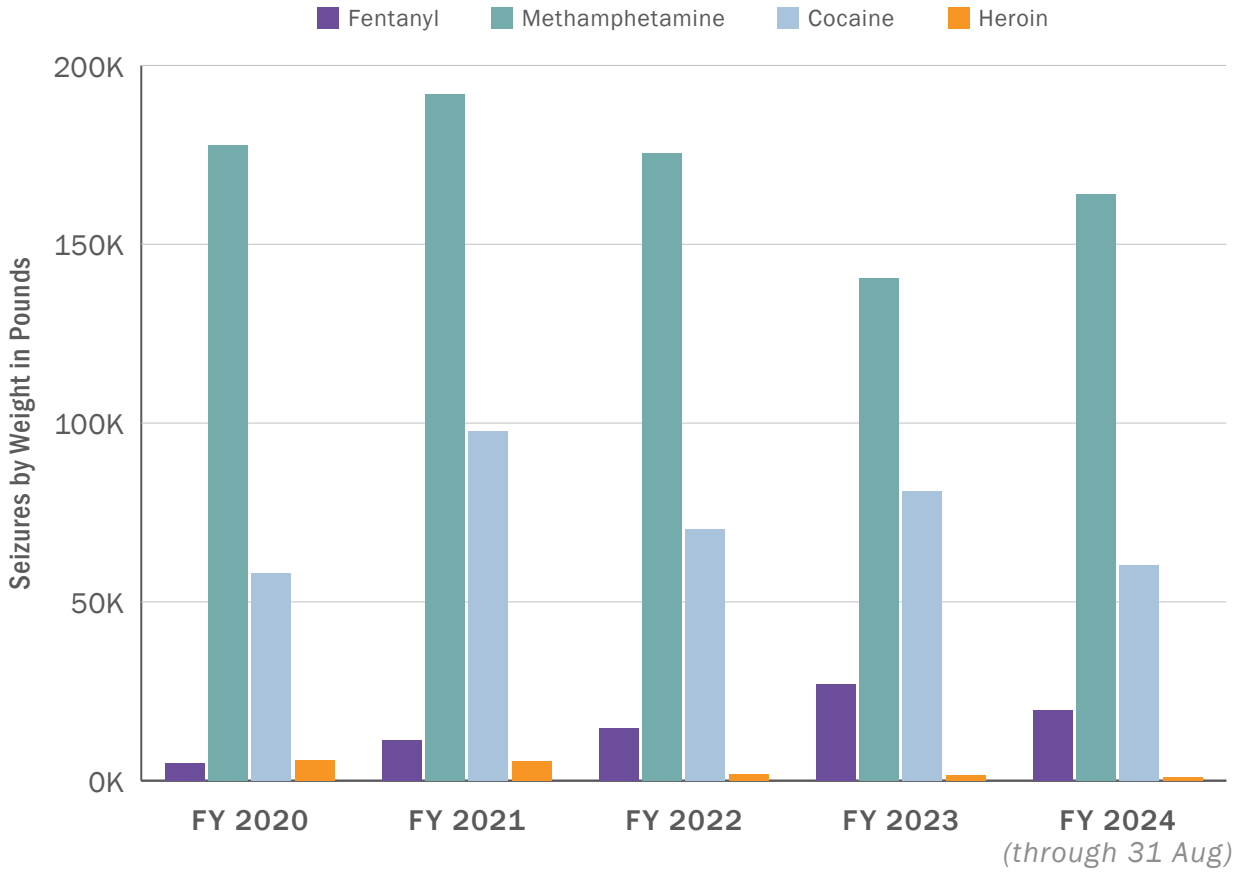
Illegal Drugs

We expect illegal drugs smuggled into and sold in the United States will continue to kill more Americans than any other harmful security threat. Drug consumption kills tens of thousands of Americans each year, although drug overdoses tracked by the Centers for Disease Control and Prevention declined in 2023 for the first time since 2018. While fentanyl seizure volumes are significantly below those of methamphetamine and cocaine, fentanyl remains a top concern due to its potency, lethality, and availability.[11] Fentanyl seizures have declined this year from record high seizures in FY 2023, but still remain elevated. DHS still seized enough fentanyl to kill the entire American population many times over. Criminal actors and criminal drug manufacturers are responding to increased US and partner nation efforts targeting the precursor chemicals needed for fentanyl production by modifying existing chemicals and substituting different chemicals in their drug compositions. Criminals also are adapting their smuggling methods to circumvent US customs regulations aimed at blocking the import of these chemicals and drug manufacturing equipment into the United States. US Customs and Border Protection (CBP) in FY 2024 year-to-date has also seized more methamphetamine at the US-Mexico border than in all of FY 2023, and we noted small increases in overdoses related to both cocaine and methamphetamine.

- We expect US-bound fentanyl smuggling and seizures to remain high into 2025 as Mexico-based TCOs seek to meet user demand and the drug remains profitable. So far into FY 2024, CBP and US Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) seizures of fentanyl and pill presses—which traffickers use to make toxic drug mixtures that often include fentanyl—have declined compared to 2023, but still remain elevated. In the first 10 months of FY 2024, DHS seized over 27,000 pounds of fentanyl, compared to the over 43,000 pounds seized in 2023, a decline of nearly 40 percent. In this same timeframe, DHS seized 2,200 pill presses bound for the United States, down from the 3,600 pill presses seized in 2023. We note that seizure totals alone are not necessarily reflective of drug flow volumes.
- The Sinaloa Cartel and New Generation Jalisco Cartel, two large Mexico-based TCOs, remain the primary smugglers of fentanyl, methamphetamine, cocaine, and heroin into the United States.[12] These TCOs and others almost certainly will continue to rely on their vast illicit networks to obtain chemicals and finished drugs for the illicit US drug market. *(For more information on TCO exploitation of the US border, see page 16.)* Primarily US-based traffickers are also increasingly augmenting their fentanyl-related products with additives, such as xylazine, and fentanyl alternatives, such as nitazenes—both of which are sourced from China-based firms. Nitazene can be 10 times more potent than fentanyl alone. These addictive, inexpensive fentanyl combinations and alternatives increasingly contribute to overdoses in the Homeland.

- China-based companies that supply chemical precursors and pill pressing equipment, and the drug traffickers that seek to acquire these drug supplies, continue to adapt and use alternative routes and chemical compounds to mitigate increased US and third-country law enforcement efforts targeting the sale and import of these items. For example, this year, China shut down 25 companies selling fentanyl precursors and sent a warning to its pharmaceutical industry, which prompted suppliers to change tactics, such as modifying customs labeling on packages to avoid scrutiny. In 2024, traffickers increasingly used South Korea as an alternative transit point en route to Mexico or the United States in an attempt to obscure the origins of pill pressing equipment and evade law enforcement interdictions.
- In FY 2024, CBP seizures of methamphetamine have surpassed amounts seized in FY 2023, and we expect this will continue into the next year. Meanwhile, cocaine seizures remain high relative to other drugs but below totals for FY 2023. Drug traffickers will continue to produce and smuggle these drugs to meet sustained US consumer demand as long as they remain lucrative for TCOs. In contrast to overall overdose numbers, overdoses linked to methamphetamine and cocaine increased about 4 percent in 2023, in part due to consumer co-use of these drugs with fentanyl. In 2025, we expect that drug traffickers will continue to adulterate cocaine and methamphetamine to make them more potent and addictive.

CBP Border Seizures of Fentanyl, Methamphetamine, Cocaine, and Heroin FY 2020–2024



24-385-IA

Nation-States: Influence Operations and Transnational Repression

We expect state actors will continue to pose a host of threats to the Homeland and public safety. Specifically, China, Iran, and Russia will use a blend of subversive, undeclared, criminal, and coercive tactics to seek new opportunities to undermine confidence in US democratic institutions and domestic social cohesion. Advances in AI likely will enable foreign adversaries to increase the output, timeliness, and perceived authenticity of their mis-, dis-, and malinformation designed to influence US audiences while concealing or distorting the origin of the content.[13] *(For more information on the use of AI by threat actors, see pages 26–27; for more on influence operations against the 2024 US election cycle, see pages 10–11.)*[14]

- Russia likely will continue to use traditional state-sponsored media, inauthentic websites, social media networks, online bots, trolls, and individuals to amplify pro-Kremlin narratives and conduct information operations targeting the United States. For example, over the past year, Russian influence actors have amplified stories regarding US migration flows to stoke discord in the United States. One Russian malign influence campaign used generative AI to create current event news articles on inauthentic websites designed to appear as recognizable Western and US-based media outlets.[15]
- Since its 2022 invasion of Ukraine, Russia's information operations have focused on justifying its actions and seeking to reduce US domestic and Western support for Kyiv. In support of these efforts, Moscow is also leveraging "influence-for-hire" firms—allegedly independent, nongovernment-linked entities—likely to reach larger US audiences and bolster operational security by concealing Moscow's ties with these firms' promotion of pro-Kremlin narratives.
- Iran is becoming increasingly aggressive in its foreign influence efforts, seeking to stoke discord and undermine confidence in our democratic institutions. Over the last year, Iranian information operations have focused on weakening US public support for Israel and Israel's response to the 7 October 2023 HAMAS terrorist attack. These efforts have included leveraging ongoing protests regarding the conflict, posing as activists online, and encouraging protests. Prior to the 2020 US presidential election, Iran also attempted to amplify divisive narratives to incite violence, influence the US electorate, and degrade trust in the electoral process.
- The PRC largely focuses its influence operations on discrediting the US government and enhancing Beijing's global standing. To this end, it is improving its ability to develop, tailor, and disseminate disinformation using increasingly sophisticated tactics and technologies, including AI. For example, AI has enabled Beijing to improve the authenticity of social media accounts used in disinformation campaigns. The PRC is also conducting information operations targeting US disaster response operations, which could impact recovery activities and place emergency management personnel, facilities, and survivors at risk. PRC disinformation campaigns that seek to exploit US disasters, as when it blamed the Hawaii wildfires on US military activity, may also reduce trust in US institutions and officials and dissuade survivors from pursuing federal recovery response and support. *(For more information on the PRC's disinformation efforts, see pages 11 and 26.)*

Nation-states also continue to engage in transnational repression activity targeting ethnic and religious minorities, political dissidents, and journalists in the United States.[16] We expect China and Iran to remain the foremost transnational repression threats in the United States.

- The PRC continues its efforts to control and silence dissent and criticism abroad of the Chinese Communist Party and its General Secretary, Xi Jinping. In March 2024, the Department of Justice (DOJ) indicted seven China-based Chinese nationals for their involvement in a PRC-backed criminal hacking group targeting US-based critics, businesses, and political officials with malicious cyber operations intended to intimidate and silence dissidents and steal from their businesses. This group has been active for approximately 14 years, demonstrating the PRC's commitment to monitoring and targeting US and foreign critics and bolstering our confidence that the PRC will continue to pursue perceived enemies in the Homeland.
- Iran almost certainly will continue to target US-based Iranian dissidents because Iran views their anti-regime activities as an existential threat. In the past several years, Iran has used US persons, Iranian diaspora members, and third-country nationals to surveil, harass, and intimidate regime dissidents. Iran's use of violence—to include murder—against US-based regime opponents since the early days of the Iranian Revolution, and the regime's global persecution of opponents, strengthens our assessment that it will continue to pursue dissidents in the Homeland.

Threat Actors Likely To Focus on 2024 Election Cycle

Our electoral processes are an attractive target for threat actors, and we expect many will seek to influence the 2024 election cycle, while some others may seek to access or interfere with election systems. While law enforcement is still investigating the motives behind the apparent assassination attempts on a former US President, these incidents highlight the magnitude of the threat surrounding the election cycle. Some DVEs, particularly those motivated by anti-government or partisan issues, will likely view a wide range of targets indirectly and directly associated with elections as viable targets for violence with the intent of instilling fear among voters, candidates, and election workers, as well as disrupting election processes leading up to and after the November election. Foreign malign influence actors almost certainly will target democratic processes across federal, state, and local governments, aiming to affect US voter preferences, exacerbate social tensions, and undermine confidence in our democratic institutions and processes, including election operations. Separately, foreign state-affiliated cyber actors and cyber criminals almost certainly view network infrastructure that supports US elections as attractive targets. There is no reporting, however, to suggest that foreign adversary targeting of such systems has ever prevented an eligible voter from casting a ballot, compromised the integrity of any ballots cast, or disrupted the ability to tabulate votes or transmit election results in a timely manner.

- We expect DVEs will pose the most significant physical threat to government officials, voters, and elections-related personnel and infrastructure, including polling places, ballot drop box locations, voter registration sites, campaign events, political party offices, and vote counting sites. In particular, anti-government or anti-authority DVEs, many of whom likely will be inspired by partisan policy grievances or conspiracy theories, will pose the most significant threat. We have also recently observed a rise in disruptive tactics targeting election officials and offices—like those observed in past election cycles—including hoax bomb threats, swatting, doxxing, and mailing white powder letters, intended to instill fear and disrupt campaign and election operations. We remain concerned that the use of these tactics will increase particularly as we approach Election Day, with the intent of disrupting voting and ballot counting processes. Some DVEs could also react violently should their preferred candidate lose, or they could seek to exploit possible civil unrest if there are perceptions of election fraud.
- Online users in forums frequented by some DVEs have increasingly called for violence linked to the 2024 election cycle and seek to promote violence in response to politically and socially divisive topics, like immigration, abortion rights, and LGBTQIA+ issues or significant current events. We expect DVEs will continue to rely on these issues to justify violence and promote their causes into the coming year.

- As the election approaches, we expect foreign malign influence actors to increase their overt and covert use of media outlets, networks of inauthentic social media accounts, and agents of influence to launder and spread their preferred narratives and further their election-related goals. We are beginning to see Russia target specific voter demographics, promote divisive narratives, and denigrate specific politicians. Russia seeks to shape electoral outcomes, undermine electoral integrity, and amplify domestic divisions, while using a variety of approaches to bolster its messaging and lend an air of authenticity to its efforts. Iran, meanwhile, perceives this year's elections as particularly consequential for its own national security interests, and we have observed increasingly aggressive Iranian activity during this election cycle, specifically involving influence operations targeting the American public and cyber operations targeting presidential campaigns. Iran, the PRC, and Russia have also increasingly used generative AI to create more believable text, inauthentic synthetic audio, and video that may enhance their ability to reach US audiences while hiding their origins.[17]
- US election infrastructure—including voter registration databases and associated information technology (IT) infrastructure and systems—may be targeted by a broad swath of opportunistic malicious cyber actors. These critical elections components and systems typically hold sensitive personally identifiable information of US persons, much of which may also be publicly or commercially available, that could be used to facilitate follow-on foreign malign influence campaigns or other illicit activity. Financially motivated cyber criminals may penetrate and steal information from these systems to sell online or use the information obtained for other illicit or criminal purposes like fraud, scams, or additional cyber operations. Malicious cyber actors are also likely to employ election-themed spear-phishing—targeted phishing—and smishing—phishing using text messages—against individuals like election workers, political party and campaign staff and volunteers, and state and local government employees to gain access to networks of interest, including election-related targets, to collect intelligence or other sensitive information.[18] The Intelligence Community is confident that Iranian actors have—through social engineering and other efforts—sought access to individuals with direct access to the presidential campaigns of both political parties. Such activity, including thefts and disclosures of information, are intended to influence the US election process. Iran and Russia have used these tactics not only in the United States during this and prior federal election cycles, but also in other countries around the world.


U.S. COAST

BORDER AND IMMIGRATION SECURITY

Overview: *Within this section, we examine the threats posed by TCOs, terrorists, and other threat actors seeking to exploit our borders and migration system. The complex irregular migration trends complicate our ability to identify and thwart these threats.*

The challenging border and immigration security trends we have faced over the last several years are likely to continue. Encounters with migrants have declined from monthly record highs in December 2023, with US-Mexico border encounters in July reaching the lowest monthly encounters in over three years. Still, the factors that have driven the surge in migration numbers, including persistently poor economic, social, and political conditions in migrants' home countries and the relative strength of the US economy, remain in place. As part of this flow of migrants, we are also encountering individuals in the Terrorist Screening Data Set, known as the "terrorist watchlist." Individuals on this list are associated with information indicating they may be directly engaged in or supporting terrorist activities as well as known associates of watchlisted individuals. Inclusion on the list triggers increased scrutiny when such an individual is encountered during the immigration process. TCOs similarly exploit this complex environment to smuggle deadly drugs across our borders, often through ports of entry, and to extort and mislead migrants seeking to enter the United States. We expect TCOs will continue to evolve their tactics, use new technologies, and work to corrupt and undermine our partner nations' security forces and rule of law.

Migration and Watchlist Encounter Trends

While FY 2024 year-to-date overall migrant encounters at the US-Mexico border remain high compared to pre-pandemic historical trends, monthly encounters have declined since December 2023 and, as of July, were the lowest in over three years.[19] This trend is probably explained, in part, by increased Mexican enforcement efforts and migrant reactions to shifts in US asylum policy. As in FY 2023, migrants continue to come from a broader set of countries than in years past, often leveraging other countries' lax visa policies to enter the Western Hemisphere en route to the United States. Migration often results from a complex mix of factors, including persistently poor economic, social, and political conditions in migrants' home countries and the relative strength of the US economy. Factors that could impact and cause fluctuations in migrant encounters over the next year include real or perceived changes in US or regional immigration policy, as well as unforeseen events that change conditions in home, host, and transit countries.

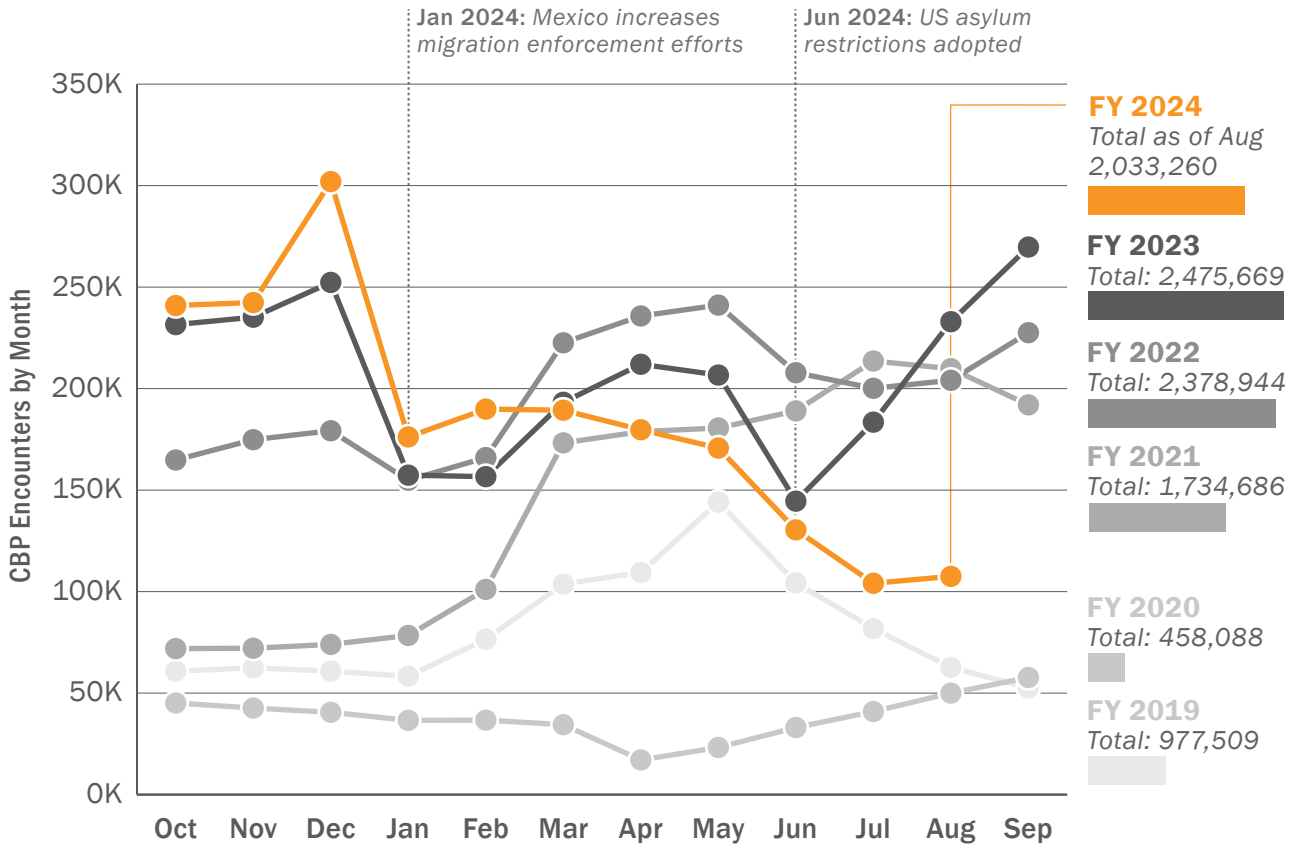
- Encounters at the US-Mexico border peaked in December 2023—probably due, in part, to a brief pause in Mexican enforcement measures—before declining throughout 2024 after Mexico restored and heightened these enforcement measures. Following US policy changes in June 2024, which restricted asylum eligibility and increased the consequences for crossing the border without authorization, public posts online suggested that prospective migrants perceived an increased risk of repatriation, which probably drove further decreases in migrant encounters and spurred more migrants to seek lawful pathways to enter the United States. Encounters with migrants from Eastern Hemisphere countries—such as China, India, Russia, and western African countries—in FY 2024 have decreased slightly from about 10 to 9 percent of overall encounters, but remain a higher proportion of encounters than before FY 2023.
- Over the next year, we expect migrant reactions to real or perceived changes in both US and regional immigration policies to influence some potential migrants' decisions to attempt irregular entry into the United States. In July, some US-bound migrants told news media that they hoped to reach the US-Mexico border before the 2024 election, perceiving that a change in administration might result in border closures and the end of CBP One appointments. Misinformation—sometimes peddled by human smugglers—about changes in immigration policy can prompt sudden influxes of migrants to the border with little warning.
- While the US-Mexico border remains the primary destination for irregular migration, migrant encounters along the US-Canada border continue to increase, with over 181,000 migrant encounters in FY 2024 through August, compared to about 170,000 encounters at the same time in FY 2023. US Coast Guard maritime migrant interdictions have dropped significantly, with only 3,132 migrants interdicted in FY 2024 through August compared to 12,128 in the same timeframe in FY 2023.

Over the next year, we expect some individuals with terrorism ties and some criminal actors will continue their efforts to exploit migration flows and the complex border security environment to enter the United States. *(For more information on terrorist threats, see pages 2–4.)*

- Individuals with potential terrorism connections continue to attempt to enter the Homeland at both the US-Mexico and US-Canada borders and also through the immigration system. Encounters with individuals in the Terrorist Screening Data Set at both borders have declined since January 2024, after increasing each year since FY 2021 as overall migration increased. The Terrorist Screening Data Set includes individuals directly engaged in or supporting terrorist activities as well as known associates of watchlisted individuals, such as family members. Through July of FY 2024, approximately 139 watchlisted individuals have been encountered at the US-Mexico border, most of whom attempted to illegally enter the United States between ports of entry; this number has decreased from 216 during the same timeframe in FY 2023. Through July of FY 2024, CBP encountered 283 watchlisted individuals at the US-Canada border, down from 375 encountered during the same timeframe in FY 2023. In contrast to the US-Mexico border, many watchlist encounters along the US-Canada border occur at ports of entry, and the vast majority of these individuals have legal status in Canada. These numbers reflect CBP's Terrorist Screening Data Set encounters with all nationalities, including US persons, at and between ports of entry at the US-Canada and US-Mexico borders.

CBP Migrant Encounters at US-Mexico Border FY 2019–August FY 2024

Following record migrant encounters in December 2023, encounters decreased in the months after Mexico increased migration enforcement efforts. Encounters decreased further in the summer, following migrant reactions to new US restrictions on asylum for noncitizens who unlawfully cross the border. These encounters include CBP One appointments.



Transnational Criminal Organizations

Mexico-based TCOs will continue to exploit the complex security environment at the US border to smuggle drugs and migrants to and across our border. As in past years, these groups use violence, coercion, and bribery in Mexico to protect and expand their revenue streams and access US border crossings; they also continually develop new tactics and use new technologies in their efforts to evade border security efforts. *(For more information on the impact of illicit drugs on the Homeland, see pages 6–7.)*

- Mexico-based TCOs, to include cartels and human smuggling organizations, will almost certainly continue to smuggle irregular migrants across the US-Mexico border. TCOs based in Mexico use human smuggling and migrant extortion to supplement their other major revenue streams, such as drug smuggling and kidnapping. Independent human smugglers in Mexico and in Latin America are also spreading misinformation online to prey on migrants' hardships and provide travel guidance promising entry into the United States.
- Mexico-based TCOs will also continue to attack, kidnap, and murder rivals and Mexican security officials—as they did during Mexico's 2024 presidential election cycle—to consolidate control over lucrative smuggling routes to and along the US-Mexico border. In addition to violence, we also expect cartels to exploit a variety of surveillance tactics to protect their smuggling operations, including incorporating advanced technological tools. For example, cartels use drones to surveil US law enforcement along the southwest border and to inform their decisions on smuggling operations.
- TCOs, besides those based in Mexico, are also exploiting the US border for drug smuggling. For example, since at least 2016, Honduran nationals have expanded their narcotics trafficking operations in the western United States, using their relationships with Mexico-based TCOs to source drugs. Between January 2022 and October 2023, Honduran drug trafficking cells began distributing Sinaloa Cartel-sourced fentanyl pills and powder across the region. Prior to 2022, these traffickers primarily distributed heroin, cocaine, and methamphetamine.
- While TCOs based in Mexico move large amounts of drugs over the US-Mexico border—mainly through land ports of entry—we also expect cocaine trafficking to the Homeland via the maritime domain—particularly through South and Central America and the Caribbean—to remain high in 2025. Mexico-based TCOs very likely will continue to use their partnerships with TCOs in Ecuador and Colombia to direct cocaine shipments toward the United States via this domain.

Human Trafficking

Human trafficking—specifically sex trafficking and forced labor—imposes physical, psychological, and financial harm to trafficking victims and impacts border security, public safety and health, and the US economy.[20,21] Human traffickers continue to exploit victims domestically and internationally, including child victims of exploitation. There have been reported cases of human trafficking in all US states, territories, and jurisdictions. *(For more information on the impacts of forced labor on the US economy, see page 30.)*

- Transnational sex trafficking organizations within the United States continue to use various businesses, such as illicit massage businesses, bars and nightclubs, and private brothels, as well as online venues, such as commercial sex websites, to conduct illegal activities that earn them approximately $2.5 billion annually. There are human trafficking networks from Central and South America, Eastern Europe, and Asia involved in trafficking operations across several US jurisdictions.
- Social media platforms almost certainly will continue to serve as a "digital hunting field" for traffickers to "groom" and recruit potential victims and reach customers. Traffickers also capture victims' online identities to monitor their online activities.
- Forced labor through domestic servitude at private residences or businesses is a rapidly evolving threat in the Homeland that victimizes vulnerable populations while often posing minimal risk to traffickers. Foreign domestic workers are particularly vulnerable to abuse due to their immigration status, language and cultural barriers, and lack of community ties.


CBP
FIELD OPERATIONS
FEDERAL OFFICER

CRITICAL INFRASTRUCTURE SECURITY

Overview: *Within this section, we examine physical and cyber threats from domestic and foreign actors—including terrorists, adversarial nation-states, and nonstate actors—to the resources, assets, and structures of our critical infrastructure sectors. Critical infrastructure provides the goods and services that are the backbone of our national and economic security and the well-being of all Americans. Lifeline sectors—such as the telecommunications, energy, transportation, and water and wastewater sectors—are vital to national essential and critical functions.*

Over the next year, domestic and foreign adversaries almost certainly will continue to threaten the integrity of US critical infrastructure, in part, because they perceive targeting these sectors would have cascading impacts on US industries and our standard of living. We are particularly concerned about the credible threat from nation-state cyber actors to US critical infrastructure. The PRC continues its efforts to pre-position on US networks for potential cyber attacks in the event of a conflict with the United States. Further, a range of adversarial foreign cyber actors are honing their techniques to disrupt US services or to conduct espionage focused on gaining access to US networks and stealing sensitive information. Separately, DVEs and FTOs are calling for physical attacks on critical infrastructure in furtherance of their ideological goals and, at times, in response to international conflicts.

Disruptive and Destructive Cyber Attacks Targeting Critical Infrastructure

We are facing an evolving landscape of threats from highly sophisticated nation-state cyber actors; ideologically motivated criminal hacktivists who have, up to now, conducted only nuisance-level attacks;[23] and financially motivated cyber criminals who opportunistically and relentlessly pursue profits. We expect adversarial state cyber actors will continue to seek access to, or to pre-position themselves on, US critical infrastructure networks. In particular, PRC state-sponsored actors could exploit such access or pre-positioning for cyber attacks in the event of an imminent conflict or periods of heightened tensions and potentially disrupt critical functions that support our economy, critical services, and way of life—possibly including continuity of government. Cyber actors working for or sympathetic to our adversaries, and who are opposed to US support to our international partners, have launched sporadic attacks on US critical infrastructure. Specifically, ongoing conflicts in Ukraine and Gaza have given rise to a range of ideologically motivated criminal hacktivists and adversarial state-affiliated actors conducting cyber attacks against US critical infrastructure.

- PRC state-sponsored cyber actors have pre-positioned cyber exploitation and attack capabilities for disruptive or destructive cyber attacks against US critical infrastructure in the event of a major crisis or conflict with the United States. One PRC state-sponsored cyber campaign, publicly known as Volt Typhoon, gained access to the IT environments of multiple critical infrastructure organizations over the last several years and continues to target US critical infrastructure. These compromises have been primarily lifeline sectors, including the communications, energy, transportation, and water and wastewater sectors, in the Homeland and US territories. The Cybersecurity and Infrastructure Security Agency and other government agencies assess that Volt Typhoon actors are pre-positioning themselves on IT networks to enable lateral movement to operational technology (OT) assets to disrupt functions.[22] Volt Typhoon's use of victims' legitimate built-in network administration tools allows it to evade detection by blending in with normal network traffic—"known as living off the land"—which hampers detection and attribution of their activities.
- Iranian government and other cyber actors sympathetic to Tehran's interests will continue to target US critical infrastructure, among other targets, in retaliation for US support to Israel during the Gaza conflict. Iran will use a range of opportunistic tactics, including exploiting publicly known software and hardware vulnerabilities, social engineering techniques, and publicly available cybersecurity tools. After HAMAS's October 2023 attack on Israel, dozens of pro-Iran criminal hacktivist groups conducted primarily low-level cyber attacks—such as distributed denial-of-service attacks—against Israeli, Palestinian, and US networks and websites. Later that November, Iranian IRGC-affiliated cyber actors—ostensibly posing as a criminal hacktivist group—used default credentials to successfully compromise and deface Israeli-manufactured OT devices used by US critical infrastructure sector entities.
- Russian state-sponsored cyber actors continue to seek ways to improve their sophisticated ability to stealthily execute cyber operations and identify new vulnerabilities they could

leverage against a variety of critical infrastructure targets. In late 2023, these actors gained access to a large IT firm's internal e-mails, including those of its cybersecurity teams, which could provide them with unique insights for future campaigns and make it more difficult for victims to detect their activity.

- We expect criminal hacktivists sympathetic to Russia will continue to carry out disruptive cyber attacks against poorly protected Western critical infrastructure to weaken US resolve in supporting Ukraine. After Russia's 2022 invasion of Ukraine, criminal hacktivists pledged support for the Russian government and targeted the United States and other countries for providing material support to Ukraine. In January 2024, pro-Russia criminal hacktivists disrupted multiple US municipality water distribution systems, demonstrating criminal hacktivist intent and capability to disrupt US critical infrastructure entities.

Financially motivated cyber criminals and state-affiliated actors will continue to employ ransomware and other schemes that will disrupt targeted US critical infrastructure entities and impose significant financial costs on their victims. Financially motivated cyber criminals, similar to other malicious cyber threat actors, consistently evolve and adapt to take advantage of software vulnerabilities, poor network security configurations, and social engineering tactics to gain systems access. Ransomware actors likely will continue to opportunistically target victims they believe will provide the largest payouts.

- Ransomware actors in 2023—the most recent annual data available—attacked entities in most US critical infrastructure sectors in their efforts to financially extort victims; we expect the healthcare and public health (HPH), critical manufacturing, IT, financial services, and government services and facilities sectors to remain the most affected targets.
- The HPH sector, for example, experienced an 18 percent increase in reported ransomware attacks in calendar year 2023. In FY 2024, ransomware attacks against this sector caused local- and national-level disruptions to patient care and services. In late calendar year 2023, a ransomware attack on the IT network of a large national hospital provider caused disruptions to subsidiary healthcare providers in multiple states. A 2024 ransomware attack against the United States' largest payment exchange platform for prescription drugs led to nationwide disruptions to pharmacy and hospital services for at least two weeks and cost over $20 million in ransom payments.
- North Korean cyber actors almost certainly will continue to target US financial entities, including individuals, venture capital firms, exchanges, and especially cryptocurrency-related users and entities, to finance Pyongyang's strategic priorities and weapons programs and to reduce the impact of international sanctions. These actors have stolen hundreds of millions of dollars in cryptocurrency over the last several years.

Disruptive and Destructive Physical Attacks Targeting Critical Infrastructure

DVEs and criminal actors with a range of motivations—some unclear—likely will continue to call for and carry out physical attacks against US critical infrastructure. Violent extremists view such attacks as advancing their ideological and sociopolitical goals, a trend that is consistent with historic drivers. DVEs and FTOs, as well as other criminal actors, increasingly called for physical attacks on infrastructure in response to flash point events over the last year, including the ongoing Israel-HAMAS conflict and upcoming US election cycle. *(For more information on threats to the 2024 US election cycle, see pages 10–11.)* Attacks and plots commonly involved lone offenders or small groups and used simple tactics that required minimal technical knowledge or preoperational planning.

- HAMAS's 7 October terrorist attack against Israel and the subsequent Israeli government operations in Gaza are driving an increase in media calls from FTOs like ISIS and al-Qa'ida for lone offender attacks against critical infrastructure, including US government buildings and US-based foreign embassies. In particular, al-Qa'ida and its affiliates have renewed calls for attacks against diplomatic facilities and the transportation sector, particularly civil aviation. We are concerned about the possibility that FTO-inspired or enabled insiders with access to critical infrastructure may seek ways to exploit potential vulnerabilities and increase their knowledge of security procedures for attack plotting. Additionally, FTO-inspired attacks and plots abroad since the onset of the Israel-HAMAS conflict present examples of tactics and targets that could be emulated or improved upon by US-based lone offenders. *(For more information on foreign terrorist threats to the Homeland, see pages 3–4.)*
- Some violent actors continue to attack electric grid substations and transformers with firearms, including a series of unattributed shootings against transformers and electricity infrastructure near Lansing, Michigan, from August 2023 through July 2024. However, the impacts on the energy sector's ability to provide services have been predominantly localized and short-term. Over the last year, violent actors with a range of motivations and some DVEs, particularly racially or ethnically motivated violent extremists driven by a belief in the superiority of the white race and accelerationism, have encouraged sabotage or attacks against the energy, communications, and HPH sectors, as well as other critical infrastructure sectors.[23,24] Separately, we continue to be concerned about adversary threats to the aviation and air cargo systems, including the potential use of the aviation domain to carry out terrorist plots and the potential use of the air cargo supply chain to ship concealed dangerous and potentially deadly items.
- We continue to observe concerning UAS activity over sensitive critical infrastructure sites, which could interfere with regular facility operations, disrupt emergency response or authorized flight operations, and provide intelligence to malign actors. Many unauthorized UAS belong to unknown operators, challenging our ability to characterize whether the intent is benign or malicious. We currently have no information suggesting violent extremists are using drones in attack planning, but in some instances, DVEs and FTOs have considered using UAS to conduct intelligence collection, to drop explosives and other items on US critical infrastructure for disruption purposes, and to endanger takeoffs and landings at airports via the mere presence of UAS.

Intelligence Collection Against Critical Infrastructure Networks

In addition to our adversaries targeting US critical infrastructure for destructive and disruptive attacks, adversaries also target the entities that make up critical infrastructure sectors for foreign intelligence collection. Adversarial nation-states continue to use cyber tactics to access and steal sensitive information from US networks, including those of entities that are part of critical infrastructure, for broader espionage purposes to advance their military, diplomatic, and economic goals.

- PRC state-sponsored cyber activity continues to represent the largest and most dynamic espionage threat to the United States. The PRC's pre-positioning efforts on US critical infrastructure probably also provide its cyber actors with broad access and insight into sensitive and proprietary data across an array of US critical infrastructure networks. PRC cyber actors, including a group associated with the Ministry of State Security, also exploit known vulnerabilities and publicly available tools, which complicates detection and attribution of their espionage activities.
- Russian government-affiliated cyber actors will continue to seek access to US federal, state, and local government and private sector networks for espionage purposes. These cyber actors persistently prioritize compromising US entities in the software supply chain to improve their capabilities and decrease victims' ability to protect against and detect such activity. Moreover, compromises of US firms within key elements of US software supply chains can be used as springboards for access to other US entities, which store data that Russia can use to advance its cyber espionage goals. For example, in late 2023, Russian Foreign Intelligence Service actors compromised a software development platform that would have enabled them to affect software supply chain operations.
- North Korea has virtually deployed thousands of highly skilled IT workers to work around the world, earning revenue to alleviate the impact of financial sanctions and to fund regime priorities. These IT workers deliberately obfuscate their identities, locations, and nationalities, typically using fake personas, proxy accounts, stolen identities, and falsified or forged documentation to apply for jobs at US and foreign companies. North Korea's malicious cyber program could use these workers' activities to gain privileged access to US systems and proprietary information, and thereby bolster North Korea's economic, diplomatic, and military modernization efforts.

Artificial Intelligence: Promise and Peril

Powerful AI technologies are driving economic and technological advancements in the United States, but these technologies—especially generative AI—are also having the unintended consequence of adding layers of complexity to the threats we face. In 2025, we expect malicious cyber actors will continue to use advancements in generative AI to incrementally enhance their ability to develop malware, vulnerability scanning, and exploit tools and to improve their social engineering tactics and operations. Adversarial states will continue to use AI in their malign influence campaigns as the technology lowers technical thresholds and improves adversaries' abilities to effectively personalize and scale more credible messages for target audiences. *(For more information on foreign malign influence activities, see pages 8–11.)* We expect FTOs, their supporters, and DVEs will continue to experiment with generative AI with the aims of improving their media content and output and radicalizing more people to violence.

- Generative AI is helping threat actors generate, manipulate, and disseminate synthetic media, such as deepfakes, making it a particularly useful tool for malign influence campaigns.[25] AI-generated and manipulated content—such as videos, audio, images, and text, all of which can include disinformation—have permeated the internet, impacting US search engine algorithms and video-streaming platforms. In May 2024, an individual used generative AI to create synthetic voice messages of the US President, designed to mislead voters before the New Hampshire primary. AI-generated disinformation content also degrades the information environment by drowning out factual content. In July, the DOJ seized a Russian social media bot-farm that used AI to build social media accounts that spread pro-Russian positions and divisive content in the hopes of influencing US audiences. In late 2023, the PRC used AI to generate and spread disinformation in English and other languages, as well as fake images, to allege that the devasting fires in Hawaii were caused by the United States testing a "weather weapon." We expect the PRC and Russia will continue to use generative AI to improve the scale and scope of their influence activities that target US audiences. Attribution will become more difficult as the language of the content improves and allows the content to blend more easily into the social media environment.

- FTOs and DVEs are exploring the benefits of advanced AI technologies to support their operations, messaging, and recruitment. We expect a range of violent extremists will increasingly attempt to use AI to augment attack plans, fill gaps in technical expertise, and expand the reach of their violent extremist messaging online. Violent extremists could also leverage AI to generate content intended to sow social discord, which could encourage real-world violence. Over the last year, FTOs, FTO supporters, HVEs, and online users in forums associated with DVEs have used or explored AI creation and language translation capabilities to develop and refine weapon-making techniques, acquire targeting guidance, generate violent media content, and translate violent messaging.
- Generative AI is also streamlining exploit development, vulnerability scanning, and social engineering campaigns, probably increasing the cyber threat to US networks. The recent surge of publicly available generative AI technologies has given malign cyber actors easily accessible tools that enhance the speed and scale of malicious cyber tactics, cutting the time and resources needed to generate phishing e-mails and conduct vulnerability scanning. Cyber criminals have also developed generative AI services to support and scale their financially motivated, malicious cyber activity. Generative AI's increasing ability to produce high-quality, compelling written content and improved voice capabilities will likely enhance malicious actors' ability to deceive victims through phishing e-mails and vishing schemes, potentially enabling an increase in fraud and network compromises.[26] As AI enables an increase in the scope of an already rising volume of cyber attacks, further automation of organizational cybersecurity efforts may help to more effectively counter persistent attacks and reduce the strain on human network defenders.
- Threat actors have also demonstrated their ability to get around rules that are meant to keep generative AI chatbots from returning dangerous information, such as bomb-making instructions, or sensitive data. This may have implications for US entities charged with securing personally identifiable information, especially sectors like healthcare and financial services. Threat actors have also manipulated open-source data used to train AI chatbots and AI models, which could lead to biased or erroneous outputs, highlighting the potential hazard of integrating AI into critical systems and operations.

THREATS TO ECONOMIC SECURITY

Overview: *In this section, we examine state threat actors who view our economy and commercial activities as vulnerable to manipulation, disruption, and exploitation, and who view our technology and intellectual property as critical resources for growing their own economic, military, and political power.*

Multifaceted and diverse economic threats from state actors, primarily the PRC, harm US producers and consumers and degrade the competitiveness and future health of US companies and industries. Our adversaries will continue manipulating markets, employing economic espionage and coercive economic tools, and seeking to illicitly acquire our technologies and intellectual property to develop advantages at the expense of the United States. The PRC likely will remain our greatest economic security threat because of its aggressive use of anticompetitive, coercive policies and theft of US intellectual property, technology, and trade secrets. Furthermore, we expect our supply chains will remain vulnerable to foreign manipulation, conflict, economic shocks abroad, climate-related events, and public health crises that affect economic productivity and consumer demand.

Economic Manipulation and Coercion

Foreign actors harm US economic competitiveness through supply chain manipulation, uncompetitive practices, and forced labor. In this space, the PRC will probably continue to pose the biggest threat. The PRC co-opts Chinese businesses through incentives and broad regulatory authorities to create unfair market competition that undermines US competitiveness and provides the PRC government with more access to global resources.

- The PRC's influence over critical mineral supply chains endangers US economic security and the research and development of emerging technology. The PRC will work to maintain its dominance by increasing investment in overseas mining operations and using export controls to manipulate markets for valuable minerals. Beijing's 2023 export control restrictions on gallium, germanium, graphite, and most recently antimony—minerals essential for renewable energy and advanced technology products, including semiconductors—demonstrate the PRC's willingness to manipulate critical supply chains to advance its economic and strategic interests. The PRC likely will continue to pursue global partnerships that enable the extraction and production of critical minerals and reduce opportunities for US firms abroad.
- The PRC's Counter Espionage Law update likely will continue to hinder US business operations in China, undermining opportunities for competitive US firms looking to enter the market. In February 2024, China amended the law to reduce non-Chinese citizens' access to business and government information and reiterated warnings to Chinese citizens that foreign consultancies, including due diligence firms that support US businesses, threaten PRC national security. Beijing may also use this law to force US firms operating in China to disclose proprietary business information, an obligation that could compromise US firms' competitiveness and US persons' private information held by these firms.
- Our nearshoring efforts, changes to global shipping routes, PRC market concentration in key supply chain nodes such as ship-to-shore cranes, and new international port infrastructure provide the PRC and potentially other foreign actors pathways to interfere with US supply chains and evade tariffs.[27] For example, the PRC is investing heavily in port infrastructure in Chancay, Peru under terms that favor PRC shipping companies, potentially giving Beijing greater influence over regional shipping operations. Meanwhile, some PRC firms have established production lines in Central and South American countries that have more favorable trade agreements with the United States to bypass tariffs and access US markets.
- The use of forced labor in manufacturing abroad harms the US economy, legitimate global trade, competition, and supply chains. For example, foreign actors' use of forced labor in the fishing industry artificially lowers the costs of fishing operations, distorts markets, and harms supply chains, undercutting US businesses that adhere to ethical labor practices. Similarly, the textile industry, like other industries, suffers when competitors use forced labor, violate customs laws, and engage in other illegal practices to undercut US businesses and drive prices unfairly low. Moreover, Beijing's ongoing efforts to obfuscate its use of Muslim Uyghurs for forced labor raises the likelihood that US businesses and persons may unknowingly violate US law by importing goods manufactured with forced labor.

Economic Espionage and Influence

The PRC and other foreign adversaries also will continue their aggressive efforts to target and steal sensitive US information, research, and technology, resulting in billions of dollars in economic losses, damage to US competitiveness, and the transfer of cutting-edge technology to adversarial militaries. Since 2023, US authorities have charged more than 20 individuals for activities related to intellectual property theft and for violations of US sanctions or export controls for China, Iran, and Russia. PRC officials' engagements with US state, local, and private sector officials—also known as subnational engagements—probably also enable PRC economic espionage activities and enhance Beijing's ability to influence local policy to favor PRC priorities over US national interests.

- China's illicit procurement efforts have primarily focused on stealing sensitive US technology and intellectual property from US manufacturers and research institutions. Iran, North Korea, and Russia, by contrast, primarily purchase finished aerospace, electronic, and military technology products illegally through third-country intermediaries. For example, a recent Ukrainian study identified more than 700 US-labeled semiconductors in weaponry seized from the Russian military on Ukrainian battlefields despite US sanctions banning most trade with Russia since 2022.
- Some foreign nationals take advantage of research opportunities in the United States to gain access to sensitive industries—such as military equipment and technology development, aerospace, and semiconductors—and exploit that access to benefit foreign governments. Several of the individuals arrested for such activities over the past year were funded by the PRC's People's Liberation Army talent funding programs. We expect the PRC will continue to compel its US-based students and researchers to transfer valuable technology and intellectual property to the PRC to help its commercial and military programs.
- We remain concerned that the PRC and other foreign adversaries will seek to use subnational engagements, such as sister-city relationships and diplomatic activities, as well as academic exchanges and programs and business partnerships to influence policy and gain access to sensitive US information, research, and technology as well as regional resources. The PRC and PRC-linked businesses also probably hope to use subnational engagements to help improve economic relations with the United States and may try to exploit these engagements to cultivate and recruit insiders and solicit or elicit sensitive information. The PRC aims to increase subnational engagements, as demonstrated by recent Chinese delegation visits and summits, suggesting that the scope and scale of PRC influence, recruitment, and elicitation efforts may increase as these engagements grow. The PRC may also use these engagements as a means to facilitate foreign investment activities that provide them access to US critical infrastructure and sensitive technology.
- The PRC pursues industrial espionage and investments in US firms to gain access to sensitive information on, and control over, entities in US critical infrastructure, including in the telecommunications, transportation, energy, and food and agriculture sectors. The PRC uses a variety of methods to obfuscate its malign intent and activities. The same sensitive technology and business information that informs insights into critical infrastructure operations can also confer unfair economic advantages onto PRC firms. For example, the PRC's longstanding effort to steal US seed and other agricultural technology, and its continued struggle with food insecurity and environmental degradation, raise our concern that Beijing could increase its targeting of this critical infrastructure sector.

Climate Change, Natural Disasters Compound National Security Threats

The impacts of climate change and natural disasters will continue to pose acute and systemic challenges to the United States, often converging with and exacerbating more traditional national security threats, including those to critical infrastructure, the economy, and the border. Heat waves, wildfires, droughts, heavy precipitation, and other extreme weather events increase risks to our transportation infrastructure, maritime shipping operations, and global supply chains, and they have the potential to impact the availability of goods and services, generating cascading economic effects. In addition, natural disasters or extreme weather events abroad that disrupt local economies or result in food insecurity have the potential to exacerbate migration flows to the United States and to tax US law enforcement resources, particularly along our southern border.

Definitions and Contextual Notes

[1] For the purposes of this paper, the **Election Cycle** covers the timeframe from the first presidential primary elections to Inauguration Day in January 2025.

[2] A **Foreign Terrorist Organization (FTO)** is any foreign organization that is designated by the Secretary of State in accordance with the criteria section 219 of the Immigration and Nationality Act (INA), which are 1) It must be a foreign organization; 2) The organization must engage in terrorist activity or retain the capability and intent to engage in terrorist activity or terrorism; and 3) The organization's terrorist activity or terrorism must threaten the security of US nationals or the national security (national defense, foreign relations, or economic interest) of the United States.

[3] A **Domestic Violent Extremist (DVE)** is an individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals wholly or in part through unlawful acts of force or violence. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics alone does not constitute violent extremism and may be constitutionally protected. DVEs can fit within one or multiple categories of ideological motivation and can span a broad range of groups or movements. I&A utilizes this term synonymously with "domestic terrorist."

[4] A **Homegrown Violent Extremist (HVE)** is a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction or influence from a foreign actor.

[5] A **Lone Offender** is an individual motivated by one or more violent extremist ideologies who, operating alone, supports or engages in acts of unlawful violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor.

[6] For the purpose of this product, **Conspiracy Theories** are defined as a subset of narratives in which the ultimate cause of an event is believed to be due to a malevolent plot by multiple actors working together or as an effort to explain some event or practice by reference to the machinations of powerful people, who attempt to conceal their role (at least until their aims are accomplished), as per the National Counterterrorism Innovation, Technology, and Education Center, a DHS Center of Excellence. DHS does not hold a position on the veracity of the claims associated with these theories.

[7] The attack and plot data related to domestic violent extremists, homegrown violent extremists, and targeted violence are subject to change and are based on currently available information. Notably, the apparent attempted assassinations of a former US President in July and September are not currently counted in these numbers due to the ongoing investigations into the attackers' respective motives. More incidents may be categorized as attacks or plots as investigations progress and new information becomes available.

[8] **Swatting** is a harassment tactic in which emergency services are falsely contacted and dispatched without legitimate justification to an unwitting person's location. **Doxxing** is the action or process of publishing private or sensitive identifying information about a particular individual or group on the internet, typically with malicious intent and without consent.

[9] **Radicalization** is the process through which an individual changes from a nonviolent belief system to a belief system that includes the willingness to actively advocate, facilitate, or use unlawful violence as a method to effect societal or political change.

[10] A **Mass Casualty Attack** is defined as any premeditated killing or incapacitation of four or more people in violation of the criminal laws of the United States or any State or subdivision within the United States under circumstances suggesting that individual victims were attacked indiscriminately (i.e., not for any personal, financial, or other motivation particular to the individual victim). An attack need not take place in the same location to qualify as a mass casualty incident; an incident is ongoing so long as there is no "cooling off" period.

[11] In terms of volume, fentanyl is generally seized in smaller quantities compared to other drugs. However, 1 kilogram of fentanyl can produce 1 million to 1.5 million pills. Two milligrams of fentanyl can be lethal, and DEA analysis has found 42 percent of pills tested for fentanyl contained at least 2 milligrams of fentanyl.

[12] **Transnational Criminal Organization (TCO)** refers to those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.

[13] **Misinformation** is false, inaccurate, or misleading information that is spread regardless of the intent to deceive. An adversary's intent can change misinformation to disinformation. **Disinformation** is false or misleading information that is deliberately created or spread with the intent to deceive or mislead. **Malinformation** is an adversary's deliberate use of otherwise verifiable information with malicious intent, such as by amplifying the information selectively, out of context, or to the detriment of specific persons.

[14] **Influence Operations** are discrete activities by a state, nonstate actor, or proxy, sometimes to achieve specific goals under a larger influence campaign objective.

[15] **Generative AI** is a set of algorithms that uses available data to contextualize a user's prompt and generate a new output, including video, audio, images, and text.

[16] **Transnational Repression** is the act of a government reaching across national borders, often illicitly, to silence dissent among its diaspora and exile communities.

[17] **Synthetic Media** is text, audio, image, or video that is altered or modified from its original form often through the use of AI algorithms.

[18] **Phishing** is the practice of masquerading as a reputable source via e-mail to attempt to steal sensitive information, such as usernames and passwords, financial information, or to convince a target to download malware.

[19] **Migrant Encounters** include migrants encountered and apprehended by CBP's Border Patrol under Title 8 authorities between ports of entry; migrants encountered by the CBP's Office of Field Operations at ports of entry and determined to be inadmissible to the United States under Title 8 authorities, including CBP One appointments; and migrants encountered and expelled between March 2020 and May 2023 under Title 42 authorities.

[20] **Human Trafficking** involves exploiting individuals for the purposes of forced labor or commercial sexual exploitation. It is common for those who are willingly smuggled into the United States to then become victims of human trafficking.

[21] **Forced Labor** occurs when individuals are compelled against their will to provide work or service through the use of force, fraud, or coercion. US law prohibits the importation of goods mined, produced, or manufactured wholly or in part from forced labor.

[22] **Operational Technology** refers to systems used to monitor and control physical devices and processes.

[23] **Racially or Ethnically Motivated Violent Extremists** are groups or individuals who facilitate or engage in the potentially unlawful use or threat of force or violence with the intent to intimidate or coerce, in furtherance of political and/or social agendas, which are deemed to derive from bias, often related to race or ethnicity, held by the actor against others, including a given population or group. This includes DVEs motivated by their belief in the superiority of the white race, as well as DVEs motivated by real or perceived racism and injustice in American society, the desire for a separate black homeland, and/or violent interpretations of religious teachings.

[24] **Accelerationism** is a concept suggesting the existing social order should be pushed to such a degree that Western countries become failed states, giving rise to changes that would reshape the world in radical ways. Some racially or ethnically motivated violent extremists following a white supremacist extremism version of accelerationism advocate for acts of social disruption up to and including violence and taking violent action to prompt responses that would gain support from those advocating for the superiority of the white race.

[25] **Deepfakes** are pictures or videos of a person in which their face or body has been digitally altered so that they appear to be someone else, typically used maliciously or to spread false information.

[26] **Vishing** is similar to phishing, but done through phone calls or voice messages, as opposed to e-mail.

[27] **Nearshoring** is the transferring of business processes—like manufacturing—to a nearby country. For example, both US and PRC companies are moving production from the PRC to Mexico.

Photo credits: Getty, US Customs and Border Protection, US Coast Guard, and California Department of Water Resources.

Homeland Security