Homeland Threat Assessment

October 2020

Homeland Security

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

Contents

Foreward

In my role as Acting Secretary, I receive intelligence, operational, law enforcement, and other information on a daily basis. This Homeland Threat Assessment (HTA), the first of its kind for the U.S. Department of Homeland Security (DHS), draws upon all sources of information and expertise available to the Department, including from intelligence, law enforcement, and our operational Components. The result is a "Whole-of-DHS" report on the threats to the Homeland. This HTA is as close as the American people will get to seeing and understanding the information that I see as Secretary and that our employees see in their national security missions. As you read through the HTA you should have faith in knowing that these threats were identified using the best intelligence, operational information, and employee knowledge available to the Department.

Identifying Threats using a Whole-of-DHS Approach

The men and women serving in our operational Components are the experts in their national security and homeland security missions, making their insights critical in threat identification and prevention. Our operational Components provided information about the threats they see and combat in performance of their mission. DHS is the first and last line of defense against many threats facing our

country. Our ability to mitigate these threats is predicated on our ability to understand them and to inform the American people. I hope all Americans take a moment to review this HTA and visit DHS.gov to learn how they can protect themselves from these threats.

Today's Threat Environment

Combatting terrorism will always be a priority to the Department of Homeland Security. Foreign terrorist organizations (FTO) still have the intent to attack the Homeland within and from beyond our borders. In the 19 years since September 11th, 2001, the United States Government (USG), DHS, and our foreign partners have taken the fight directly to those responsible for the attacks on that day, and to other FTOs who seek to destroy our country based on an ill-informed and twisted ideology. We have enhanced our ability to identify and prevent individuals affiliated with these organizations from traveling or immigrating to the United States. We have enhanced security and processes at our airports, ports of entry, and beyond our borders. We have built the world's greatest counterterrorism ecosystem to keep Americans safe. More specifically, DHS has partnered with other USG agencies and foreign governments to raise the baseline for screening and vetting in the United States. In the last few years we have enhanced existing vetting programs, created the National Vetting Center (NVC), expanded biographic

"DHS has a vital mission: to secure the nation from the many threats we face. This requires the dedication of more than 240,000 employees in positions that range from aviation and border security to emergency response, from cybersecurity analyst to chemical facility inspector. Our duties are wide-ranging, and our goal is clear — keeping America safe."

Secretary Chad Wolf, State of the Homeland, September 9, 2020

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

and biometric information sharing programs, and enacted national-level policies requiring foreign governments to share essential information for vetting purposes or face potential travel restrictions.

Trade and economic security is Homeland Security. We are increasingly concerned about the threat posed by nation state actors in an emerging era of great power competition. DHS is specifically concerned with the direct and indirect threat posed to the Homeland by the People's Republic of China (PRC). The Chinese Communist Party (CCP)-led PRC is challenging America's place as the world's global and economic leader. Threats emanating from China include damaging the U.S. economy through intellectual property theft, production and distribution of counterfeit goods, and unfair trade practices. DHS has a mandate to mitigate these threats and we will do so with a clear-eyed view that China is a long-term strategic competitor to the U.S.

Domestic violent extremism is a threat to the Homeland. As Americans, we all have the right to believe whatever we want, but we don't have a right to carry out acts of violence to further those beliefs. The Department works with other Government, non-Government, and private sector partners to prevent individuals from making this transition from protected speech to domestic terrorism reflected by violence. As Secretary, I am concerned about any form of violent extremism. That is why we design our programs to be threat agnostic – ensuring that we can combat a broad range of domestic threats. However, I am particularly concerned about white supremacist violent extremists who have been exceptionally lethal in their abhorrent, targeted attacks in recent years. I am proud of our work to prevent terrorizing tactics by domestic terrorists and violent extremists who seek to force ideological change in the United States through violence, death, and destruction.

Exploitation of Lawful and Protected Speech and Protests. During the course of developing the HTA we began to see a new, alarming trend of exploitation of lawful protests causing violence, death, and destruction in American communities. This anti-government, anti-authority and anarchist violent extremism was identified by DHS in September 2019 when we published our Strategic Framework for Countering Terrorism and Targeted Violence. As the date of publication of this HTA, we have seen over 100 days of violence and destruction in our cities. The co-opting of lawful protests led to destruction of government property and have turned deadly.

Indeed, DHS law enforcement officers suffered over 300 separate injuries and were assaulted with sledgehammers, commercial grade fireworks, rocks, metal pipes, improvised explosive devices, and more. This violence, perpetrated by anarchist extremists and detailed in numerous public statements that remain available on the DHS website, significantly threatens the Homeland by undermining officer and public safety—as well as our values and way of life. While the HTA touches on these issues, we are still in the nascent stages of understanding the threat this situation poses to Americans, the Homeland, and the American way of life.

Cyber security threats from nation-states and non-state actors present challenging threats to our Homeland and critical infrastructure. DHS has a critical mission to protect America's infrastructure, which includes our cyber-infrastructure. We are concerned with the intents, capabilities, and actions of nation-states such as China, Russia, Iran, and North Korea. Nation-state targeting of our assets seeks to disrupt the infrastructure that keeps the American economy moving forward and poses a threat to national security. On top of the threats to critical infrastructure, cybercriminals also target our networks to steal information, hold organizations

hostage, and harm American companies for their own gain.

Nation-states will continue to try to undermine American elections. Threats to our election have been another rapidly evolving issue. Nation-states like China, Russia, and Iran will try to use cyber capabilities or foreign influence to compromise or disrupt infrastructure related to the 2020 U.S. Presidential election, aggravate social and racial tensions, undermine trust in U.S. authorities, and criticize our elected officials. Perhaps most alarming is that our adversaries are seeking to sway the preferences and perceptions of U.S. voters using influence operations. Americans need to understand this threat and arm themselves with all information available to avoid falling prey to these tactics.

While Russia has been a persistent threat by attempting to harm our democratic and election systems, it is clear China and Iran also pose threats in this space. The IC's Election Threat Update from August 2020 and Microsoft's announcement of cyber-attacks from China, Russia, and Iran provide further evidence of this threat and underscore the importance in public and private partnerships to secure democratic processes. DHS's #Protect2020 website can help you understand the threat to our elections and increase your preparedness and awareness.

Transnational Criminal Organizations (TCOs) continue to profit at the expense of American lives. Mexican cartels and other TCOs will continue to smuggle hard narcotics like fentanyl, heroin, and methamphetamine into our communities, contributing to an alarming level of overdoses in the United States. No American community is immune from the impact of these drugs. Furthermore, cartels will continue to use dangerous human smuggling methods to facilitate migrants to our borders, putting these migrants and our officers and agents at significant risk given the current COVID-19 pandemic.

The threat of illegal and mass migration to the United States. Traditional migration push factors like insecurity and economic conditions continue to push individuals north to the United States. While we are addressing illegal migration through a network of initiatives, we are concerned that during a pandemic this poses a more specific threat to the migrants, the communities they transit, to U.S. border communities, and to our officers and agents who encounter migrants when they enter the United States. To mitigation this threat we instituted enhanced restrictions at our borders, limited travel to only essential travelers and implemented a Center for Disease Control (CDC) order that protects Americans from COVID-19.

Natural occurrences continue to harm the life and property of Americans. In 2020 alone we have seen an unprecedented storm season that has taken the livelihoods of many Americans in our Gulf states and a historic wildfire season that has caused devastation on the West Coast. Americans in-between our coasts also face the threat of natural disasters from a variety of causes. On top of the threat to life and safety, these events have devastating impacts on local and national economies. The Department is at the forefront of providing information to help Americans prepare, and we stand ready to respond after these events occur.

Likewise, a foreign-born virus reached our shores in 2020. COVID-19 is the most recent and deadly, in a list of infectious diseases that have threatened the lives of Americans. We have seen unprecedented impact to life, health, and public safety from COVID-19 and taken action to prevent our healthcare system from being overburdened from COVID-19 patients. DHS was at the forefront mitigating threat and we took decisive action to restrict air and sea travel from disease hot-spots, close our land borders to non-essential travel, provide lifesaving PPE to Americans, prevent fraudulent PPE from entering our supply chains, and identify fraudsters who are trying to exploit this situation for their own personal gain.

Conclusion

As you read the HTA you will become more acutely aware of the threats facing the American people, the Homeland, and the American way of life. You will also gain a clearer picture of the broad mission of the Department of Homeland Security. It is my privilege and honor to serve as the Acting Secretary of an organization whose employees willingly and bravely put themselves in harm's way every day to protect us all. The men and women of the Department live up to our motto: With honor and integrity, we will safeguard the American people, our Homeland, and our values.

Structure of the Threat Assessment

The Department of Homeland Security (DHS) is the first and last line of defense against the many threats facing our country. Our ability to mitigate these threats is predicated on our ability to understand them and to inform the American people. The DHS Homeland Threat Assessment[1] (HTA) identifies the primary threats facing the United States of America at and inside our borders. This Assessment draws upon all sources of information and expertise available to the Department, including from intelligence, law enforcement, and our operational components.

The purpose of the HTA is to provide the American people with an overview of the information collected and analyzed by DHS employees around the world and provided to the Secretary of Homeland Security.

The HTA is primarily informed by intelligence analysis prepared by the DHS Office of Intelligence and Analysis (I&A) and by the Component intelligence offices, which identified the leading security threats to the Homeland based on a review of all-source intelligence information and analysis. Given the array of potential issues, I&A's scoped its analysis to focus on key threats covered by the intelligence elements of the Department, which expert analysts considered most likely and with the potential to significantly affect U.S. security.

The HTA was also informed by the expertise and insights of the Department's Operational Components, which assess and respond to threats on a daily basis, as well as the informed views of the DHS Office of Strategy, Policy, and Plans (PLCY), which leads threat identification and prevention activities.

This inaugural HTA presents a holistic look from across the Department and provides the American people with the most complete, transparent, and candid look at the threats facing our Homeland. It breaks down the major threats to the Homeland in the following sections:

1. ***The Cyber Threat to the Homeland***
2. ***Foreign Influence Activity in the Homeland***
3. ***Threats to U.S. Economic Security***
4. ***The Terrorist Threat to the Homeland***
5. ***Transnational Criminal Organization Threats to National Security***
6. ***Illegal Immigration to the United States***
7. ***Natural Disasters***

[1]As used in this document, "Threat Assessment" has the meaning given in the DHS Lexicon: a "product or process of evaluating information based on a set of criteria for entities, actions, or occurrences, whether natural or manmade, that have or indicate the potential to harm life, information, operations and/or property."

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

The Cyber Threat to the Homeland

Cyber threats to the Homeland from both nation-states and non-state actors will remain acute. U.S. critical infrastructure faces advanced threats of disruptive or destructive cyber-attacks. Federal, state, local, tribal and territorial governments, as well as the private sector, will experience an array of cyber-enabled threats designed to access sensitive information, steal money, and force ransom payments.

Nation State Threats

Russia—which possesses some of the most sophisticated cyber capabilities in the world—can disrupt or damage U.S. critical infrastructure networks via cyber-attacks. Russian state-affiliated actors will continue targeting U.S. industry and all levels of government with intrusive cyber espionage to access economic, policy, and national security information to further the Kremlin's strategic interests.

- Russia probably can conduct cyber-attacks that would result in at least localized effects over hours to days and probably is developing capabilities that would cause more debilitating effects.
- We expect Russian cyber actors to use a range of capabilities including social engineering, publicly known software and hardware vulnerabilities, poorly configured networks, and sophisticated "zero-day" attacks that exploit security weaknesses in software.
- Under Russian law, the Federal Security Service (FSB) can compel Russian firms doing business in the United States—or Russians working with U.S. firms—to comply with FSB information sharing and operational mandates, presenting additional routes for cyber espionage.

China already poses a high cyber espionage threat to the Homeland and Beijing's cyber-attack capabilities will grow. Chinese cyber actors almost certainly will continue to engage in wide-ranging cyber espionage to steal intellectual property[2] and personally identifiable information (PII) from U.S. businesses and government agencies to bolster their civil-military industrial development, gain an economic advantage, and support intelligence operations. China possesses an increasing ability to threaten and potentially disrupt U.S. critical infrastructure.

- We expect China's cyber operations against U.S. companies to focus on the critical manufacturing, defense industrial base, energy, healthcare, and transportation sectors.
- Beijing has targeted information technology and communications firms whose products and services support government and private-sector networks worldwide, while concurrently advocating globally for Chinese information technology companies that could serve as espionage platforms.
- Under China's 2017 National Intelligence Law, Beijing can compel businesses based in China and Chinese citizens living abroad to provide intelligence to the Chinese government.
- We remain concerned about China's intent to compromise U.S. critical infrastructure in order to cause disruption or destruction.
- China's efforts to dominate the 5G world pose new challenges to U.S. efforts to national security, privacy, resistance to malign influence, and human rights. The exponential increases in speed, connectivity, and productivity could render American systems particularly vulnerable to Chinese cyber threats.

While Russia and China are the most capable nation-state cyber adversaries, Iranian and North Korean cyber actors also pose a threat to U.S. systems, networks, and information. Iran continues to present a cyber espionage threat and is developing access in the Homeland that could be repurposed for destructive cyber-attacks. North Korean cyber capabilities, while sophisticated, probably will remain confined to criminal

generation of revenue. If Pyongyang's intent changes, however, it probably could quickly build capabilities to conduct broader espionage activity or threaten infrastructure with disruptive cyber-attacks.

Cybercrime

Cybercriminals increasingly will target U.S. critical infrastructure to generate profit, whether through ransomware, e-mail impersonation fraud, social engineering[3], or malware. Underground marketplaces that trade in stolen information and cyber tools will continue to thrive and serve as a resource, even for sophisticated foreign adversaries.

- Ransomware attacks—which have at least doubled since 2017—often are directed against critical infrastructure entities at the state and local level by exploiting gaps in cybersecurit
- Victims of cybercriminal activity in 2018 reported over $2.7 billion in losses—more than twice the amount lost in 2017. This figure does not represent the full scope of loss because some victims do not report incidents.

Cyber Threat to the U.S. Democratic Processes

Some state or non-state actors likely will seek to use cyber means to compromise or disrupt infrastructure used to support the 2020 U.S. Presidential election and the 2020 U.S. Census. Given the national importance of these events, any related cyber activities—or mere claims of compromise—might fuel influence operations aimed at depressing voter turnout or census participation, misinforming about democratic processes, or shaping perceptions about the integrity or outcome of the election or census (see subsequent section regarding Foreign Influence in the Homeland).

- Advanced persistent threat or other malicious cyber actors likely will target election-related infrastructure as the 2020 Presidential election approaches, focusing on voter PII, municipal or state networks, or state election officials directly. Operations could occur throughout the 2020 election cycle—through pre-election activities, Election Day, and the post-election period.
- Adversaries' cyber capabilities vary greatly—as does the cyber defensive posture of electoral boards to stymie such actors. Adversaries could attempt a range of election interference activities, including efforts to target voter registration systems; to compromise election system supply chains; to exploit poor cybersecurity practices on protected election systems or networks; or to hack official election websites or social media accounts.
- Unidentified cyber actors have engaged in suspicious communications with the U.S. Census public-facing network over at least the last year, including conducting vulnerability scans and attempting unauthorized access. Cyber activity directed at the U.S. Census could include attempts to gain illicit access to census-gathered bulk data; to alter census registration data; to compromise the census infrastructure supply chain; or conducting denial-of-service attacks.

OPPORTUNITY FOR CYBER ACTORS TO EXPLOIT COVID-19

Both cybercriminals and nation-state cyber actors—motivated by profit, espionage, or disruption—will exploit the COVID-19 pandemic by targeting the U.S. healthcare and public health sector; government response entities, such as the U.S. Department of Health and Human Services and the Federal Emergency Management Agency; and the broader emergency services sector.

- Cybercriminals most likely will deploy ransomware for financial gain, whereas nation-state cyber actors might seek to capture insights into U.S. response plans and scientific information related to testing, therapeutics, and vaccine development.
- We expect that cybercriminals and nation-state cyber actors will target victims in the United States with COVID-19-themed spear-phishing e-mails, which we already have observed overseas. These e-mails appear to claim to be from official government sources, including the U.S. Centers for Disease Control and Prevention and the U.S. Department of State.

[2]On Thursday, September 17, 2020, FBI Director Wray described China's unmatched success in stealing American intellectual property as "the greatest transfer of wealth in the history of the world." U.S. House of Representatives, Committee on Homeland Security, Annual Hearing on Threats to the Homeland.

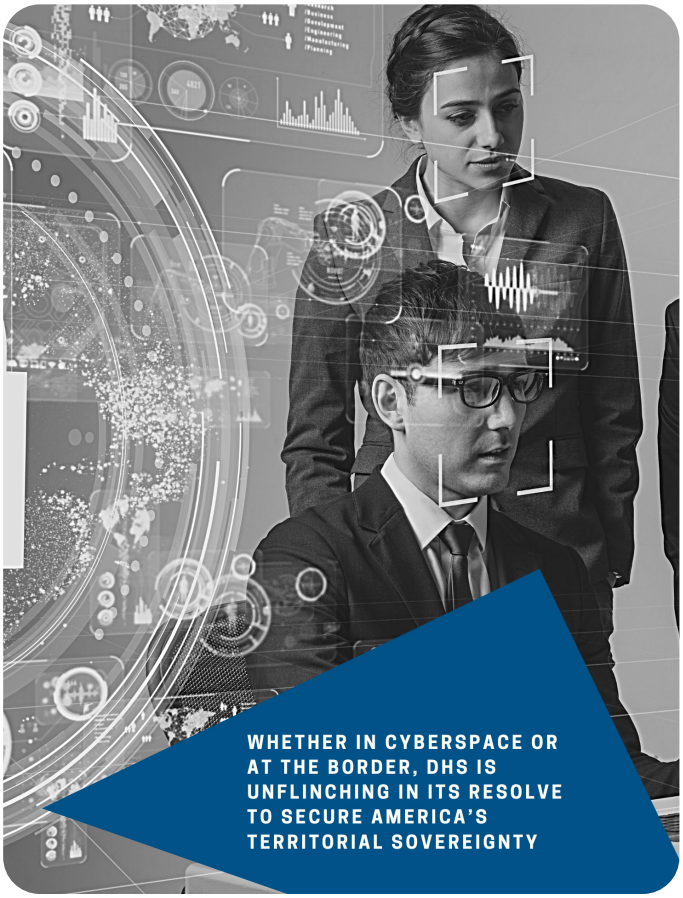
[3]Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions.

Foreign Influence Activity in the U.S.

Foreign influence activity will target U.S. foreign and domestic policy, international events such as COVID-19, and democratic processes and institutions, including the 2020 Presidential election. Russia is the likely primary covert influence actor and purveyor of disinformation and misinformation within the Homeland. We assess that Moscow's primary objective is to increase its global standing and influence by weakening America—domestically and abroad—through efforts to sow discord, distract, shape public sentiment, and undermine trust in Western democratic institutions and processes.

Amplifying U.S. Socio-Political Division

- Russian influence actors will continue using overt and covert methods to aggravate social and racial tensions, undermine trust in U.S. authorities, stoke political resentment, and criticize politicians who Moscow views as anti-Russia. Although some of this activity might be framed in the context of the U.S. election—seemingly in support of or opposition to political candidates—we assess that Moscow's overarching objective is to weaken the United States through discord, division, and distraction in hopes that America becomes less able to challenge Russia's strategic objectives.



- Russian influence actors will engage in media manipulation—across social media platforms, proxy websites[4], and traditional media, to include state-controlled outlets—to exacerbate U.S. social, political, racial, and cultural fault lines.[5]
- Russian actors will attempt to undermine national unity and sow seeds of discord that exploit perceived grievances within minority communities, especially among African Americans. Russian influence actors often mimic target audiences and amplify both sides of divisive issues to maximize discord, tailoring messaging to specific communities to "push and pull" them in different ways.
- The Russian government promulgates misinformation, threats, and narratives intended to incite panic or animosity among social and political groups. For example, Russian actors amplified narratives such as U.S. law

[4] Proxy Website: Foreign news outlets, think tanks, and investigative journalist websites on behalf of foreign governments or foreign government-linked businessmen and oligarchs in a non-overt or non-attributed way and that echo foreign government narratives, talking points, and disinformation. State media often cite these proxy websites and portray them as credible and independent sources of information.

enforcement ignoring ICE detention requests and releasing an illegal immigrant accused of rape; assaults on supporters and opponents of the President; and portrayals of U.S. law enforcement as racially biased. Russian influence actors also have exploited national tragedies, such as the 2017 mass shooting in Las Vegas, and protest movements—sometimes magnifying both a protest and a counter-protest—such as the 2017 protest activity in Charlottesville.

COVID-19 Influence Narratives

Russian online influence actors are advancing misleading or (what they perceive as) inflammatory narratives about the COVID-19 pandemic probably to stoke fear, undermine the credibility of the U.S. government, and weaken global perceptions of America. Moscow probably will study the American public's reaction to its COVID-19 disinformation to improve future influence campaigns aimed at shaking public confidence in Washington, which it can unleash opportunistically during a crisis, hostilities, or a period of degraded relations.

- Russian online influence actors have claimed that the U.S. President is incapable of managing the COVID-19 crisis and sought to exacerbate public concerns by amplifying content critical of the U.S. response to the public health crisis and the economic downturn. In contrast, the actors highlighted China's and Russia's alleged success against the COVID-19 outbreak and praised President Putin's COVID-19 plan and Russia's ample supply of tests.
- Russian online influence actors spread misinformation and conspiracy theories about the origin of COVID-19, claiming it is a U.S.-engineered biological weapon that U.S. military officials spread in China.

Chinese operatives probably are waging disinformation campaigns using overt and covert tactics—including social media trolls—to shift responsibility for the pandemic to other countries, including the United States. China might increase its influence activities in response to what it views as anti-China statements from the U.S. Government over China's role in the pandemic.

- Since August 2019, more than 10,000 suspected fake Twitter accounts have been involved in a coordinated influence campaign with suspected ties to the Chinese Government. Among these are hacked accounts from users around the world that post messaging and disinformation about the COVID-19 pandemic and other topics of interest to China.
- China's Foreign Ministry, state media, and official Twitter accounts promote overt narratives claiming the coronavirus may have originated in the United States, criticize the U.S. pandemic response, and publicize

FOREIGN INFLUENCE DEFINITIONS:

Foreign Influence. Any covert, fraudulent, deceptive, or unlawful activity of foreign governments—or persons acting on their behalf—undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting U.S. democratic processes or institutions or otherwise affecting socio-political sentiment or public discourse to achieve malign objectives.

- Covert Influence: Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action.
- Overt Influence: Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda.
- Disinformation: A foreign government's deliberate use of false or misleading information intentionally directed at another government's decisionmakers and decision-making processes to mislead the target, force it to waste resources, or influence a decision in favor of a foreign government's interests.
- Misinformation: Foreign use of false or misleading information. Misinformation is broader than disinformation because it targets a wide audience rather than a specific group.

[5] *We note that U.S. Persons linking, citing, quoting, or voicing the same themes, narratives, or opinions raised by these influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the direction or under the control of a foreign threat actor. Furthermore, variants of the topics covered in this report, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors.*

China's COVID-19-related medical assistance to U.S. cities and states. China has doubled the number of official government posts disseminating false narratives about COVID-19 and has carried out persistent and large-scale disinformation and influence operations that correlate with diplomatic messaging.

- China most likely will continue amplifying narratives supportive of its pandemic response while denigrating U.S. official criticism that Beijing views as tarnishing its global image.

Iranian online influence actors are employing inauthentic social media networks, proxy news websites, and state media outlets to amplify false narratives that seek to shift responsibility for the COVID-19 pandemic to the United States and other Western nations. Tehran probably will continue to malign the United States for enforcing economic sanctions, arguing these sanctions hinder Iran's ability to put forward an appropriate public health response to the pandemic.

- Iranian actors have spread COVID-19 disinformation and false narratives through videos, cartoons, and news stories from state media outlets on popular social media platforms to appeal to U.S. and Western audiences.
- Iranian operatives have covertly used proxy networks and sites to advance narratives suggesting that the United States created the virus as a bioweapon, that Western media is spreading lies about COVID-19 in Iran, and that the Iranian response to the pandemic was better than that of the United States.

2020 U.S. Presidential Election

Ahead of the 2020 U.S. elections, adversaries are using covert and overt influence measures to try to sway U.S. voters' preferences and perspectives about candidates, political parties, policies, and the electoral process itself. Influence actors will adjust their goals and tactics as the election nears.

Russia uses online influence operations in its attempt to sway U.S. voter perceptions. As noted earlier, although some Russian influence activity appears to be in support of or in opposition to specific political candidates, Moscow's overarching objective is to undermine the U.S. electoral process and weaken the United States through discord, division, and distraction in hopes America becomes less able to challenge Russia's strategic objectives.

- Russian online influence actors have attacked or praised multiple 2020 U.S. Presidential candidates—including candidates of both major political parties. Russia uses divisive measures to disrupt the electoral process—including denigrating former Vice President Biden and what it sees as an anti-Russia "establishment"—as part of a broader effort to divide and destabilize America. Russian online influence actors' have opined on a wide swath of socio-political issues relevant to the 2020 elections.
- Russian online influence actors probably will engage in efforts to discourage voter turnout and to suppress votes in the 2020 U.S. election using methods they have deployed since at least 2016. Before the 2016 U.S. Presidential election, Russian trolls directed messages at specific audiences with false information about the time, manner, or place of voting to suppress votes. Russian influence actors also posed as U.S. persons and discouraged African

EVOLVING INFLUENCE TRADECRAFT AND TARGETING

Russian influence actors are evolving their methods of interacting with target U.S. audiences and obfuscating detection of their online influence activity.

- We expect that influence actors will evolve their ability to create and operate fake social-media accounts, thereby obfuscating their online influence activity.
- Russian influence actors likely will use U.S.-based servers and other computer infrastructure—including virtual private networks—to mask their location, obscure login activity, and prevent account banning.
- Russian influence actors probably will leverage artificial intelligence to automate the creation and distribution of memes with socially divisive messages on social media. Previously, Russian actors mass produced politically themed picture memes called "demotivators," some of which they produced under the guise of U.S. activist groups.

Americans, Native Americans, and other minority voters from participating in the 2016 election.

Ahead of the election, China likely will continue using overt and covert influence operations to denigrate the U.S. Presidential Administration and its policies and to shape the U.S. domestic information environment in favor of China. China will further use its traditional "soft power" influence toolkit—overt economic measures and lobbying—to promote U.S. policies more aligned with China's interests.

Iran will continue to promote messages supporting its foreign policy objectives and to use online influence operations to increase societal tensions in the United States. Tehran most likely considers the current U.S. Administration a threat to the regime's stability. Iran's critical messaging of the U.S. President almost certainly will continue throughout 2020.

Russian influence actors see divisive issues regarding the 2020 Census, such as the consideration of adding a citizenship question, as an opportunity to target a fundamental democratic process. In addition to potential cyber operations, Russia might use social media messaging—much like it does in the context of US elections—to attempt to discourage public participation in the census, to promote a loss of confidence in census results, or to undermine trust in public institutions.

Influencing State and Local Governments

Foreign governments—principally China—seek to cultivate influence with state and local leaders directly and indirectly, often via economic carrots and sticks such as informal and legal or social agreements that seek to promote cultural and commercial ties. Chinese officials calculate that U.S. state- and local-level officials enjoy a degree of diplomatic independence from Washington and may leverage these relationships to advance policies that are in China's interest during times of strained relations.

- China views a state or locality's economic challenges—including healthcare challenges due to COVID-19—as a key opportunity to create a dependency, thereby gaining influence. Beijing uses Chinese think tanks to research which U.S. states and counties might be most receptive to China's overtures.
- During the beginning of the COVID-19 outbreak, Beijing leveraged sister city relationships with U.S. localities to acquire public health resources. In February, Pittsburgh shipped its sister city, Wuhan, 450,000 surgical masks and 1,350 coverall protective suits. Pittsburgh also established a GoFundMe account that raised over $58,000 to support Wuhan response efforts by providing medical supplies.
- In Chicago, Chinese officials leveraged local and state official relationships to push pro-Chinese narratives. Also, a Chinese official emailed a Midwestern state legislator to ask that the legislative body of which he was a member pass a resolution recognizing that China has taken heroic steps to fight the virus.
- The Chinese government invites U.S. officials and business leaders on carefully choreographed trips to China, promising them lucrative investment projects and business deals. Although visits this year largely have been postponed due to COVID-19, the Chinese government probably will continue to cultivate state and local relationships virtually and by offering enticements, which might include bailing out U.S. companies, investing in real estate in economically hard-hit areas, and selling medical equipment and supplies at reduced cost.

Threats to U.S. Economic Security

COVID-19 Effects on Economic Security and Health Security

The COVID-19 pandemic has destabilized U.S. supply chains and introduced opportunities for economic competitors to undermine the United States. This will lead to dramatic and sustained disruptions to the global economy and could challenge U.S. economic and supply chain security.

- In response to measures to control cross-border flows of people and goods, which have significantly disrupted international trade and supply chains, countries will invest in domestic industries and in countries they consider more reliable suppliers, considering the ability to control illicit activity and protect intellectual property rights. Varying social distancing and lockdown policies will continue to strain and disrupt goods supply chains at multiple levels.
- Access to personal protective equipment (PPE) and pharmaceuticals sourced from abroad or that depend on global supply chains will remain especially vulnerable to disruptions due to sustained demand, foreign government actions to secure these supplies for their countries' use, and the length of time required to reconstitute these production capabilities elsewhere.
- Counterfeiters and other malicious actors have exploited the high demand for essential goods during the outbreak by selling substandard or non-approved PPE, vitamins, medicines, and other goods to desperate customers, posing a threat to public health and undermining legitimate businesses. Many manufacturers and distributors have failed to verify that the goods they are selling meet performance specifications. China has been a particularly persistent source of such counterfeit goods.
- Targeting illicit Chinese manufacturers who produced and disseminated fraudulent or prohibited COVID-19 PPE and medical supplies to the United States has resulted in the seizure of over 1,000,000 FDA-prohibited COVID-19 test kits and 750,000 counterfeit masks.
- China is collecting information on U.S. supply chain shortages and is using the COVID-19 crisis to build additional leverage with the United States, given that Beijing controls many critical commodities. China could exploit future shortages of critical supplies by conditioning their provision on U.S. acquiescence in other matters important to Beijing.

The political nature of international critiques regarding COVID-19 responses may depress reporting in future public health crises. This highlights the importance of the Global Health Security Agenda and need for continued effort to drive increased participation.

- Several countries employed denial and deception efforts to conceal COVID-19 statistics and/or limit COVID-19 testing to maintain a low case count. Countries that were transparent in reporting their COVID-19 case count have occasionally been the subject of criticism by adversarial countries. These influence operations may induce countries to limit transparency during future outbreaks, increasing the risk that outbreaks will turn into pandemics as they will not be addressed robustly while still locally or regionally contained.

Exploiting U.S. Academic Institutions and Research

China will continue seeking U.S. research and expertise vital to its economic and military advancement by using a wide range of government, non-government, and private actors and platforms. China—which has mobilized vast resources to support its industrial development and defense goals—will continue exploiting U.S. academic institutions and the visa system to transfer valuable research and intellectual property (IP) that Beijing calculates will provide a military or economic advantage over the United States and other nations. Beijing uses some visiting professors, scholars, and students in the United States as non-traditional collectors (NTCs)—individuals who conduct their espionage-like activities by exploiting open systems rather than clandestinely—by virtue of their participation in targeted research and development activities. These NTCs most often include a subset of graduate- and post-graduate-level researchers studying in certain science, technology, engineering, and mathematics (STEM) fields. Although some NTCs are unwitting,

others are cognizant of their role and some have admitted to stealing research from U.S. institutions to advance Chinese research. These non-traditional collectors depart the United States and return to China, taking research and materials without the consent of the academic institutions, often deliberately hiding the material prior to their departure to prevent its detection.

- In January 2020, a Chinese post-graduate researcher in Boston was indicted for allegedly attempting to smuggle stolen vials of biological research; he stated that he planned to bring them to China to conduct research in his own laboratory and publish the results under his own name.
- In June 2020, a Chinese student was arrested at Los Angeles International Airport for visa fraud, having failed to disclose on his visa application that he was an Officer in the People's Liberation Army (PLA). During an outbound interview with U.S. Customs and Border Protection (CBP), he admitted to providing access to research from a California university to the PLA. He said that his supervisor—the director of his military university laboratory in China—instructed him to observe the university's layout and bring the information to replicate it in China.

China's government-run talent recruitment programs facilitate licit and illicit transfer of U.S. technology, IP, and know-how to further China's Science and Technology development and military modernization. The programs recruit overseas academics, scientists, and other experts and reward them for stealing proprietary information and delivering it to the Chinese government to gain an advantage over the United States. Recipient contracts in many cases require them to keep the terms secret and transfer IP rights to the sponsoring Chinese institution. Some program participants are incentivized or obligated to establish "shadow laboratories" in China that mirror U.S. taxpayer-funded research to provide China with early insights into U.S. research before discoveries are shared globally. Several U.S. professors selected by these programs have been charged with crimes, including fraud and theft of trade secrets.

Now that the U.S. government is aware of these methods of exploiting academic institutions and research, Beijing's strategy will likely change. Considering the issuance of Presidential Proclamation 10043 banning the entry of certain students associated with China's military-civil fusion strategy—as well as increased awareness by U.S. industry, academia, and local governments of China's tactics for acquiring technology and IP—we expect NTCs will adjust their methods, including by taking different paths to travel to the United States or shifting their studies abroad while still aiming to collect sensitive U.S. information and intellectual property.

Foreign Investment in the United States

Although Chinese foreign direct investment in the United States over the last two years has decreased from record highs, China will continue to pursue select investment in the United States to gain new technologies that it cannot produce domestically, to develop its own industrial base, and to secure access to critical supply chains.

- Some Chinese firms will adapt to enhanced U.S. national security vetting of foreign direct investment—introduced as part of the Foreign Investment Risk Review Modernization Act (FIRRMA)—by using new types of investment structures and new legal methods. Foreign companies seeking to invest in U.S. businesses might bolster efforts to obfuscate their links to intelligence or security services, such as by using cutout organizations for acquisitions.

Threats to U.S. Supply Chain Integrity

China and Russia will continue to represent the top threats to U.S. supply chain security, given the sophisticated intelligence and cyber capabilities they can use to infiltrate trusted suppliers and vendors to target equipment and systems. Criminal actors also will engage in efforts to compromise supply chains, with such methods as inserting malicious code in a third party's software to conduct operations against firms that use the software. Criminal and state actors also attempt to compromise supply chains through protectionist measures and by exploiting rapid procurement procedures at the local, state, and federal level during disasters.

- We are especially concerned about adversaries' exploitation of information and communications technology (ICT) supply chains given that the goods that rely on these supply chains play a vital role in most aspects of life. Some actors might exploit ICT through "white labeling"—rebranding equipment or altering equipment's visual appearance to obfuscate the original manufacturer—to get compromised goods into supply chains.
- As Chinese firms become more competitive globally and achieve market dominance in

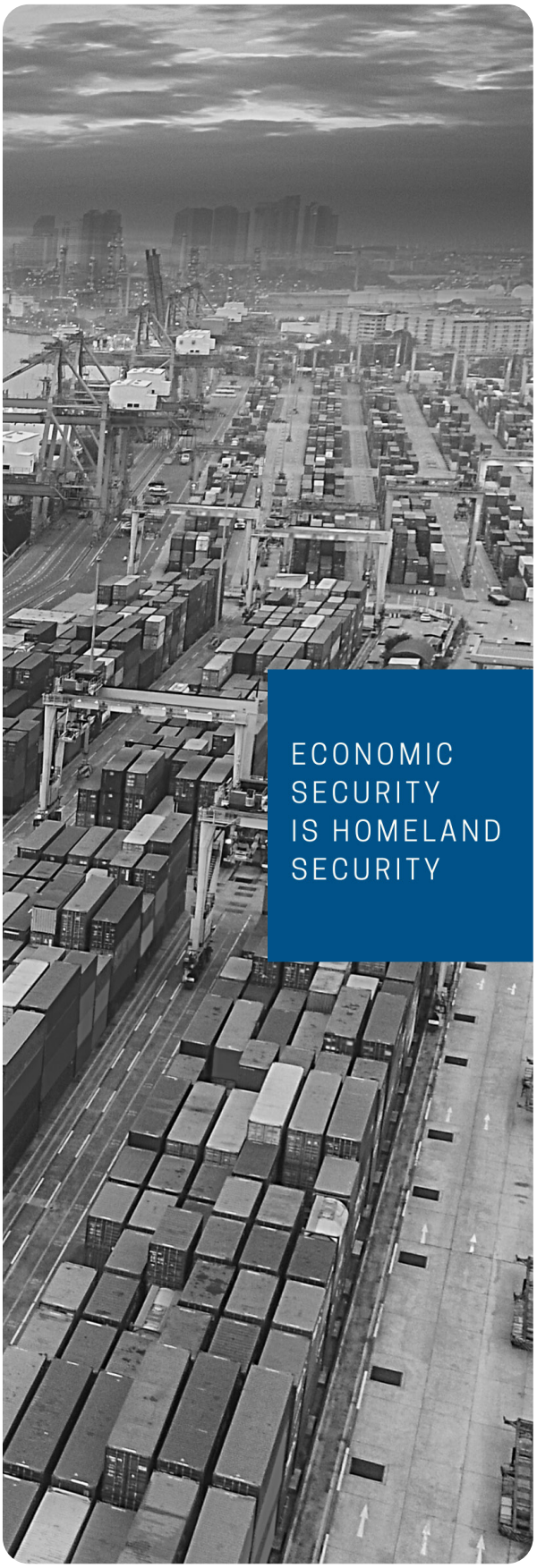
key sectors, the United States will be less able to source and supply key goods and services that are not dependent on Chinese investment or suppliers.

- The United States and other nations competing for globally scarce resources during disasters, will struggle to keep up with economies that lower quality standards and requisition U.S. subsidiaries manufacturing facilities to hoard supplies. During the COVID-19 outbreak, Chinese state-owned enterprises were encouraged to convert manufacturing without having the capacity or quality control to produce medical supplies and equipment. In addition to quality control issues, Chinese suppliers export products under one licensed company's name but source their products from second, third or fourth factories with little to no traceability down the chain of supply. In March, a Canadian manufacturer of face masks with factories in China, reported the Chinese government requisitioned all production and nothing was being exported.
- China began accumulating critical medical supplies rather than ship them to buyers in other countries – indicating apparent knowledge of the outbreak and efforts to hoard critical medical supplies.

Violations of U.S. Trade Laws and Policies

China will remain the leading source of U.S. trade policy violations. Actions by China-based criminal organizations will continue to present the principal challenge to U.S. enforcement of trade laws and policies in the year ahead, despite progress in U.S.-China negotiations aimed at addressing this issue.

- Chinese entities' infringement on the IP rights of U.S. entities costs the U.S. economy as much as $600 billion annually and adversely impacts U.S. industries and competitiveness.
- In Fiscal Year 2019, DHS seized more counterfeit goods originating from China than any other country. Counterfeit goods from China and Hong Kong pose the greatest challenge to IP enforcement and present health and safety risks to the public due to the sub-standard quality of most counterfeit products.



The Terrorist Threat to the Homeland

Ideologically motivated lone offenders and small groups pose the most likely terrorist threat to the Homeland, with Domestic Violent Extremists presenting the most persistent and lethal threat. Foreign terrorist organizations will continue to call for Homeland attacks but probably will remain constrained in their ability to direct such plots over the next year. Iran will maintain terrorist capabilities, including through proxies such as Lebanese Hizballah, as an option to deter the United States from taking action Tehran considers regime-threatening.

Violent Extremism in the United States

The primary terrorist threat inside the United States will stem from lone offenders and small cells of individuals, including Domestic Violent Extremists[6] (DVEs) and foreign terrorist-inspired Homegrown Violent Extremists[7] (HVEs). Some U.S.-based violent extremists have capitalized on increased social and political tensions in 2020, which will drive an elevated threat environment at least through early 2021. Violent extremists will continue to target individuals or institutions that represent symbols of their grievances, as well as grievances based on political affiliation or perceived policy positions.

The domestic situation surrounding the COVID-19 pandemic creates an environment that could accelerate some individuals' mobilization to targeted violence or radicalization to terrorism. Social distancing may lead to social isolation, which is associated with depression, increased anxiety, and social alienation. Similarly, work disruptions, including unexpected unemployment and layoffs, can also increase risk factors associated with radicalization to violence and willingness to engage in acts of targeted violence.

- Violent extremist media almost certainly will spread violent extremist ideologies, especially via social media, that encourage violence and influence action within the United States.
- Violent extremists will continue their efforts to exploit public fears associated with COVID-19 and social grievances driving lawful protests to incite violence, intimidate targets, and promote their violent extremist ideologies.
- Simple tactics—such as vehicle ramming, small arms, edged weapons, arson, and rudimentary improvised explosive devices (IEDs)—probably will be most common. However, lone offenders could employ more sophisticated means, to include advanced and/or high-consequence IEDs and using crude chemical, biological, and radiological materials.
- While ISIS and other Foreign Terrorist Organizations (FTOs) have called for attacks in the West using "all available means," biological-focused attempts would likely involve crudely produced toxins and poisons. Similarly, during the COVID-19 outbreak, domestic extremists have called for the spread of the SARS-CoV-2 virus through unsophisticated means. While significant expertise and infrastructure limits the threat by low-level actors, even rudimentary actions can result in economically significant costs and incite fear without a corresponding risk to health.

Some DVEs and other violent actors[8] might target events related to the 2020 Presidential campaigns, the election itself, election results, or the post-election period. Such actors could mobilize quickly to threaten or engage in violence. Violence related to government efforts to mitigate the COVID-19 pandemic and amidst otherwise ongoing lawful protests has exacerbated the typical

[6] Domestic Violent Extremist (DVE): 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 may not constitute extremism, and may be constitutionally protected.

[7] Homegrown Violent Extremist (HVE): 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 (FTO), but is acting independently of direction by an FTO. 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 from or influence from a foreign actor.

election-season threat environment.

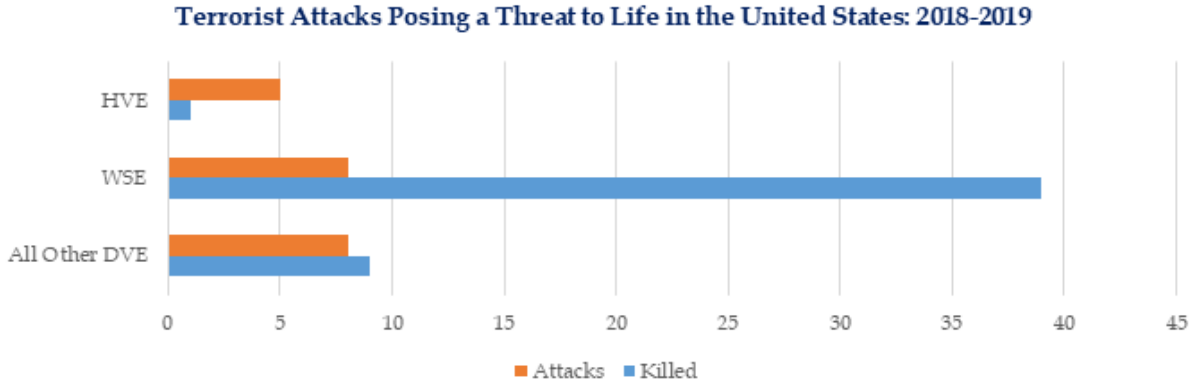
- Some DVEs have heightened their attention to election- or campaign-related activities, candidates' public statements, and policy issues connected to specific candidates, judging from domestic terrorism plots since 2018 targeting individuals based on their actual or perceived political affiliations.
- Open-air, publicly accessible parts of physical election infrastructure, such as campaign-associated mass gatherings, polling places, and voter registration events, would be the most likely flashpoints for potential violence.

Among DVEs, racially and ethnically motivated violent extremists—specifically white supremacist extremists[9] (WSEs)—will remain the most persistent and lethal threat in the Homeland. Spikes in other DVE threats probably will depend on political or social issues that often mobilize other ideological actors to violence, such as immigration, environmental, and police-related policy issues.

- WSEs have demonstrated longstanding intent to target racial and religious minorities, members of the LGBTQ+ community, politicians, and those they believe promote multi-culturalism and globalization at the expense of the WSE identity. Since 2018, they have conducted more lethal attacks in the United States than any other DVE movement.
- Some WSEs have engaged in outreach and networking opportunities abroad with like-minded individuals to expand their violent extremist networks. Such outreach might lead to a greater risk of mobilization to violence, including traveling to conflict zones.
- Other racially or ethnically motivated violent extremists could seek to exploit concerns about social injustice issues to incite violence and exploit otherwise peaceful protests movements.

Another motivating force behind domestic terrorism that also poses a threat to the Homeland is anti-government/anti-authority violent extremism.

- These violent extremists, sometimes influenced by anarchist ideology, have been associated with multiple plots and attacks, which included a significant uptick in violence against law enforcement and government symbols in 2020. This ideology is also exploited by hostile nation-states, which seek to promote it through disinformation campaigns and sow additional chaos and discord across American society.
- Anti-government and/or anti-authority violent extremists are likely to be emboldened by a perceived success exploiting otherwise peaceful protest movements and concealing violent tactics. These violent extremists are increasingly



This chart depicts DVE and homegrown violent extremists (HVEs) attacks in the US since 2018 that posed a threat to life, based on DHS data. 2019 was the most lethal year for domestic violent extremism in the United States since the Oklahoma City bombing in 1995. We are still evaluating data for incidents occurring in 2020. VEs perpetrated 16 attacks, killing 48, whereas HVEs conducted 5 attacks and killed 1 person. Among DVE actors, WSEs conducted half of all lethal attacks (8 of 16), resulting in the majority of deaths (39 of 48). All the DVE attackers had a dominant violent extremist ideology, with many motivated by multiple violent extremist ideologies or violent extremist ideologies unconnected to global violent extremist groups.

taking advantage of large protest crowds to conduct violence against government officials, facilities, and counter-protestors.

- We also remain particularly concerned about the impacts from COVID-19 where anti-government and anti-authority violent extremists could be motivated to conduct attacks in response to perceived infringement of liberties and government overreach as all levels of government seek to limit the spread of the coronavirus that has caused a worldwide pandemic.
- Ideologies driven by such DVE's often are reinforced by a variety of online content, including conspiracy theories and political commentary they view as controversial. Current events that DVEs perceive as infringing on their worldviews often contribute to periods of increased ideologically motivated violence, including recently during the COVID-19 pandemic and nationwide lawful protests.
- The domestic threat environment is rapidly evolving. Operational reporting shows that DHS law enforcement officers suffered over 300 separate injuries while they were present during months of nightly unrest in Portland, Oregon. This is but one example among many across the country, including in Brooklyn, New York, and Kenosha, Wisconsin, where law enforcement officers have been injured or killed. These increasingly pervasive incidents highlight the threat of anarchist violence that has accelerated in our cities in recent months.

Foreign Terrorist Threats

Foreign terrorist organizations (FTOs), including al-Qa'ida and the Islamic State of Iraq and ash-Sham (ISIS), will maintain interest in attacking the Homeland but we expect the primary threat from these groups to remain overseas in the coming year due to sustained U.S. counterterrorism pressure. Nevertheless, these groups can adapt quickly and resurge, and terrorists overseas will continue to probe for vulnerabilities in U.S. immigration and border security programs. Collectively, vulnerabilities may create an illegal migration environment that FTOs could exploit to facilitate the movement of affiliated persons towards the United States.

- The primary threat to the Homeland from FTOs probably will manifest as "inspired" attacks. FTOs seek to inspire violent extremism in the United States and continue to use social media and other online platforms to call for attacks against the United States. Despite territorial defeats in Iraq and Syria, ISIS continues to draw support from HVEs in the United States and the group's global calls for attacks have intensified since the death last year of senior leader Abu Bakr al-Baghdadi.
- Transportation infrastructure—especially the aviation sector—almost certainly will remain a primary target for terrorists plotting overseas. While terrorists continue to pursue flight school training and the use of insiders, plotting against domestic aviation targets most likely will remain aspirational among FTOs and their supporters over the next year.
- Terrorists and other criminal actors might look to unmanned aircraft systems (UAS) to threaten critical infrastructure. In 2019, there were nearly 4,000 reports of unique incidents of UAS activity near U.S. critical infrastructure or public gatherings. Although we have no indication that any of these events were terrorism-related, it is possible that malicious or criminal actors will turn to UAS tactics.

Iran and Lebanese Hizballah

Iran will continue to develop and maintain terrorist capabilities as an option to deter the United States from taking what Tehran considers regime-threatening actions or to retaliate for such activity, real or perceived. The Government of Iran and its proxy, Lebanese Hizballah (LH), have demonstrated the intent to conduct an array of operations in the Homeland. Iran or LH could advance an attack plot—with little to no warning—in response to heightened tensions. The U.S. Government in recent years has arrested several individuals acting on behalf of the Government of Iran or LH who have conducted surveillance indicative of contingency planning for lethal attacks in the U.S.

Weapons of Mass Destruction and Other Chemical, Biological, Radiological, and Nuclear Threats

The overall global WMD threat will continue

[8] *In this instance, and for the purposes of this report, "violent actors" refers to groups or individuals who facilitate or engage in unlawful acts of violence with the intent to cause serious bodily harm and/or damage to critical infrastructure.*

[9] *Homegrown White Supremist Extremist (WSE): A group or individual who facilitates or engages in acts of unlawful violence directed at the federal government, ethnic minorities, or Jewish persons in support of their belief that Caucasians are intellectually and morally superior to other races and/or their perception that the government is controlled by Jewish persons.*

to rise in 2021. Spurred by continued capability expansion, modernization, low yield weapons development, eroding international norms, information proliferation, emerging drone concerns and increasing actor awareness; the risk of intentional chemical, biological, radiological or nuclear incidents in the homeland and abroad has likely increased.

- Biological threats (deliberate, accidental, and naturally occurring) are more diverse and continue to expand with increased global interconnectivity and rapid advances in biotechnology, genomics, and other legitimate-use capabilities that could introduce risks to global health and food security and the potential for adversaries to develop novel biological warfare agents. Notably, the biological agent attribution shortfalls coupled with the now known devastating impacts may lead to a resurgence of state and non-state biological weapon pursuits.
- Chemical threats are particularly notable as we continue in the most significant and sustained period of chemical weapons use in decades. The publicity of emerging chemical weapons compounds and increases in information availability is evolving the chemical threat landscape. This global trend could manifest as an increased domestic threat.
- Radiological attacks are less likely, guidelines for hazards and safe handling of radiation sources reduce the likelihood of radiological attacks; however, actors driven by extremist ideology could pose a threat if they have knowledge and access of locations to aid radioactive materials acquisition. The major licensed users of radioactive material in the United States are in the energy, healthcare, and construction sectors with larger activity sources protected by physical security measures. The amount of radioactive material in use is not expected to increase in the short term.
- Nuclear threats remain enduring and will remain largely unchanged. The number of nuclear weapons states will probably remain unchanged over the next year. Concerns remain related to lower yield weapons development and regional expansion of nuclear capabilities by several nuclear weapons states and the subsequent increasing risks of weapons loss or nuclear conflict that could have global impacts. Non-state actors continue to face

significant barriers to acquiring special nuclear material for use in an improvised nuclear device, but vulnerabilities remain. Experts do, however, estimate the rate of nuclear security improvement around the globe has decreased since 2018. The COVID-19 pandemic has drawn government resources away from normal functions, similar to resource shifts observed globally in military and other defense sectors; nuclear security may also be vulnerable to resource shifts which could increase risks of theft or sabotage of nuclear facilities. Domestic and foreign-based non-state actors attempting to steal special nuclear material for use in a nuclear weapon will continue to pose a threat to the Homeland.

TCO Threats to U.S. Security

Transnational Criminal Organizations (TCOs)—especially those based in Mexico—will continue to undermine public health and safety in the Homeland and threaten U.S. national security interests. They represent an acute and devastating threat to public health and safety in the Homeland and a significant threat to U.S. national security interests. Beyond their complicity in the 71,000 drug overdose deaths in the U.S. last year, TCOs destabilize partner nations, decrease citizen confidence in good governance, foment corruption, and destroy confidence in the international banking system. Countering these organizations' malign activities will remain an enduring challenge to US safety and security. TCOs will continue to take advantage of illegal migration flows to enter the United States and attempt to exploit legal immigration avenues. Criminal elements attempting to provide a level of legitimacy to their illicit immigration claims by intermingling with migrants travelling to the US Southwest border pose an intrinsic risk to the U.S. lawful immigration system.

Mexico-based Cartels

Among TCOs, Mexico-based cartels pose the greatest threat to the Homeland because of their ability to control territory—including along the U.S. Southwest Border—and co-opt parts of government, particularly at a state and local level. Although COVID-19 has disrupted some cartel operations, their ability to move large quantities of illicit goods into and throughout the Homeland remains largely intact.

- Of the Mexico-based TCOs, the Sinaloa and Jalisco New Generation Cartel (CJNG) networks pose the greatest cross-border drug smuggling threat in the near-term; they dominate the lucrative trafficking of cocaine, heroin, fentanyl, and methamphetamine to the United States.
- Mexican TCO fracturing, disruption of previous drug supply chains, and territorial disputes—especially over important cross-border plazas—almost certainly will lead to increased violence in Mexico, along the U.S. Southwest Border, in the year ahead. Mexican border states experienced nearly 12,000 homicides in 2019, most of which involved TCOs.
- As U.S.-based gangs—some of which provide retail-level drug distribution and sales for Mexican TCOs—vie for access to new users, the United States may face increased criminal violence in some parts of the country. Social distancing lockdown measures, however, probably will moderate any increase in the near term, as opportunistic crimes become less frequent.

Illicit Drugs

The COVID-19 pandemic has slowed the pace of drug trafficking into the United States; however, the threat of illicit drugs—including the rates of overdoses—will persist as traffickers adapt and drug compositions become more potent. TCOs continue to distribute synthetic narcotics such as fentanyl and methamphetamine.

- Potent opioid narcotics like fentanyl and heroin almost certainly will continue to cause alarming levels of overdose in the United States over the next year. The use of stimulant drugs like methamphetamine and cocaine will continue, and distributors will explore new markets in the United States beyond major transportation hubs and regional cities.

- TCOs engaged in the manufacturing of fentanyl and methamphetamine will likely experience mid-term disruption due to COVID-19 response measures that may hinder their receipt of chemicals from international suppliers. Production and transportation of heroin, cocaine, and marijuana also has been affected by travel restrictions and stay-at-home orders within the Western Hemisphere.

Human Smuggling

Mexico-based cartels play an influential role in human smuggling, often facilitating illicit migration over and near the border. Mexico-based drug cartels control large sections of territory just south of the United States southwest land border and have traditionally taxed human smugglers and traffickers to move migrants through their areas of operation. Since the COVID-19 pandemic began, these criminal groups have continued efforts to facilitate the movement of migrants throughout most of their routes.

Exploitation of Others for Profit

Criminal elements will continue to exploit others to facilitate their pursuit of illicit profits.

- Human trafficking—both sex trafficking and forced labor—remains a significant issue. Top threats include sex trafficking and juvenile sex trafficking, domestic labor trafficking and indentured servitude, and goods imported into the United States that were produced by forced labor. These illicit activities often have a nexus to criminal organizations, such as those operating illicit massage businesses or engaged in exploitation of migrant and undocumented populations.
- Child exploitation is also a significant issue. Top threats in this area include the proliferation of online Child Sexual Abuse Material, live streaming of child sexual exploitation, online enticement and extortion, and child sex trafficking.
- Criminal networks engage in multiple types of illicit financial activities to maintain affirmative control of their proceeds, including bulk cash smuggling, trade-based money laundering (TBML), third party money laundering (3PML), virtual currency-based money laundering and fraud, and transnational financial fraud schemes. The top threats in the illicit finance area are Chinese TCOs, money laundering organizations specializing in supporting drug trafficking organizations, Colombian money brokers, West African TCOs, and cyber hacking groups.

Illegal Immigration to the United States

The duration and severity of the COVID-19 pandemic will shape migration to the U.S. Southwest Border into 2021, along with traditional push and pull factors stemming from weak economic and political conditions in the region. COVID-19's impact on Caribbean nations increases the chance of a mass migration event from Cuba or Haiti. Although the majority of migrants do not pose a national security or public safety threat, pathways used by migrants to travel to the United States have been exploited by threat actors. As a result, surges of migrants could undermine our ability to effectively secure the border without adversely impacting other parts of the immigration system.

Illegal Immigration via Land

The duration and severity of the COVID-19 pandemic in the United States and within Central and South America and the Caribbean will shape illegal immigration to the U.S. Southwest Border, exacerbating the underlying economic and political conditions in the region. As COVID-19-related restrictions on mobility ease, we are seeing an increase in illegal immigration flows to pre-pandemic levels.

- Illegal immigration flows within the Western Hemisphere have begun to increase after a short-term decline in response to the world-wide COVID-19 pandemic and countries instituting border transit restrictions. Over the medium term, mass migration might occur if the economies of the Caribbean, Central and South American countries continue to decline and if the health and humanitarian response capabilities continue to deteriorate due to COVID-19. Mass migration especially might occur if these negative conditions are coupled with an economic resurgence in the United States.
- COVID-19-related international travel restrictions that many countries have instituted have curtailed some illegal immigration from outside the Western Hemisphere. When these measures are lifted, there will be sporadic illegal immigration into and through the region.
- Weak job markets, high crime rates, and governmental or non-state repression will remain key drivers of U.S.-bound migration from the Caribbean and Central and South America, especially as COVID-19-related citizen mobility restrictions ease in the region. Seasonal weather changes and perceptions of U.S. and Mexican immigration and enforcement policies and measures also will shape migration patterns as inter-governmental division and inconsistent messaging continue to impede Congressionally mandated immigration enforcement policies.

Human Trafficking

Human traffickers continue to use force, fraud, and coercion against millions of victims worldwide, as many of them attempt to gain entry to the United States via the southwest land border. Many victims never seek assistance from law enforcement because of language barriers, fear of retaliation from their traffickers and/or fear of law enforcement. This allows traffickers to force victims into labor or commercial sexual exploitation. Traffickers continue to target people they believe to be susceptible for a wide variety of reasons including but not limited to psychological or emotional vulnerability, economic hardship, natural disasters, political instability or a lack of a social safety net.

- Increased illegal immigration to the U.S. Southwest Border will require United States Citizenship and Immigration Services (USCIS) to re-examine how resources are properly aligned at the Southwest Border, likely impacting the larger asylum system. Increasing numbers of

apprehensions will lead to an increased number of fear claims, requiring USCIS to dedicate additional resources to protection screenings and away from addressing case backlogs such as the asylum case backlog.

- Social distancing requirements could continue to affect work taking place in detention facilities along the Southwest border. Budgetary impediments towards immigration enforcement and lack of bipartisan support of detention measures continue to undermine U.S. immigration enforcement policies. Such inconsistent practices continue to lead to the release of dangerous criminal aliens and absconders who may then commit additional crimes when they might otherwise have been expeditiously detained and removed from the United States.
- Since 2014, DHS has experienced repeated illegal immigration surges at the Southwest Border. DHS anticipates that the number of apprehensions at the border will significantly climb post-pandemic, with the potential for another surge as those who were previously prevented from seeking entry into the United States arrive at the border and as poor economic conditions around the world fuel migration. This high volume of illegal immigration, including unprecedented numbers of family units and unaccompanied alien children arrivals, stretch government resources, and create a humanitarian and border security crisis that cripples the immigration system.
- Record migration at the Southwest Border took up limited U.S. Immigration and Customs Enforcement (ICE) detention resources, drove increases in the agency's average daily population (ADP), resulted in decreased interior arrests (including arrests of criminals), and forced ICE to balance its critical public safety mission in the interior with its support for DHS efforts to secure the border. As the pandemic subsides, ICE will conduct additional enforcement operations to uphold its public safety mission and address the growing fugitive backlog.
- DHS projects that until fundamental changes are made to the immigration enforcement process, including legislation that addresses current legal loopholes that incentivize high levels of illegal immigration, the United States will periodically experience additional humanitarian and border security crises.

Illegal Immigration at Sea

The impact of COVID-19 very likely will affect maritime migration from both migrant origin and transit countries in the Caribbean through 2021. Weak socio-economic conditions in Cuba, political instability and food insecurity in Haiti, and the uncertainty of COVID-19 impacts in the region will increase the chances of a maritime mass migration event, although the overall risk remains low.

- Interviews of interdicted migrants reveal that some still desire to come to the United States, regardless of the risk posed by COVID-19, rather than face the deteriorating economic conditions in their home countries.
- Measures such as border closures, quarantines, and a reduction in legitimate vessel traffic can disrupt migrant flows; however, increased food insecurity and unemployment, reduced economic opportunities, a lack of medical infrastructure, and other second- and third-order effects in migrants' home countries serve as likely push factors resulting in increased maritime migration to the United States.
- In the event of increased maritime migration, the U.S. Coast Guard and USCIS will need to increase interdiction and screening resources in the region. This could result in the reallocation of limited resources, impacting the ability to conduct other operations.

Natural Disasters

Natural disasters—which refer to all types of severe weather, including floods, earthquakes, hurricanes, wildfires, and winter storms—remain an ongoing threat to the nation. These disasters pose a significant threat to human health and safety, property, critical infrastructure, and homeland security while subjecting the nation to frequent periods of insecurity, disruption, and economic loss. Over the last year, the United States has faced the COVID-19 crisis while simultaneously dealing with numerous natural disasters. These natural disasters require the Department to readjust its priority focus, as resources continue to be reallocated to focus on responding to multiple natural disasters, while continuing to handle its traditional roles and responsibilities.

Hurricanes

Hurricanes pose a persistent hazard to life and property. DHS assesses that hurricanes will continue to pose a hazard for the United States and its territories in the coming months. While their individual impact varies based on the intensity and duration of the storms, hurricanes are one of nature's most destructive forces, which can cause enormous damage and may precipitate mudslides, flash floods, storm surges, and wind and fire damage. Severe weather events associated with hurricanes can have widespread impacts across multiple states, take lives, damage or destroy property, and impact the nation's economic capability. They have the potential to overwhelm the emergency response and recovery capabilities of the affected state(s) and may require the sustained deployment of Federal assets.

- The 2020 season has been the second most active Atlantic hurricane season on record, behind only the 2005 season. This season was the first to see seven named tropical cyclones make landfall in the continental United States before September, which became the most active September on record with 10 tropical or subtropical storms.
- As a result of the COVID-19 pandemic, the Nation continues to face unprecedented challenges as we respond to the compounding issues surrounding the 2020 hurricane season. Although the operating environment has changed the mission of helping people before, during, and after disasters remains the same. Federal, state, local, tribal, and territorial officials, along with the private sector and non-governmental organizations, must continue to partner together to fulfill their respective missions and help disaster survivors.

Wildfires

Wildland fires pose a major threat to lives, property, and ecosystem integrity. Wildfires increase the likelihood of adverse impacts, including flooding, erosion, reduced water quality, loss of key wildlife habitat, and other ecological and economic impacts.

- Thus far in 2020, there have been 94 large fires, which have burned approximately 5.37 million acres throughout the West. September alone saw 87 large fires burning simultaneously uncontained from the West Coast to the Rocky Mountains, with over 25 Fire Management Assistance Grants approved. Wildfires not only pose a threat to key infrastructure, housing, and public safety but also contribute to poor air quality.
- Efforts to undertake better and more active land management will be needed at every level of government in order to reduce the annual threat of wildfires. Such challenges cannot be addressed simply within the federal government, but must also involve state and private actors to better prepare to minimize the impacts of wildfires.

Homeland Security

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

www.dhs.gov