Department of Justice

STATEMENT OF
JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

AT A HEARING ENTITLED
"THREATS TO THE HOMELAND"

PRESENTED
OCTOBER 8, 2015

Statement of
James B. Comey
Director
Federal Bureau of Investigation

Before the
Committee on Homeland Security and Governmental Affairs
United States Senate

At a Hearing Entitled
"Threats to the Homeland"

October 8, 2015

Good afternoon Chairman Johnson, Ranking Member Carper, and members of the committee. Thank you for the opportunity to appear before you today to discuss the current threats to the Homeland and our efforts to address new challenges including terrorists' use of technology to communicate — both to inspire and recruit. The widespread use of technology propagates the persistent terrorist message to attack U.S. interests whether in the homeland or abroad. As the threat to harm Western interests evolves, we must adapt and confront the challenges, relying heavily on the strength of our Federal, State, local, and international partnerships. Our successes depend on interagency cooperation. We work closely with our partners within the Department of Homeland Security and the National Counterterrorism Center to address current and emerging threats.

Counterterrorism

Counterterrorism remains the FBI's top priority, however, the threat has changed in two significant ways. First, the core al Qaeda tumor has been reduced, but the cancer has metastasized. The progeny of al Qaeda – including AQAP, al Qaeda in the Islamic Maghreb, and the Islamic State of Iraq and the Levant (ISIL) have become our focus.

Secondly, we are confronting the explosion of terrorist propaganda and training on the Internet. It is no longer necessary to get a terrorist operative into the United States to recruit. Terrorists, in ungoverned spaces, disseminate poisonous propaganda and training materials to attract troubled souls around the world to their cause. They encourage these individuals to travel, but if they can't travel, they motivate them to act at home. This is a significant change from a decade ago.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the FBI and the Intelligence Community as a whole.

Conflicts in Syria and Iraq continue to serve as the most attractive overseas theaters for Western-based extremists who want to engage in violence. We estimate approximately 250 Americans have traveled or attempted to travel to Syria to participate in the conflict. While this number is lower in comparison to many of our international partners, we closely analyze and assess the influence groups like ISIL have on individuals located in the United States who are inspired to commit acts of violence. Whether or not the individuals are affiliated with a foreign terrorist organization and are willing to travel abroad to fight or are inspired by the call to arms to act in their communities, they potentially pose a significant threat to the safety of the United States and U.S. persons.

ISIL has proven relentless in its violent campaign to rule and has aggressively promoted its hateful message, attracting like-minded extremists to include Westerners. To an even greater degree than al Qaeda or other foreign terrorist organizations, ISIL has persistently used the Internet to communicate. From a homeland perspective, it is ISIL's widespread reach through the Internet and social media which is most concerning as ISIL has aggressively employed this technology for its nefarious strategy. ISIL blends traditional media platforms, glossy photos, in-depth articles, and social media campaigns that can go viral in a matter of seconds. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago.

Unlike other groups, ISIL has constructed a narrative that touches on all facets of life — from career opportunities to family life to a sense of community. The message isn't tailored solely to those who are overtly expressing symptoms of radicalization. It is seen by many who click through the Internet every day, receive social media push notifications, and participate in social networks. Ultimately, many of these individuals are seeking a sense of belonging.

As a communication medium, social media is a critical tool for terror groups to exploit. One recent example occurred when an individual was arrested for providing material support to ISIL by facilitating an associate's travel to Syria to join ISIL. The arrested individual had multiple connections, via a social media networking site, with other like-minded individuals.

There is no set profile for the susceptible consumer of this propaganda. However, one trend continues to rise — the inspired youth. We've seen certain children and young adults drawing deeper into the ISIL narrative. These individuals are often comfortable with virtual communication platforms, specifically social media networks.

ISIL continues to disseminate their terrorist message to all social media users — regardless of age. Following other groups, ISIL has advocated for lone offender attacks. In recent months ISIL released a video, via social media, reiterating the group's encouragement of lone offender attacks in Western countries, specifically advocating for attacks against soldiers and law enforcement, intelligence community members, and government personnel. Several incidents have occurred in the United States and Europe over the last few months that indicate this "call to arms" has resonated among ISIL supporters and sympathizers.

In one case, a New York-based male was arrested in September after he systematically attempted to travel to the Middle East to join ISIL. The individual, who was inspired by ISIL propaganda, expressed his support for ISIL online and took steps to carry out acts encouraged in the ISIL call to arms.

The targeting of U.S. military personnel is also evident with the release of names of individuals serving in the U.S. military by ISIL supporters. The names continue to be posted to the Internet and quickly spread through social media, depicting ISIL's capability to produce viral messaging. Threats to U.S. military and coalition forces continue today.

Social media has allowed groups, such as ISIL, to use the Internet to spot and assess potential recruits. With the widespread horizontal distribution of social media, terrorists can identify vulnerable individuals of all ages in the United States — spot, assess, recruit, and radicalize — either to travel or to conduct a homeland attack. The foreign terrorist now has direct access into the United States like never before.

In other examples of arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. As a result, it is imperative the FBI and all law enforcement organizations understand the latest communication tools and are positioned to identify and prevent terror attacks in the homeland.

We live in a technologically driven society and just as private industry has adapted to modern forms of communication so too have terrorists. Unfortunately, changing forms of Internet communication and the use of encryption are posing real challenges to the FBI's ability to fulfill its public safety and national security missions.. This real and growing gap, to which the FBI refers as "Going Dark," is an area of continuing focus for the FBI; we believe it must be addressed given the resulting risks are grave both in both traditional criminal matters as well as in national security matters. The United States Government is actively engaged with private companies to ensure they understand the public safety and national security risks that result from malicious actors' use of their encrypted products and services. However, the Administration is not seeking legislation at this time.

The FBI is utilizing all lawful investigative techniques and methods to combat the threat these individuals may pose to the United States. In conjunction with our domestic and foreign partners, we are rigorously collecting and analyzing intelligence information as it pertains to the ongoing threat posed by foreign terrorist organizations and homegrown violent extremists. We continue to encourage robust information sharing; in partnership with our many Federal, State, and local agencies assigned to Joint Terrorism Task Forces around the country, we remain vigilant to ensure the safety of the American public. Be assured, the FBI continues to pursue

increased efficiencies and information sharing processes as well as pursue technological and other methods to help stay ahead of threats to the homeland.

Intelligence

Integrating intelligence and operations is part of the broader intelligence transformation the FBI has undertaken in the last decade. We are making progress, but have more work to do. We have taken two steps to improve this integration. First, we have established an Intelligence Branch within the FBI headed by an Executive Assistant Director ("EAD"). The EAD looks across the entire enterprise and drives integration. Second, we now have Special Agents and new Intelligence Analysts at the FBI Academy engaged in practical training exercises and taking core courses together. As a result, they are better prepared to work well together in the field. Our goal every day is to get better at using, collecting and sharing intelligence to better understand and defeat our adversaries.

The FBI cannot be content to just work what is directly in front of us. We must also be able to understand the threats we face at home and abroad and how those threats may be connected. Towards that end, intelligence is gathered, consistent with our authorities, to help us understand and prioritize identified threats and to determine where there are gaps in what we know about these threats. We then seek to fill those gaps and learn as much as we can about the threats we are addressing and others on the threat landscape. We do this for national security and criminal threats, on both a national and local field office level. We then compare the national and local perspectives to organize threats into priority for each of the FBI's 56 field offices. By categorizing threats in this way, we strive to place the greatest focus on the gravest threats we face. This gives us a better assessment of what the dangers are, what's being done about them, and where we should prioritize our resources.

Cyber

An element of virtually every national security threat and crime problem the FBI faces is cyber-based or facilitated. We face sophisticated cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. On a daily basis, cyber-based actors seek our state secrets, our trade secrets, our technology, and our ideas — things of incredible value to all of us and of great importance to the conduct of our government business and our national security. They seek to strike our critical infrastructure and to harm our economy.

We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. For example, as the Committee is aware, the Office of Personnel Management ("OPM") discovered earlier this year that a number of its systems were compromised. These systems included those that contain information related to the background investigations of current, former, and prospective Federal government employees, as well as other individuals for whom a Federal

background investigation was conducted. The FBI is working with our interagency partners to investigate this matter.

FBI agents, analysts, and computer scientists are using technical capabilities and traditional investigative techniques — such as sources, court-authorized electronic surveillance, physical surveillance, and forensics — to fight cyber threats. We are working side-by-side with our Federal, State, and local partners on Cyber Task Forces in each of our 56 field offices and through the National Cyber Investigative Joint Task Force (NCIJTF), which serves as a coordination, integration, and information sharing center for 19 U.S. agencies and several key international allies for cyber threat investigations. Through CyWatch, our 24-hour cyber command center, we combine the resources of the FBI and NCIJTF, allowing us to provide connectivity to Federal cyber centers, government agencies, FBI field offices and legal attachés, and the private sector in the event of a cyber intrusion.

We take all potential threats to public and private sector systems seriously and will continue to investigate and hold accountable those who pose a threat in cyberspace.

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the Bureau have never been higher. Our fellow citizens look to us to protect the United States from all of those threats and the men and women of the Bureau continue to meet — and exceed — those expectations, every day. I want to thank them for their dedication and their service.

Chairman Johnson, Ranking Member Carper, and committee members, I thank you for the opportunity to testify concerning the threats to the Homeland and terrorists' use of the Internet and social media as a platform for spreading ISIL propaganda and inspiring individuals to target the homeland, and the impact of the Going Dark problem on mitigating their efforts. I am happy to answer any questions you might have.