# Department of Justice

**STATEMENT OF**

**CHRISTOPHER A. WRAY**
**DIRECTOR**
**FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE**

**COMMITTEE ON**
**HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**
**UNITED STATES SENATE**

**AT A HEARING ENTITLED**

**"WORLDWIDE THREATS"**

**PRESENTED**

**SEPTEMBER 24, 2020**

**STATEMENT OF**
**CHRISTOPHER A. WRAY**
**DIRECTOR**
**FEDERAL BUREAU OF INVESTIGATION**

**BEFORE THE**

**COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**
**UNITED STATES SENATE**

**AT A HEARING ENTITLED**
**"WORLDWIDE THREATS"**

**PRESENTED**
**SEPTEMBER 24, 2020**

Good afternoon, Chairman Johnson, Ranking Member Peters, and Members of the Committee. Thank you for the opportunity to appear before you today to discuss the current threats to the United States Homeland. I am pleased to be here representing the nearly 37,000 dedicated men and women of the FBI.

While the COVID-19 pandemic has presented unique and unprecedented challenges to the FBI workforce, I am proud of their dedication to our mission of protecting the American people and upholding the Constitution. Hostile foreign actors, violent extremists, and opportunistic criminal elements have seized upon this environment. As a result, we are facing aggressive and sophisticated threats on many fronts. Whether it is terrorism now moving at the speed of social media, or the increasingly blended threat of cyber intrusions and state-sponsored economic espionage, or malign foreign influence and interference or active shooters and other violent criminals threatening our communities, or the scourge of opioid trafficking and abuse, or hate crimes, human trafficking, crimes against children — the list of threats we are worried about is not getting any shorter, and none of the threats on that list are getting any easier.

***Counterterrorism***

Preventing terrorist attacks remains the FBI's top priority. However, the threat posed by terrorism — both international terrorism ("IT") and domestic violent extremism — has evolved significantly since 9/11.

The greatest threat we face in the Homeland is that posed by lone actors radicalized online who look to attack soft targets with easily accessible weapons. We see this lone actor threat manifested both within Domestic Violent Extremists ("DVEs") and Homegrown Violent Extremists ("HVEs"), two distinct sets of individuals that generally self-radicalize and mobilize to violence on their own. DVEs are individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences, such as racial bias and anti-government

sentiment. HVEs are individuals who have been radicalized primarily in the United States, and who are inspired by, but not receiving individualized direction from, Foreign Terrorist Organizations ("FTOs").

Many of these violent extremists, both domestic and international, are motivated and inspired by a mix of ideological, socio-political, and personal grievances against their targets, which recently have more and more included large public gatherings, houses of worship, and retail locations. Lone actors, who by definition are not likely to conspire with others regarding their plans, are increasingly choosing these soft, familiar targets for their attacks, limiting law enforcement opportunities for detection and disruption ahead of their action.

DVEs pose a steady and evolving threat of violence and economic harm to the United States. Trends may shift, but the underlying drivers for domestic violent extremism — such as perceptions of government or law enforcement overreach, socio-political conditions, racism, anti-Semitism, Islamophobia, misogyny, and reactions to legislative actions — remain constant. As stated above, the FBI is most concerned about lone offender attacks, primarily shootings, as they have served as the dominant lethal mode for domestic violent extremist attacks. More deaths were caused by DVEs than international terrorists in recent years. In fact, 2019 was the deadliest year for domestic extremist violence since the Oklahoma City Bombing in 1995.

The top threat we face from domestic violent extremists stems from those we identify as Racially/Ethnically Motivated Violent Extremists ("RMVE"). RMVEs were the primary source of ideologically-motivated lethal incidents and violence in 2018 and 2019 and have been considered the most lethal of all domestic extremists since 2001. Of note, the last three DVE attacks, however, were perpetrated by Anti-Government Violent Extremists.

The spate of attacks we saw in 2019 underscore the continued threat posed by DVEs and perpetrators of hate crimes. The FBI works proactively to prevent acts of domestic terrorism and hate crimes. For example, in November 2019, the Denver Joint Terrorism Task Force arrested Richard Holzer on federal charges of attempting to obstruct religious exercise by force using explosives. This disruption is just one example of the strength of our Domestic Terrorism-Hate Crimes ("DT-HC") Fusion Cell. Our Counterterrorism ("CTD") and Criminal Divisions ("CID") working together were able to prevent a potential terrorist attack before it occurred and, for the first time in recent history, make a proactive arrest on a Hate Crimes charge. Through the DT-HC Fusion Cell, subject-matter experts from both CTD and CID work in tandem to innovatively use investigative tools and bring multiple perspectives to bear in combatting the intersecting threats of domestic terrorism and hate crimes, preventing attacks and providing justice to victims.

We recognize that the FBI must be aware not just of the domestic violent extremism threat, but also of threats emanating from those responding violently to First Amendment-protected activities. In the past, we have seen some violent extremists respond to peaceful movements through violence rather than non-violent actions and ideas. The FBI is involved only when responses cross from ideas and Constitutionally-protected protests to violence. Regardless of the specific ideology involved, the FBI requires that all domestic terrorism

Investigations be predicated based on activity intended to further a political or social goal, wholly or in part involving force, coercion, or violence, in violation of federal law.

HVEs and FTOs have posed a persistent threat to the Nation and to U.S. interests abroad, while their tradecraft, tactics, and target sets have evolved. The international terrorism threat to the U.S. has expanded from sophisticated, externally-directed FTO plots to include individual attacks carried out by HVEs who are inspired by designated terrorist organizations. As stated above, the FBI assesses HVEs are the greatest, most immediate international terrorism threat to the Homeland. These individuals are FTO-inspired individuals who are in the U.S., have been radicalized primarily in the U.S., and are not receiving individualized direction from FTOs. We, along with our law enforcement partners, face significant challenges in identifying and disrupting HVEs. This is due, in part, to their lack of a direct connection with an FTO, an ability to rapidly mobilize without law enforcement detection, and their frequent use of encrypted communications.

Many FTOs use various digital communication platforms to reach individuals they believe may be susceptible and sympathetic to violent terrorist messages. However, no group has been as successful at drawing people into its perverse ideology as ISIS, which has proven dangerously competent at employing such tools. ISIS uses traditional media platforms as well as widespread social media campaigns to propagate its ideology. Terrorists in ungoverned spaces — both physical and virtual — readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages in the U.S. either to travel to foreign lands or to conduct an attack on the Homeland. Through the Internet, terrorists anywhere overseas now have direct access to our local communities to target and recruit our citizens and spread their message faster than was imagined just a few years ago.

We remain concerned that groups such as the Islamic State of Iraq and ash-Sham ("ISIS") and al-Qaeda intend to carry out large-scale attacks in the U.S. Despite their territorial defeat in Iraq and Syria, ISIS remains relentless and ruthless in its campaign of violence against the West and has aggressively promoted its hateful message, attracting like- minded violent extremists. The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who use messaging apps and participate in social networks. Ultimately, many of the individuals drawn to ISIS seek a sense of belonging. Echoing other terrorist groups, ISIS has advocated lone offender attacks in Western countries. Recent ISIS videos and propaganda have specifically advocated attacks against soldiers, law enforcement, and intelligence community personnel.

As noted above, ISIS is not the only terrorist group of concern. Al-Qaeda maintains its desire for large-scale, spectacular attacks. While continued counterterrorism pressure has degraded the group's Afghanistan-Pakistan senior leadership, in the near term, al-Qaeda is more likely to focus on building its international affiliates and supporting small-scale, readily achievable attacks in key regions such as East and West Africa. Simultaneously, over the last

year, propaganda from al-Qaeda leaders seeks to inspire individuals to conduct their own attacks in the U.S. and the West. For example, the December 2019 attack at Naval Air Station Pensacola demonstrates that groups such as al-Qaeda continue to be interested in encouraging attacks on U.S. soil.

The FBI regularly reviews intelligence to ensure that we are appropriately mitigating threats from any place by any actor, and the possible violent responses and actions. We are sensitive to First Amendment-protected activities during investigative and intelligence efforts so as to ensure that our investigative actions remain aligned with our authorities and are conducted with the appropriate protections in place for privacy and civil liberties.

As the threat to the United States and U.S. interests evolves, we must adapt and confront these challenges, relying heavily on the strength of our federal, State, local, Tribal, and international partnerships. The FBI uses all lawful investigative techniques and methods to combat these terrorist threats to the United States. Along with our domestic and foreign partners, we are collecting and analyzing intelligence concerning the ongoing threat posed by violent extremists motivated by any ideology and desire to harm Americans and U.S. interests. We continue to encourage information sharing, which is evidenced through our partnerships with many federal, State, local, and Tribal agencies assigned to Joint Terrorism Task Forces around the country. Be assured, the FBI continues to strive to work and share information more efficiently, and to pursue a variety of lawful methods to help stay ahead of these threats.

***Election Security***

In less than two months, Americans will exercise one of their most important and cherished freedoms; the right to vote in a democratic election. Our nation is confronting multi-faceted foreign threats seeking to both influence our national policies and public opinion, and cause harm to our national dialogue. The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

Foreign influence operations — which include covert, coercive, or corrupt actions by foreign governments to influence U.S. political sentiment or public discourse or interfere in our processes themselves — are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. This year's election cycle, amid the COVID-19 pandemic, provides ample opportunity for hostile foreign actors to conduct disinformation campaigns and foreign influence operations in an effort to mislead, sow discord, and, ultimately, undermine confidence in our democratic institutions and values and in our government's response to our current health crisis.

Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries — hoping to reach a wide swath of Americans covertly from outside the United States — to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, the Foreign Influence Task Force ("FITF") was established to identify and counteract malign foreign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and is composed of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions and public confidence; develop a common operating picture; raise adversaries' costs; and, reduce their overall asymmetric advantage.

The task force brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and — importantly — to be more agile. Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had a number of instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia. Utilizing lessons learned over the last year and half, the FITF is widening its aperture to confront malign foreign operations of China, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent "surge" capability on election and foreign influence threats.

We have also further refined our approach. All efforts are based on a three-pronged approach, which includes investigations and operations; information and intelligence sharing; and a strong partnership with the private sector. Through the efforts of the FITF, and lessons learned from both the 2016 and 2018 elections, the FBI is actively engaged in identifying, detecting, and disrupting threats to our elections and ensuring both the integrity of our democracy is preserved and the will of the American people is fulfilled.

Protecting policymakers is an important part of our efforts to combat malign foreign influence and protect our elections. As you are aware, the FBI and our interagency partners have been providing ongoing election security threat briefings to Congress. We will continue to do so throughout the fall and into the future, where there is actionable intelligence.

***Lawful Access***

I want to turn now to an issue continuing to limit law enforcement's ability to disrupt these increasingly insular actors. We are all familiar with the inability of law enforcement agencies to access data, even with a lawful warrant or court order, due to "end-to-end" encryption. Increasingly, device manufacturers and communications service providers have employed encryption in such a manner that only the users or parties to the communications can access the content of the communications or devices. This is known as "end-to-end" encryption.

This development has meant that, in recent years, the FBI has observed a decline in its ability to gain access to the content of both domestic and international terrorist communications, due to the widespread adoption of encryption for Internet traffic and the prevalence of mobile messaging apps using end-to-end encryption as default.

The FBI certainly recognizes how encryption increases the overall safety and security of the Internet for users. But, in fulfilling the FBI's duty to the American people to prevent acts of terrorism, this kind of end-to-end encryption creates serious challenges. Accessing content of communications by, or data held by, known or suspected terrorists pursuant to judicially authorized, warranted legal process is getting more and more difficult.

The online, encrypted nature of radicalization, along with the insular nature of most of today's attack plotters, leaves investigators with fewer dots to connect. As was evident in the December 9, 2019, shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Alshamrani was able to communicate using warrant-proof, end-to-end encrypted apps deliberately to evade detection by law enforcement. It took the FBI several months to access information in his phones, during which time we did not know whether he was a lone wolf actor, or whether his associates may have been plotting additional terrorist attacks.

If law enforcement loses the ability to detect criminal activity because communication between subjects — data in motion — or data held by subjects — data at rest — is encrypted in such a way making content inaccessible, even with a lawful order, our ability to protect the American people will be degraded. Providers and law enforcement must continue to collaborate to explore possible technical solutions that would provide security and privacy to those using the Internet while also contributing to the FBI's ability to complete its mission.

Despite the successes that result from the hard work of the men and women of the FBI, our Joint Terrorism Task Forces, and our partners across the government, terrorism continues to pose a persistent threat to the Homeland and our interests overseas.

***China Threat***

The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It is a threat to our economic security and by extension, to our national security.

As you have seen from the recent closure of the Chinese Consulate in Houston, this issue is not just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves. Our adversaries' targets are our nation's core economic assets — our information and ideas, our innovation, our research and development, our technology. No country poses a broader, more severe threat to those assets than China. It is the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history. If you are an American adult, it is more likely than not that China has stolen your personal data.

In 2017, the Chinese military conspired to hack Equifax and made off with the sensitive personal information of 150 million Americans — we are talking nearly half of the American population and most American adults. Our data is not the only thing at stake here — so is our health, livelihood, and security.

The FBI is opening a new China-related counterintelligence case approximately every ten hours. Of the nearly 5,000 active FBI counterintelligence cases currently underway across the country, almost half are related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research. They are going after cost and pricing information, internal strategy documents, personally identifiable information — anything that can give them a competitive advantage.

It is important to be clear: this is not about the Chinese people as a whole, and certainly not about Chinese-Americans as a group, but it is about the Chinese government and the Chinese Communist Party. Every year, the United States welcomes more than 100,000 Chinese students and researchers into this country. For generations, people have journeyed from China to the United States to secure the blessings of liberty for themselves and their families — and our society is better for their contributions. So, when the FBI's refers to the threat from China, we mean the Government of China and the Chinese Communist Party.

Confronting this threat effectively does not mean that we should not do business with the Chinese. It does not mean that we should not host Chinese visitors. It does not mean that we should not welcome Chinese students or coexist with China on the world stage. But it does mean that when China violates our criminal laws and international norms, we are not going to tolerate it, much less enable it. The FBI and our partners throughout the U.S. government will hold China accountable and protect our nation's innovation, ideas, and way of life — with the help and vigilance of the American people.

***Cyber***

With the advent of the COVID-19 pandemic, the nature of the cyber threat has become increasingly concerning. As more individuals telework and increasingly use the cloud, we encounter less secure networks. As a result, the scope of our cyber threats has changed, the impact has deepened, and many of the players have become more dangerous as we have become increasingly vulnerable. We are still seeing hack after hack and breach after breach. We hear about it daily in the news. The more we shift to the Internet as the conduit and the repository for everything we use and share and manage, the more danger we are in.

Today we are worried about a wider-than-ever range of threat actors, from multi-national cyber syndicates to nation-state adversaries. And we are concerned about a wider-than-ever gamut of methods continually employed in new ways, like the targeting of managed service providers —MSPs — as a way to access scores of victims by hacking just one provider.

China's Ministry of State Security ("MSS") pioneered that technique and, as you saw in July, we indicted two Chinese hackers who worked with the Guangdong State Security Department of the MSS. These individuals conducted a hacking campaign lasting more than ten years, targeting countries with high technology industries, to include the United States. The industries targeted included, among others, solar energy; pharmaceuticals; and defense. Cybercrimes like these, directed by the Chinese government's intelligence services, threaten not only the United States but also every other country that supports fair play, international norms, and the rule of law, and they also seriously undermine China's desire to become a respected leader in world affairs.

Theft of intellectual property is not the only cyber threat presented by the People's Republic of China ("PRC") government. They are also working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. All of them, and others, are working to simultaneously strengthen themselves, and weaken the United States. And we are taking all these nation-state threats very seriously.

But as dangerous as nation-states are, we do not have the luxury of focusing on them alone. We also are battling the increasing sophistication of criminal groups that place many hackers on a level we used to see only among hackers working for governments. The proliferation of malware as a service, where darkweb vendors sell sophistication in exchange for cryptocurrency, increases the difficulty of stopping what would once have been less-dangerous offenders. It can give a ring of unsophisticated criminals the tools to paralyze entire hospitals, police departments, and businesses with ransomware. Often the hackers themselves have not become much more sophisticated — but they are renting sophisticated capabilities, requiring us to up our game as we work to defeat them, too.

Hackers have not relented under the COVID-19 pandemic. On the contrary, they have attempted to compromise the computer systems of hospitals and medical centers to obtain patient

financial data, medical records, and other information. In addition, such attacks on medical centers may lead to the interruption of computer networks and systems putting patients' lives at an increased risk when America faces its most dire health crisis in generations.

***Conclusion***

Chairman Johnson, Ranking Member Peters and Members of the Committee, thank you for the opportunity to testify today. I am now happy to answer any questions you might have.