Homeland Security

OFFICE *of* INTELLIGENCE *and* ANALYSIS

Homeland Threat Assessment

2024

With honor and integrity, we will safeguard the American people, our Homeland, and our values.

TABLE OF CONTENTS

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

Methodology

The Department of Homeland Security (DHS) Intelligence Enterprise Homeland Threat Assessment reflects the insights from across the Department, the Intelligence Community, and other critical homeland security stakeholders. It focuses on the most direct, pressing threats to our Homeland during the next year and is organized into four sections. We organized this assessment around the Department's missions that most closely align or apply to these threats—public safety, border and immigration, critical infrastructure, and economic security. As such, many of the threat actors and their efforts cut across mission areas and interact in complex and, at times, reinforcing ways.

Going forward, the annual Homeland Threat Assessment will serve as the primary regular mechanism for articulating and describing the prevailing terrorism threat level, which has previously been done through our issuance of National Terrorism Advisory System (NTAS) bulletins. In the future, the issuance of NTAS bulletins will be reserved for situations where we need to alert the public about a specific or imminent terrorist threat or about a change in the terrorism threat level.

Executive Summary

Terrorism, both foreign and domestic, remains a top threat to the Homeland, but other threats are increasingly crowding the threat space. During the next year, we assess that the threat of violence from individuals radicalized in the United States will remain high, but largely unchanged, marked by lone offenders or small group attacks that occur with little warning. Foreign terrorist groups like al-Qa'ida and ISIS are seeking to rebuild overseas, and they maintain worldwide networks of supporters that could seek to target the Homeland.

In addition to the enduring terrorism threat, we expect illegal drugs produced in Mexico and sold in the United States will continue to kill more Americans than any other threat. During the past year, US-based traffickers have become more involved in the mixing and pressing of fentanyl, contributing to more lethal mixes of this already deadly drug.

This year, record encounters of migrants arriving from a growing number of countries have complicated border and immigration security. While monthly encounters have fallen from record highs in December, overall encounters for the fiscal year are on pace to nearly match 2022's record high total. As part of the overall increase in migration, we have also encountered a growing number of individuals in the Terrorist Screening Data Set (TSDS), also known as the "watchlist." Inclusion in the TSDS ranges from known associates of watchlisted individuals, such as family members, to individuals directly engaged in terrorist activity.

Domestic and foreign adversaries will likely continue to target our critical infrastructure over the next year, in part because they perceive targeting these sectors would be detrimental to US industries and the American way of life. While cyber attacks seeking to compromise networks or disrupt services for geopolitical or financial purposes continue apace, we noted an uptick over the last year of physical attacks on critical infrastructure. We expect the 2024 election cycle will be a key event for possible violence and foreign influence targeting our election infrastructure, processes, and personnel.

Against this backdrop of traditional homeland security threats, we expect the People's Republic of China (PRC) will continue to use predatory economic practices to advantage its firms and industries over ours. The PRC will likely continue to manipulate markets, employ economic espionage and coercive economic tools, and seek to illicitly acquire our technologies and intellectual property. Concurrently, financially motivated criminal actors are adapting new methods to improve their ability to financially extort victims and will likely continue to impose significant financial costs on the US economy over the next year.

Climate change, natural disasters, and technological advances have the potential to compound many of these threats. Climate-related disasters, such as heat waves, droughts, wildfires, coastal storms, and inland flooding, have the potential to disrupt regional economies, foster health crises like disease outbreaks, and tax law enforcement resources. Meanwhile, the proliferation of accessible artificial intelligence (AI) tools likely will bolster our adversaries' tactics. Nation-states seeking to undermine trust in our government institutions, social cohesion, and democratic processes are using AI to create more believable mis-, dis-, and malinformation campaigns, while cyber actors use AI to develop new tools and accesses that allow them to compromise more victims and enable larger-scale, faster, efficient, and more evasive cyber attacks.

PUBLIC SAFETY AND SECURITY

OVERVIEW

One of the Department's top priorities is to ensure the safety and security of the American people. Within the Public Safety and Security mission, we considered lethal threats in the Homeland, including terrorism and illegal drugs, as well as nation-state efforts to malignly influence US audiences, as the primary national security threats to our communities.

The terrorism landscape in the United States has evolved since 9/11—from foreign terrorists directing attacks in the Homeland to a more amorphous threat environment where individuals or small cells independently plot attacks to advance a range of ideologies and political objectives. Meanwhile, the production, trafficking, and sale of illegal drugs by transnational and domestic criminal actors probably pose the most lethal and persistent threat to communities in the United States. Nation-state adversaries intent on undermining our social cohesion are incorporating new technologies into their mis-, dis-, and malinformation campaigns, which will likely ramp up ahead of the elections this year *(see "Threat Actors Likely To Converge on 2024 Election Season," page 19)*. Many of these same actors seek to suppress dissidents living in the United States, violating our sovereignty and the rule of law.


NCY MEDICAL SERVICES

TERRORISM

In 2024, we expect the threat of violence from violent extremists radicalized in the United States will remain high but largely unchanged from the threat as described in the May 2023 National Threat Advisory System (NTAS) bulletin. Over the past year, both domestic violent extremists (DVEs) and homegrown violent extremists (HVEs) inspired by foreign terrorist organizations have engaged in violence in reaction to sociopolitical events. These actors will continue to be inspired and motivated by a mix of conspiracy theories; personalized grievances; and enduring racial, ethnic, religious, and anti-government ideologies, often shared online.

- Since January 2022, DVEs have conducted three fatal attacks in the Homeland resulting in 21 deaths and multiple non-lethal attacks. US law enforcement has disrupted over a half dozen other DVE plots. During the same period, only one attack was conducted by an individual inspired by a foreign terrorist organization. The individual—who is awaiting trial—was likely inspired by a spiritual mentor of al-Qa'ida and Taliban narratives and allegedly wounded three New York City Police Department officers on New Year's Eve.
- Collectively, these incidents focused on a variety of targets, including law enforcement, government, faith-based organizations, retail locations, ethnic and religious minorities, healthcare infrastructure, transportation, and the energy sector. The most lethal attack this year occurred in May in Allen, Texas, where a now-deceased attacker killed eight people at a shopping mall. The attacker was fixated on mass violence and held views consistent with racially or ethnically motivated violent extremist (RMVE) and involuntary celibate violent extremist ideologies, judging from his writings and online activities.
- While violent extremists likely will continue using accessible, easy-to-use weapons for attacks, they also will leverage online platforms and encrypted communications applications to share novel tactics and techniques. Collaboration among violent extremists online likely will grow as they strive to spread their views, recruit followers, and inspire attacks. Some RMVEs have improved the quality of their video and magazine publications online, which could help them inspire more like-minded individuals to commit attacks.

Foreign terrorist groups like al-Qa'ida and ISIS are seeking to rebuild overseas, and they maintain worldwide networks of supporters that could seek to target the Homeland. Among state actors, we expect Iran to remain the primary sponsor of terrorism and continue its efforts to advance plots against individuals in the United States.

- Foreign terrorists continue to engage with supporters online to solicit funds, create and share media, and encourage attacks while their affiliates in Africa, Asia, and the Middle East prioritize local goals. Since the US withdrawal from Afghanistan, ISIS's regional branch—ISIS-Khorasan—has garnered more prominence through a spate of high-casualty attacks overseas and English-language media releases that aim to globalize the group's local grievances among Western audiences. Individuals with terrorism connections are interested in using established travel routes and permissive environments to facilitate access to the United States.

- Iran maintains its intent to plot attacks against current and former US government officials in retaliation for the 2020 death of Islamic Revolutionary Guards Corps-Qods Force (IRGC-QF) Commander and designated foreign terrorist Qassem Soleimani. Iran relies on individuals with pre-existing access to the United States for surveillance and lethal plotting—using dual nationals, members of criminal networks, and private investigators—and has attempted plots that do not require international travel for operatives. In August 2022, the DOJ indicted an IRGC-QF member for allegedly conspiring to assassinate a former US National Security Advisor between late 2021 to mid-2022. Iran's surrogate Lebanese Hizballah also called for revenge against the United States for Soleimani's death.

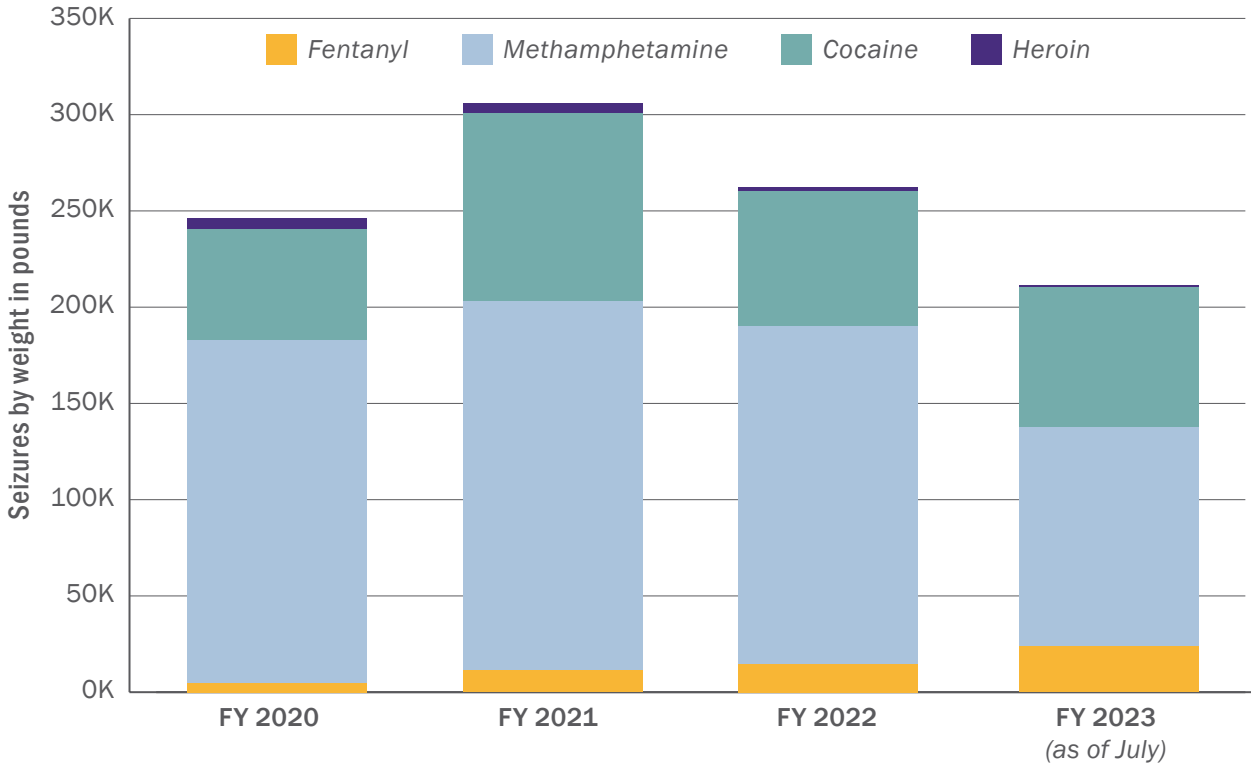
ILLEGAL DRUGS

While terrorists pose an enduring threat to the Homeland, drugs kill and harm far more people in the United States annually. The increased supply of fentanyl and variations in its production during the last year have increased the lethality of an already deadly drug, a trend likely to persist in 2024. Traffickers in Mexico and the United States are using various additives, such as xylazine, and mixing fentanyl into counterfeit prescription pills, which are driving an increase in overdoses. Given this trend, we expect fentanyl to remain the leading cause of narcotics-related deaths in the United States. The illegal narcotics trade also harms our communities by supporting violent criminal enterprises, money laundering, and corruption that undermines the rule of law.

- Seizures of fentanyl at our southern border continue to increase throughout 2023 with CBP on track to seize a record amount of fentanyl entering the United States *(see Figure 1).* CBP seizures of cocaine, heroin, and methamphetamine have either remained steady or declined each fiscal year since 2020. However, US law enforcement is increasingly encountering instances where many of these drugs are mixed with fentanyl. Preliminary data from the

Centers for Disease Control and Prevention indicate that more than 100,000 individuals have died from drug overdoses in the United States during the last year, continuing the previous year's trend. Synthetic opioids, including drugs such as fentanyl and tramadol, have accounted for roughly 75 percent of overdoses during the last year.

Figure 1: CBP Border Seizures of Fentanyl, Methamphetamine, Cocaine, and Heroin FY 2020–2023



23-316-IA

- Domestic drug traffickers have gained more influence over the composition of fentanyl pills available in the United States and have distributed potentially more deadly mixtures of the drug to both witting and unwitting users. US law enforcement seizures of pill presses purchased online have increased, suggesting these US-based traffickers are pressing a highly toxic combination of drugs into different types of pills. Fentanyl has appeared more frequently in counterfeit prescription pills, such as Adderall and Xanax, combinations that raise the risk of overdose, particularly for unwitting users. Traffickers are also bulking fentanyl powder and pills with the animal sedative xylazine ("Tranq"), challenging standard opioid overdose treatments.

- Transnational criminal organizations (TCOs) in Mexico, particularly the Sinaloa Cartel and the New Generation Jalisco Cartel, remain the primary smugglers of fentanyl and other drugs into the United States.[a] These organizations continue to use bribery and violence to grow their smuggling and narcotics production operations in Mexico, and they rely on companies in China to purchase fentanyl precursor chemicals and pill pressing equipment.

FOREIGN MISINFORMATION, DISINFORMATION, AND MALINFORMATION[b]

Nation-state adversaries likely will continue to spread mis-, dis-, and malinformation aimed at undermining trust in government institutions, our social cohesion, and democratic processes. The proliferation and accessibility of emergent cyber and AI tools probably will help these actors bolster their malign information campaigns by enabling the creation of low-cost, synthetic text-, image-, and audio-based content with higher quality. Russia, China, and Iran continue to develop the most sophisticated malign influence campaigns online. Many of the tactics these adversaries use to influence US audiences will likely be used in the lead-up to the 2024 election *(for more information on threats to elections see page 19)*.

- Generative AI enables the rapid creation of an endless supply of higher quality, more idiomatically correct text, providing influence actors the ability to expand their messaging and give it a greater aura of credibility. Already, hundreds of websites have used a publicly available, large-language, model-based chatbot to generate content, some of which was false or misleading. For example, in April, a Chinese government-controlled news site using a generative AI platform pushed a previously circulated false claim that the United States was running a lab in Kazakhstan to create biological weapons for use against China. Recently, Russian influence actors have used new AI technology in select cases to augment their operations. For instance, in June, an RT (formerly Russia Today) social media account created and shared a deepfake AI-generated video disparaging the US President and other Western leaders.
- Russia likely will continue to use traditional media, covert websites, social networks, online bots, trolls, and individuals to amplify pro-Kremlin narratives and conduct influence activities within the United States. Since its invasion of Ukraine, Russian messaging has focused on justifying its aggression, seeking to reduce US domestic support for Kyiv, and encouraging divisions among the diverse set of global partners that are helping Ukraine.

a **Transnational criminal organizations** 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.

b **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 or out of context, or to the detriment of specific persons.

- China has used state and proxy media for overt messaging and coordinated, inauthentic social media campaigns to influence US audiences—activities we expect to continue. Its influence actors likely will continue their efforts to refine and employ tactics and messaging to influence US discourse. Iran will likely also attempt to influence US audiences to promote its anti-US agenda utilizing social media and inauthentic websites.

TRANSNATIONAL REPRESSION

To augment many of their efforts in the public sphere, China, Iran, and Russia likely will continue to pursue transnational repression activity in the Homeland, undermining US laws, norms, and individuals' rights. Adversaries have targeted individuals in the United States who they perceive as threats to their legitimacy, including ethnic and religious minorities, political dissidents, and journalists. Agents of these regimes use physical assault, threats, harassment and defamation, rendition, and the manipulation of international law enforcement personnel and processes to suppress oppositional voices. China and Iran likely will remain the most aggressive actors in the United States.

- China is likely to continue its efforts to suppress the activities of dissidents in the United States, including members of the Chinese diaspora and Chinese students at US universities. Beijing also has used a small number of secret, unsanctioned "police stations" in the United States to identify, monitor, and harass dissidents. Its global "Operation Fox Hunt" has sought the extradition of Chinese dissidents under false legal pretenses.
- Iran has targeted Iranian dissidents in the United States to suppress support for potential anti-regime protests and calls for social and political reform. In early 2023, the DOJ indicted several individuals for plotting to murder a US dissident on behalf of Iran. Tehran had previously subjected the US citizen to death threats, a year-long social media campaign calling for their abduction, and the arrest of a family member in Iran.
- Iranian and Chinese intelligence services have hired US-based private investigators to monitor dissidents, suggesting US citizens may wittingly or unwittingly enable activities that result in harassment or physical harm to individuals in the United States. Similarly, in at least one instance, Russia has used a foreign national to spy on a US-based Russian dissident.

Chemical, Biological, Radiological, and Nuclear Threats Endure

Chemical, biological, radiological, and nuclear (CBRN) threats to the Homeland will persist into 2024 due to several factors, including foreign political and military developments and the global proliferation of laboratories working with dangerous biological pathogens. However, the deliberate use of such threats against the Homeland will likely be limited. Over the past year, Russia's public allusions to using nuclear weapons as part of its invasion of Ukraine demonstrate that international actors still consider nuclear threats as viable tools of statecraft. Meanwhile, the growing nexus between AI and scientific research—especially in biotech—raises the potential for deliberate and incidental creation of novel chemical compounds that can risk public health. While CBRN threats occurring abroad may not reach the Homeland, they have the potential to disrupt regional and global commerce, harming US economic interests.


NA 1.25


BORDER PATROL

BORDER AND IMMIGRATION SECURITY

OVERVIEW

The Department ensures the safety and security of our borders while managing safe, orderly, and humane immigration, travel, and trade systems. Within this section, we considered the threats posed by transnational criminal organizations, terrorists, and other threat actors seeking to exploit our border, as well as migration trends that complicate our ability to identify and interdict these threats.

The complex border and immigration security challenges we have faced over the last year are likely to continue. Although encounters with migrants have declined from record highs in December, migrants seeking entry to the United States are still arriving at a rate that is on pace to nearly match 2022 total encounters. As part of this increase, we have encountered growing numbers of individuals in the Terrorist Screening Data Set (TSDS), also known as the "watchlist."[c] Also, TCOs continue to 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.

c The Terrorist Screening Dataset (TSDS)—also known as the "watchlist"—is the U.S. government's database that contains sensitive information on terrorist identities. The TSDS originated as the consolidated terrorist watchlist to house information on known or suspected terrorists (KSTs) but has evolved over the last decade to include additional individuals who represent a potential threat to the United States, including known associates of watchlisted individuals

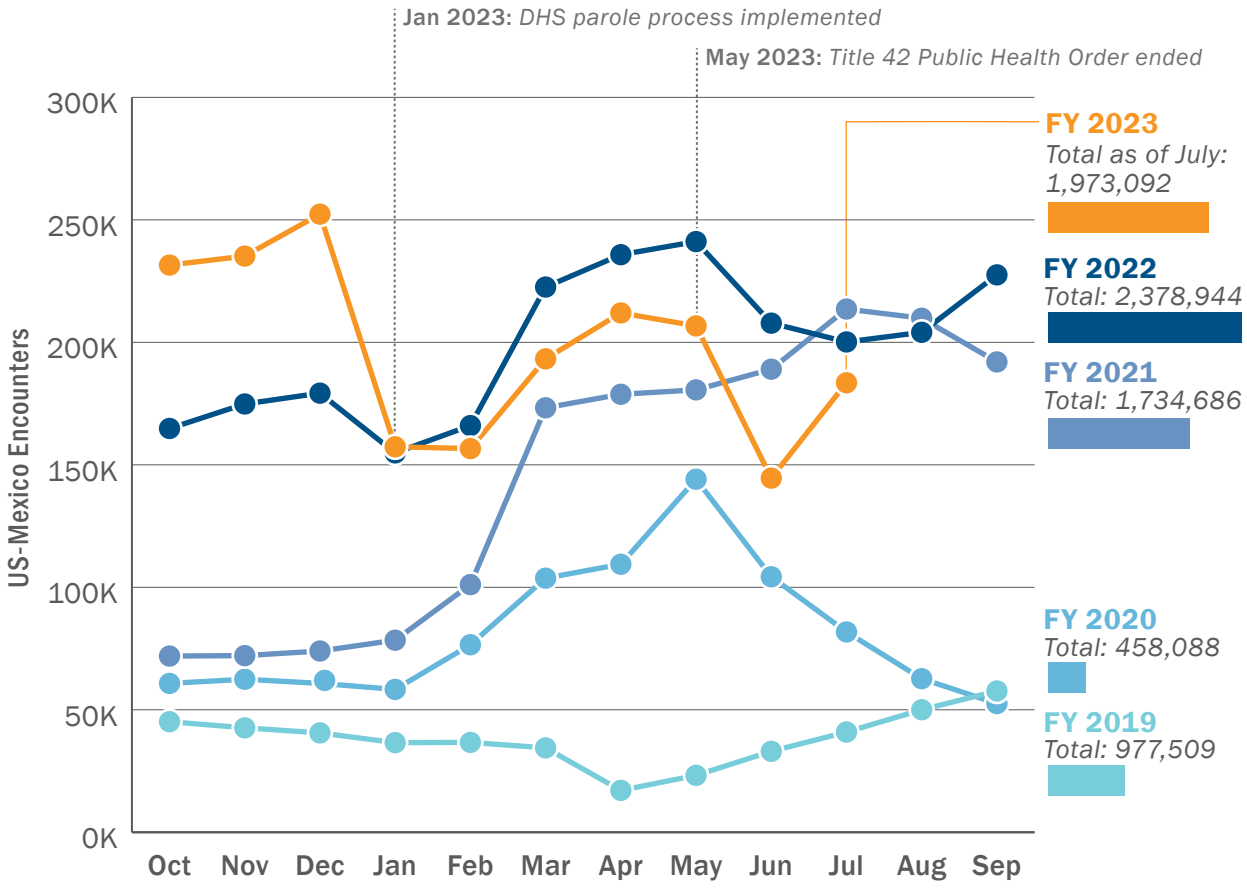
MIGRATION AND WATCHLIST ENCOUNTER TRENDS

Record numbers of migrants traveling from a growing number of countries have been encountered at our borders this fiscal year, with some monthly decreases largely attributed to migrants exploring new legal pathways or the expressed fear of penalties for irregularly crossing following the lifting of the Title 42 Public Health Order. We expect continued high numbers of migrant encounters over the next year because traditional drivers of migration to the United States remain unchanged and frustration with waiting for legal migration pathways may grow. Terrorists and criminal actors may exploit the elevated flow and increasingly complex security environment to enter the United States.

- CBP is on pace to encounter more migrants at the southern border this year than any other year except 2022 *(see Figure 2)*, with encounters spiking just prior to the January announcement of expanded parole processes for migrants from Cuba, Haiti, Nicaragua, and Venezuela. Encounters spiked again just prior to the lifting of the Title 42 Public Health Order in May, as some migrants rushed to enter the United States prior to the change. While our southern border remains the primary vector for migration, migrant encounters along the northern border have reached record highs, with over 132,000 migrants through June, compared with nearly 68,000 migrants the same time last fiscal year. Overall maritime migration encounters in FY 2023 are down compared to FY 2022. Maritime migration encounters in the Caribbean, primarily of Cuban and Haitian nationals, peaked in January, reaching a high of 5,677 migrants.
- Increased migration from the Eastern Hemisphere has exacerbated border security challenges in FY 2023, partly because many of these migrants require additional processing and repatriation resources. Encounters of migrants from the Eastern Hemisphere doubled from over 110,000 in FY 2022 to over 228,200 through June 2023. We expect the influx of these migrants will continue as they face poor economic, political, security, and climate conditions in their countries and use uneven visa policies across the globe to reach the United States.
- Individuals with potential terrorism connections continue to attempt to enter the Homeland. As of July, approximately 160 non-US persons in the TSDS attempted to enter the United States via the southern border this year, most of whom were encountered attempting to illegally enter between ports of entry. This represents an increase from the approximately 100 encounters in all of FY 2022. Inclusion in the TSDS ranges from known associates of watchlisted individuals, such as family members, to individuals directly engaged in terrorist activity.

Figure 2: US Southern Border Migrant Encounters FY 2019–July FY 2023

In January 2023, DHS announced a parole process allowing eligible nationals of Cuba, Haiti, Nicaragua, and Venezuela lawful entry to the United States, resulting in a drop in border crossings. Encounters then briefly surged as migrants anticipated increased border enforcement following the May 2023 end of the CDC's Title 42 Public Health Order, which had removed some consequences for unlawful border crossings.



23-315-IA

TRANSNATIONAL CRIMINAL ORGANIZATIONS

TCOs almost certainly will continue to smuggle drugs into our country while also exploiting migrants for financial gain. These criminal organizations likely will seek new technologies and develop novel techniques to improve their ability to evade our border security measures.

- Mexico-based TCOs, including human smuggling organizations, are leveraging small unmanned aerial systems (UAS) to enhance and protect their operations. In 2022 and 2023, US officials observed human smugglers using commercially available UAS to monitor migrants and law enforcement across the border. Drug traffickers also use small commercial UAS to augment drug smuggling and to surveil US and Mexican law enforcement activities, helping them avoid some interdiction operations.

Human Trafficking

Human trafficking—specifically transnational sex trafficking and forced labor—is an enduring threat to human and workers' rights, our economic interests and labor markets, physical and virtual borders, immigration and customs systems, and the national security of the United States.[d] While we lack reliable statistics on the prevalence of human trafficking, more than 10,000 trafficking situations with over 16,000 likely victims of trafficking were reported to the National Human Trafficking Hotline in 2021, the most recent year for which data is available.

- Transnational sex trafficking in the United States continues to primarily involve illicit massage businesses and private brothels that exploit women predominantly from Asia. Mexico-based criminal networks are also involved in sex trafficking, coercing Mexican women and girls into commercial sex across several US jurisdictions, according to ICE. Sex traffickers often use social media, dating sites, chat rooms, and other web sites to identify, groom, and recruit victims and advertise victims to prospective customers.
- Criminals involved in forced labor operations have used coercive schemes that exploit vulnerabilities in US visa programs and immigration systems, demonstrating the need for continued cross-agency coordination to mitigate these threats. Imported goods produced with forced labor remain a persistent issue and present several risks for the public, corporate, government, and military supply chains, ranging from food safety and intellectual property to national security, according to CBP.[e]

d **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.

e US law prohibits the importation of goods mined, produced, or manufactured wholly or in part from **forced labor.**


ALTO
UNITED STATES

CRITICAL INFRASTRUCTURE SECURITY

OVERVIEW

Critical infrastructure provides the goods and services that are the backbone of our national and economic security and the well-being of all Americans. Within this section, we considered physical and cyber threats from domestic and foreign actors—including terrorists, adversarial nation-states, and non-state actors—to the resources, assets, and structures of our critical infrastructure sectors.

Domestic and foreign adversaries likely will continue to threaten the integrity of US critical infrastructure—including the transportation sector—over the next year, in part because they perceive targeting these sectors would have cascading impacts on US industries and the American way of life. From attacks aimed at disrupting services to espionage focused on gaining access to networks and stealing sensitive information, these actors are constantly adapting their techniques to gain access to and potentially compromise these entities. DVEs increasingly called for physical attacks on critical infrastructure this year, while foreign adversaries are exploring new technologies like AI to improve their tactics.

DISRUPTIVE AND DESTRUCTIVE ATTACKS

DVEs and criminal actors with unclear motivations are increasingly calling for and carrying out physical attacks against critical infrastructure, particularly the energy sector. DVEs see such attacks as a means to advance their ideologies and achieve their sociopolitical goals.

- DVEs, particularly RMVEs promoting accelerationism—an ideology that seeks to destabilize society and trigger a race war—have encouraged mobilization against lifeline and other critical functions, including attacks against the energy, communications, and public health sectors. Unidentified actors have attacked electric cooling components, substations, and transformers, though the impact on the energy sector's ability to provide localized services has been minimal.

State and non-state cyber actors continue to seek opportunistic access to critical infrastructure sector targets for disruptive and destructive attacks. Common tactics include denial-of-service, website defacement, and ransomware. Some of these actors also seek to develop or improve existing capabilities that can disrupt industrial control systems that support US energy, transportation, healthcare, and election sectors.

- Malicious cyber activity targeting the United States has increased since the beginning of the Russia-Ukraine conflict, a trend we expect to continue throughout the duration of the conflict. Pro-Russia cyber criminal groups, such as Killnet, collaborate to conduct distributed denial-of-service (DDoS) attacks and other potentially disruptive attacks against US government systems and our transportation and healthcare sectors. Killnet claimed credit for a March 2022 DDoS attack against a US airport it believed was helping US efforts to aid Ukraine.
- Malicious cyber actors have begun testing the capabilities of AI-developed malware and AI-assisted software development—technologies that have the potential to enable larger scale, faster, efficient, and more evasive cyber attacks—against targets, including pipelines, railways, and other US critical infrastructure. Adversarial governments, most notably the PRC, are developing other AI technologies that could undermine US cyber defenses, including generative AI programs that support malicious activity such as malware attacks.
- The increased use of Smart City technologies—including big data, cloud computing, and sensors that inform city operations—creates new attack opportunities for adversarial state and non-state cyber actors to gain access to or carry out disruptive attacks against local government and critical infrastructure networks.
- In recent years, ransomware incidents have become increasingly prevalent among US state, local, tribal, and territorial governments and critical infrastructure entities, disrupting services. K-12 school districts have been a near constant ransomware target due to school systems' IT budget constraints and lack of dedicated resources, as well as ransomware actors' success at extracting payment from some schools that are required to function within certain dates and hours.

Threat Actors Likely To Converge on 2024 Election Season

Our electoral processes remain an attractive target for many adversaries, and we expect many of them will seek to influence or interfere with the 2024 election. Some DVEs may attempt to disrupt civic and democratic processes, mobilized by their perceptions of the upcoming election cycle. Nation-state threat actors likely will seek to use novel technologies and cyber tools to enhance their capabilities and malign influence campaigns, ultimately to undermine our confidence in a free and fair election. Cyber actors likely will seek to exploit election-related networks and data, including state, local, and political parties' networks and election officials' personal devices and e-mail accounts.

- Some DVEs, particularly those motivated by conspiracy theories and anti-government or partisan grievances, may seek to disrupt electoral processes. Violence or threats could be directed at 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.
- Russia, China, and Iran likely see the upcoming election season in 2024 as an opportunity to conduct overt and covert influence campaigns aimed at shaping favorable US policy outcomes and undermining US stability, and they will likely ramp up these efforts in advance of the election. These adversarial states are likely to use AI technologies to improve the quality and breadth of their influence operations targeting US audiences *(see "Foreign Misinformation, Disinformation, and Malinformation" for additional information on the tactics and technologies they are likely to use in the run-up to the election)*.
- Though we continue to strengthen the integrity of our elections infrastructure, cyber actors, both government-affiliated and cyber criminals, likely will remain opportunistic in their targeting of election-related networks and data, routinely attempting to exploit misconfigured or vulnerable public-facing websites, webservers, and election-related information technology systems. These actors are likely to engage in social engineering campaigns, including spear-phishing and smishing state government officials.

ESPIONAGE AGAINST CRITICAL INFRASTRUCTURE

In addition to targeting US critical infrastructure for destructive and disruptive attacks, adversaries continue to use cyber and physical espionage tactics to access and steal sensitive information from US critical infrastructure networks. Such information enables pre-positioning for future attacks, gaining insight into our attack response capabilities, and exfiltrating sensitive data for criminal profit or follow-on intelligence activities. Techniques include the use of AI-generative software programs to enhance social engineering tactics, which trick targeted individuals into disclosing sensitive information or clicking on malicious web links, for intelligence collection.

- Russian government-affiliated cyber espionage likely will remain a persistent threat to federal, state, and local governments, as well as entities in the defense, energy, nuclear, aviation, transportation, healthcare, education, media, and telecommunications industries.
- Chinese government cyber actors likely will continue to target key critical infrastructure sectors in the United States, including healthcare and public health, financial services, the defense industrial base, government facilities, and communications. Beijing's expansion of maritime logistics capabilities and the use of commercial Chinese logistics technologies increase the risk of espionage and potential disruption operations at ports.
- Iranian government cyber actors continue to employ social engineering tactics, utilize easily accessible scanning and computer hacking tools, and exploit publicly known software and hardware vulnerabilities to conduct cyber espionage against US critical infrastructure entities.

THREATS TO ECONOMIC SECURITY

OVERVIEW

America's prosperity and economic security are integral to homeland security. Within this section, we considered state and non-state threat actors who view our economy and commercial activities as vulnerable to manipulation, disruption, and exploitation, and view our technology and intellectual property as critical resources for growing their economic, military, and political power. We also considered financially motivated cyber criminals who cost US businesses millions of dollars each year, while also exposing their sensitive information.

Complex economic threats from state and non-state actors, primarily the PRC and financially motivated cyber criminals, harm US producers and consumers and degrade the competitiveness of our 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.

ECONOMIC MANIPULATION, COERCION, AND MALIGN INFLUENCE

The PRC likely will continue to use a variety of tools in an attempt to give Chinese firms competitive advantages over the United States, including extensive subsidies for state-owned enterprises and favored domestic firms, as well as barriers against US firms operating in China.

- The Chinese government recently implemented its Counter Espionage Law Update to protect data it deems relevant to its national security interests and reduce foreign access to Chinese economic, financial, and business data. Since early 2023, Chinese officials have impeded the operations of several US and Western due-diligence and consulting firms and, in at least one instance, seized electronic devices. A sustained effort by Beijing to quarantine Chinese data likely will damage US economic interests and US-China business ventures by reducing US firms' and investors' ability to vet Chinese entities and carry out fraud and corruption investigations. The updated law's ambiguous language on what constitutes national security-related information also creates legal risks for US researchers, academics, and journalists whose work supports US businesses.
- Beijing almost certainly will continue to use economic coercion as retaliation for perceived political or military challenges to its interests. This could include trade restrictions, public boycotts, and arbitrary, sometimes undeclared "administrative discrimination" procedures to block select US companies and investors from accessing China's markets. China likely will continue to pressure China-based US consultancies from investigating and reporting on China's use of forced labor in the hopes of reducing criticism of Beijing, the efficacy of the US Uyghur Forced Labor Prevention Act, and similar US initiatives.
- China's control and manipulation of critical supply chains will remain an economic security threat to the Homeland. Beijing has recently introduced export control measures on gallium and germanium—critical inputs for semiconductors and low-carbon energy technologies—giving the PRC the ability to restrict exports of these critical minerals to foreign buyers. The PRC has previously restricted exports of rare earth minerals during bilateral disputes.
- China also exploits sister city and other subnational engagements to access key services and technologies and influence national- and state-level economic policies—activities we expect to continue, increasing the need for improved coordination across US government entities.

ECONOMIC ESPIONAGE

Foreign adversaries, primarily the PRC, likely will continue efforts to target and steal sensitive US information, research, and technology. These adversaries almost certainly will continue to use students, researchers, and commercial entities as cover for their efforts to gain access to valuable US information that can damage our competitiveness, result in billions of dollars in lost profits, and transport cutting-edge technology and research to adversarial military and economic programs.

- Intellectual property theft and forced technology transfer continue to threaten global innovation and disadvantage US businesses. Beijing likely will use its opaque and discretionary administrative licensing processes to force technology transfers in exchange for business approvals. Similarly, economic espionage—largely through cyber intrusions that target confidential US business information, including trade secrets, technical data, and other proprietary information—costs US industries hundreds of billions of dollars annually.
- The PRC's use of research partnerships, academic collaborations, and talent recruitment programs to facilitate illicit transfers of US technology for use in Chinese civilian and military industries also poses a significant economic risk. Individuals participating in these programs, though they lack formal intelligence training, threaten US information integrity and national security through their access to sensitive US research and technology, proprietary business and trade data, and other valuable information they transfer to China to support their industries and militaries at the Homeland's expense.

FINANCIALLY MOTIVATED CYBER ATTACKS

In addition to disrupting the activities of targeted victims and their critical infrastructure sectors, financially motivated criminal cyber actors will likely impose significant financial costs on the US economy in the coming year. Ransomware groups that target US networks, infrastructure, and proprietary information are developing new methods to improve their ability to financially extort victims. These groups have increased their use of multilevel extortion, in which they encrypt and exfiltrate their targets' data and typically threaten to publicly release stolen data, use DDoS attacks, or harass the victim's customers to coerce the victim to pay.

- E-mail hacking schemes remain one of the costliest cybercrime activities, with losses totaling over $2.7 billion in 2022. In these attacks, cyber criminals use social engineering or computer intrusion techniques to compromise legitimate business e-mail accounts and conduct unauthorized money transfers. The average business experiences a recovery period of 22 days before resuming operations following a ransomware attack, which frequently costs 50 times more than the ransom demand. The global average cost of a data breach in 2023 was $4.45 million, a 15 percent increase over the last three years.
- Between January 2020 and December 2022, the number of known ransomware attacks in the United States increased by 47 percent. Ransomware attackers extorted at least $449.1 million globally during the first half of 2023 and are expected to have their second most profitable year. This is due to the return of "big game hunting"—the targeting of large organizations—as well as cyber criminals' continued attacks against smaller organizations. Ransomware actors continue to target a variety of victims, almost certainly reflecting malicious cyber actors' target refinement to entities perceived as the most vulnerable or likely to pay a ransom.
- In 2022, some ransomware groups adopted new tactics, such as intermittent encryption, to encrypt systems faster and reduce the chances of being detected.[f] These groups also used this technique to entice affiliates to join their Ransomware-as-a-Service operations and to improve the efficiency of their respective cyber operations.[g] In addition, some groups increased their use of a specific programming language to enhance their ability to adapt and individualize their attacks.

f **Intermittent encryption** consists of encrypting only parts of the targeted files' content. The process takes less time than full encryption but still locks data.

g **Ransomware-as-a-Service** is a business model used by ransomware developers, which includes leasing ransomware variants in the same way that legitimate software developers lease Software-as-a-Service products. Ransomware-as-a-Service provides cyber actors without sophisticated technical knowledge the ability to launch ransomware attacks by subscribing to a service, often for a nominal fee or percentage of the ransomed amount.

Climate Change, Natural Disasters Compound Threat Landscape

The impacts of climate change and natural disasters pose acute and systemic threats to the United States, often converging with more traditional national security threats. Climate-related disasters, such as heat waves, droughts, wildfires, coastal storms, and inland flooding, have the potential to disrupt regional economies, foster health crises like disease outbreaks, and tax law enforcement resources.

- Wildfires, drought, heavy precipitation, and other extreme weather events increase risks to our supply chains and have the potential to impact the availability of goods and services, generating cascading economic effects. Intensified storms and extreme seasonal weather will continue to disrupt maritime shipping routes and threaten port infrastructure, including at strategic chokepoints like the Panama Canal.
- Natural disasters or extreme weather in vulnerable nations across the world, but particularly in Latin American and Caribbean states, that result in infrastructure damage, food insecurity, and disruptions to local economies probably will drive continued migration to the United States. These events have the potential to stretch US and law enforcement resources, particularly along our southern border.
- Climate change is reshaping commercial and political interests in the Arctic. Warming seas allow increased access to the Arctic, but also intensify harsh operating environments, which likely will increase the risk of accidents that require search and rescue and pollution response capabilities. Coastline erosion and the thawing of permafrost will continue to damage Alaskan infrastructure—to include energy and transportation networks—harming commercial activities and local communities. Meanwhile, both Russia and China have signaled their intent to exploit expanding access to Arctic regions and resources, raising the risk that the Arctic could grow increasingly militarized.

Page intentionally left blank

Homeland Security

OFFICE *of* INTELLIGENCE *and* ANALYSIS

23-333-IA