

**Washington Institute for Near East Policy
19 November 2019
DAD Alcock**

**Statement for the Record:
The Evolving and Persistent Terrorism Threat to the Homeland**

First and foremost, I would like to thank you for the invitation to be part of the Washington Institute's Counterterrorism Lecture Series. It is an honor to represent the FBI and to speak to you at this esteemed event. Today, I will discuss the ever-evolving terrorism landscape, with an eye to the Homeland. My intent is to provide an overview of the threat as we see it at the FBI today, including the investigative challenges and opportunities presented by this shifting paradigm.

To level set before we begin, I'd like to explain how the FBI works counterterrorism. The FBI categorizes terrorism investigations into two programs: international terrorism and domestic terrorism. International terrorism includes investigations into members of designated foreign terrorist organizations, state sponsors of terrorism, and Homegrown Violent Extremists. The latter are individuals inside the United States, who have been radicalized primarily in the United States, and who are inspired by, but not receiving individual direction from, foreign terrorist organizations.

Domestic terrorists are individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic issues. A majority of our domestic terrorism cases fall into one of four categories: racially motivated violent extremism, anti-government/anti-authority extremism, animal rights/environmental extremism, and abortion extremism.

Because of the interests of the audience here today, my comments will focus largely on the international terrorism threat to the US. But to be clear, preventing acts of terrorism, regardless of ideology, is the FBI's number one priority.

I'd like to set the stage by discussing the FBI's evolution in the 18 years since 9/11, and why we are stronger, more agile, and better able to confront the threat of terrorism – both international and domestic. After the 9/11 attacks, we asked ourselves, "What

could we have done better?” And every day since, we have asked ourselves, “What do we need to do to keep the American People safe from terrorism today, tomorrow, and the day after that?”

We’ve torn down walls separating agencies and preventing collaboration. We’ve significantly improved the way we share information, not just among law enforcement, and the Intelligence Community, but also with the private sector and foreign partners. Sharing is now the rule, rather than the exception.

Because of this increased collaboration, we’ve developed a whole-of-government approach to combatting terrorism over the past 18 years. During the course of our investigations, we bring the full force of the US intelligence, law enforcement, and judicial system to bear against these actors.

Underpinning all of our successes is our commitment to partnerships. In fact, one of the most critical elements of the FBI’s counterterrorism strategy is the Joint Terrorism Task Force, a partnership between law enforcement at the federal, state, and local levels committed to preventing acts of terrorism.

The FBI has JTTFs in all 56 of our field offices around the country, with over 4,000 investigators, bringing a holistic capability to the fight. It’s an integrated investigative approach to terrorist detection and prevention.

What hasn’t changed is the FBI’s commitment to preventing all acts of terrorism in the United States and against US interests overseas. The whole-of-government approach we now bring to the counterterrorism mission positions us to best address the dynamic threat that we face today.

Eighteen years after 9/11, what does this terrorism threat look like? I’ll begin with what we might consider “longstanding” terrorism threats emanating from overseas groups.

We are certainly still laser-focused on foreign terrorist organizations like al-Qa’ida and ISIS. As you know, these organizations wish to cause us harm, and pose the biggest Sunni terrorist threat to US interests overseas. Simply put, the lethal threat from these groups persists despite significant setbacks and defeats.

Al-Qa'ida in particular has proven resilient, despite the death of Usama bin Laden in 2011. AQ's desire to carry out large-scale, spectacular attacks in the United States is clear. And we're also paying attention to al-Qa'ida's affiliates, like al-Qa'ida in the Arabian Peninsula and al-Qa'ida in Syria.

As we continue to monitor the situation in Syria, we know the threat from ISIS remains, despite its loss of territory, resources, and its leader Abu Bakr al-Baghdadi. Even after suffering significant defeats, ISIS can now rely on global support from its branches.

Of particular concern within our own borders, ISIS's model of online recruitment and propaganda encourages supporters to take action against soft targets from wherever they are located.

We've seen this call to action through online channels play out across America. In March, a man arrested not too far from here in Maryland admitted to planning a vehicle ramming attack in the name of ISIS. And in August, authorities disrupted a plot to conduct a stabbing in Queens on behalf of the terrorist organization. Neither of these individuals received specific direction from ISIS in their attack plan but sought out and found propaganda online, which inspired them to plot an attack.

In addition to countering the threat from Sunni terrorist groups, we also have worked to mitigate the threat from Iranian supported groups who are plotting and conducting attacks. We know the Government of Iran aims to preserve the regime and export its Islamic revolution worldwide, through the use of its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), its strategic partner Hizballah, and its proxy groups positioned to harm US interests in the Middle East.

The threat has also reached our shores. Recently, two men pleaded guilty to conducting surveillance against Jewish and Israeli facilities, and against Iranian dissidents in the US at the direction of the Government of Iran.

Although these foreign terrorist groups and state actors have suffered significant defeats through military and intelligence efforts by the US and others, we can't take our eye off the ball. Their violent determination persists.

I'll end here with discussing these organizations and nation states, because I'd like to also discuss how the threat has evolved within our borders. A decade ago, these organizations posed the largest terrorist threat to the US. Today, as evidenced by recent attacks, the greatest threat we face in the Homeland emanates from self-radicalized lone actors, of any ideology, who look to attack soft targets with easily accessible weapons.

These lone actors span our international and domestic terrorism cases, and include Homegrown Violent Extremists, inspired by foreign terrorist organizations, and Domestic Violent Extremists, inspired to commit violence in furtherance of domestic ideologies.

Homeland plotting shifted from in-person networks motivated by local radicalizers to self-starting violent extremists inspired by online ideologues and propaganda. We are seeing the internet and social media enable individuals to engage and encourage other like-minded individuals without face-to-face meetings. As FBI Director Christopher Wray often says, "Terrorism moves at the speed of social media." We find that to be true every day in our investigations.

An individual sitting in front of a computer in one country can communicate with, encourage, and inspire multiple extremist actors thousands of miles away. Social media provides an avenue for the rapid movement of information in a realm where radicalization is often a personal and anonymous process.

As you can imagine, law enforcement, the Intelligence Community, and academics aim to better understand this threat and determine commonalities, or a profile, of lone offenders. Several academic and government studies have supported the FBI's longstanding assessment that there is no useful demographic profile of lone offender terrorists. While attackers are mostly male and born in the US, the similarities largely stop there. We've seen attackers span all ends of the economic and political spectrums, with varying occupations, levels of education, marital statuses, and religions.

One interesting demographic trend we can point to over the past two years is a decrease in the average age of attackers. In 2018, juveniles comprised nearly one-third

of all identified Homeland attackers and plotters inspired by foreign terrorist organizations like ISIS and al-Qa'ida. This underscores the susceptibility of some adolescents to ideologies that appeal to a desire for a sense of belonging or identity.

Studies have also revealed that most successful attackers typically mobilize to violence in less than six months. This commonality emphasizes the unpredictability of our subjects and demonstrates the “flash to bang” mobilization lifespan, or case velocity as we call it. We may not have long to act to prevent an attack.

Additionally, while government and law enforcement facilities still represent attractive targets for violent extremists, recent attackers favored easy-to-acquire weapons—often firearms—against soft or civilian targets, hampering detection efforts. These targets, favored by attackers since 2016, have included: a high school cafeteria, a bus terminal, NYC pedestrians, a festival, and a retail center.

Selecting familiar targets reduces the need for pre-attack reconnaissance, again limiting opportunities for detection by law enforcement or bystanders.

In recent years, we have also seen individuals, particularly juveniles, mix multiple extremist ideologies to develop unique personalized justifications for violence. Often elements of these ideologies are opposed to each other. In short, ideologically fluid extremists may be drawn more to violence than to the ideology itself.

I want to turn now to an issue continuing to limit law enforcement's ability to disrupt these increasingly insular actors. We're all familiar with the inability of law enforcement agencies to access data, even with a lawful warrant or court order, due to encryption.

In recent years, the FBI observed a decline in its ability to 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. In many places, we have effectively “Gone Dark.”

As a private citizen, I certainly appreciate encryption's increase in 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, 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.

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. I believe there are solutions providers could deploy which would provide safety and security to those using the internet while also contributing to the FBI’s ability to prevent and investigate terrorism and other criminal acts like child exploitation and cybercrimes.

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. With this insular threat, we increasingly rely on the bystanders in these actors’ networks— family members, peers, community leaders, and strangers—to notice changes in behavior, and report concerns, before violence occurs.

One of the Intelligence Community’s flagship initiatives for increasing bystander reporting is the Homegrown Violent Extremist Mobilization Indicators booklet. This unclassified booklet, produced jointly by FBI, NCTC, and DHS, describes observable indicators that someone may be preparing to engage in violent extremist activity. The indicators cover activities observable online, by family or friends, religious leaders, and private sector companies such as those in the financial or shipping industry. You may think of this as the “See Something, Say Something” campaign for the modern threat.

This summer, a man living in Pittsburgh was arrested by an FBI Joint Terrorism Task Force on charges related to his alleged plot to bomb a church in the name of ISIS. The subject allegedly distributed propaganda materials and recorded a video of himself pledging allegiance to ISIS—observable mobilization indicators of imminent or near-term concern, according to the indicators booklet.

While family members and close friends likely are best positioned to observe concerning behaviors, previous research has determined family members and peers often are resistant to sharing their concerns with authorities, which further complicates detection efforts. Our JTTFs are hard at work, engaging with the public, and our private sector

partners to equip them with resources for reporting concerning behavior to law enforcement. With this shift in the terrorism threat, we recognize that tips from the public will be one of the most powerful tools we have in detecting and preventing attacks.

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.

As we saw just recently, with the arrest of a man in Pueblo, Colorado, who allegedly planned to bomb a synagogue in furtherance of his ideology, lone actors pose a lethal terrorism threat to the American people. But this case also highlights the power of the Joint Terrorism Task Force - whose reach extends from coast to coast and around the globe, and is a force multiplier in the fight against terrorism. Together, with our partners, we stand shoulder to shoulder and remain vigilant against these threats.

It's been said, "It takes a network to defeat a network." While the whole-of-government approach has been successful in mitigating many of the threats posed by overseas terrorism networks, a whole-of-society approach will be required to mitigate the evolving lone offender terrorism threat within our borders.

The FBI and our partners will continue to confront the threat posed by terrorists with determination and dedication to our mission to protect the American People and uphold the Constitution of the United States.

Thank you again for the opportunity to be here today. I look forward to answering any questions you might have.