HOW TECHNOLOGY HAS TRANSFORMED THE TERRORIST THREAT FIFTEEN YEARS AFTER 9/11

Featuring Michael Steinbach
Stein Counterterrorism Lecture Series
September 21, 2016

Read this item or watch video of the full event on our website.

Today, Michael Steinbach, the executive assistant director of the FBI's National Security Branch, delivered the latest presentation in The Washington Institute's long-running Stein Counterterrorism Lecture Series. The following are his prepared remarks.

First of all, I would like to thank Matthew Levitt and the Washington Institute for Near East Policy for inviting me to speak to you all today. All of us have had our hands full over the last couple years as we have seen the latest wave of international terrorism emanate from Syria and Iraq with the Islamic State of Iraq and al-Sham or ISIS. We have seen horrific examples across Europe, Africa, Southeast Asia and here in the United States. It does not matter whether we call it directed or inspired, the cancer growing from large swaths of ungoverned space in the Middle East directly impacts the safety of our communities here at home in the United States. In fact, I cannot do my job to keep our homeland safe without looking for answers in the Middle East. This is why the Institute's focus on improving U.S. Middle East policy is so important.

That being said, today I am not going to talk about ISIS, al-Qaeda, Hezbollah, the Levant, or any other particular group or region because strategically there is another fundamental discussion that needs to take place. As a leader in the national security arena, I want to discuss adaptability. The threats we face today have evolved and continue to do so. The complex nature of the terrorism threat requires a different way of doing business than it did just a few years earlier. It requires organizations and leaders to be agile and adapt to the ever changing threat landscape. And it does not matter where the threat originates from -- the Middle East, Africa, Indonesia. I was at Europol last week and leaders used the terms "complex" and "complexity" numerous times in describing the threats our nations face. Complex organisms such as ISIS require us to prioritize adaptability. So if you will, let me explain where we, as leaders, need to focus our attention in our efforts going forward.

The problem a decade ago seems so simple in today's world with today's threat. Let me flesh this statement out a bit. For simplicity, I will describe three fundamental paradigm shifts security organizations like the FBI have had to deal with over the past fifteen years. The first paradigm shift is 9/11, where as an organization we were required to move from a largely reactive agency to a proactive, prevent-oriented agency. At that time, I worked on a bank

robbery squad in Chicago. Success for me was to come in after a bank robbery and conduct a thorough investigation -- interview witnesses, review CCTV, conduct a neighborhood canvass, etc. The goal was to identify, arrest, and prosecute the bank robber. Such a result would often be glorified in a short news story in the *Chicago Tribune* where our keen investigative skills were applauded. But how does this investigative model hold up against the East Africa bombings, the USS *Cole* attack, the 9/11 attacks? Crime committed, investigation conducted, bad guys held accountable (if still alive). To really oversimplify this example, the first paradigm shift now asked the FBI to arrest the bank robber before he robbed the bank.

So how did we accomplish this prevent-based defense? We all know the tripwires we looked for post 9/11 were travel-based. Take for example the 2002 FBI investigation of the Lackawanna Six from New York. The group traveled overseas to an al-Qaeda camp where they trained and returned, leaving investigators a trail of records along the way. Post 9/11, this was our playbook and we were successful.

But the bad guys evolved and the second paradigm shift occurred a few years later and revolved around the anonymity of the Internet. Travel and the associated tripwires were no longer a prerequisite to conducting an attack. Now groups like al-Qaeda could inspire and radicalize remotely -- Anwar al-Awlaki became the most powerful influencer in the history of terrorism, all through his online sermons. The FBI was required to adapt as well to the changing threat, and we did by focusing on forums -- the watering holes -- where the bad guys amassed. We developed tools to deal with this new form of threat, the inspired lone wolf.

And today -- with ISIS leading the way with a dispersed and effective media apparatus -- we face a third paradigm shift, which results in individuals inspired by a faceless demon, trained anonymously via a multitude of communication platforms in a dark web no agency can peer into. While the Internet facilitated terrorists' widespread reach across the globe over the last decade, the latest evolution of the threat transcends barriers like never before and again challenges us. What I am referring to is the use of social media where a message or a video can go viral and spread across the world in minutes; where any of more than 2.3 billion active social media users can push propaganda out on a public site and then continue communicating via private encrypted messages. Social media and terrorists' effective exploitation of social media concern me. Like never before, social media allows for overseas terrorists to reach into our local communities -- to target our citizens as well as to radicalize and recruit. In other words the bad guys use the same widely available and inexpensive handheld gadget to identify both target and targeteer.

Social media is no longer just a harmless playground for our teenagers and young people; social media platforms connect many parts of our society. But by virtue of their connectivity to social media, individuals within any demographic can be a target. Groups such as ISIS have used the content from online postings to gather personal information, including photos, identities of family members, and home addresses. Today, 78 percent of Americans have at least one social media account, and more than half of the adult population accesses those platforms using a

smartphone. The worldwide abundance of smartphones as social media's access point and the volume of social media use are daunting obstacles to securing the safety of our communities.

This same social media activity can also be used to identify potential recruits. Previously, even with the anonymity of the Internet, a foreign terrorist organization had to wait for an individual to come to an online forum seeking information. In today's social media age, terrorists can proactively troll social media sites for individuals they believe may be susceptible and sympathetic to the message -- think about the distinction. These potential recruits may be just looking for a place to fit in. Online recruiters feed them a steady false narrative, suggesting they join their cause and become part of something bigger; this sense of belonging appeals to individuals who seek a purpose or who crave action. And the radicalization is not just occurring when an individual accesses a site; with social media push notifications and smartphones, it's radicalization literally twenty-four hours a day, seven days a week.

More so than ever before, and partly as a result of this third paradigm shift, we truly live in two distinct worlds -- a physical world and a digital world. For years, we in the law enforcement and intelligence community built out the terrorist networks through the physical world, identifying the facilitators, financiers, planners, and operators. Today we must often build out a network starting with an anonymous online moniker -- with no clue as to whether the individual is male or female, young or old, in Syria or the United States. In 2015, the FBI had about seventy terrorism disruptions, with a large percentage of those investigations beginning in the digital world.

This is where the challenges of today become particularly evident with two byproducts of social media, of the digital world. Those two byproducts are volume and encryption. They are overwhelming in their span and complexity. And they build an invisible barrier between us and the bad guys. Now, a bad guy has the ability to create numerous identities with a few strokes of the keyboard or swipe of the smartphone. He develops relationships and once an individual confides a willingness to act, the conversation switches to platforms with end-to-end encryption for heightened privacy. The use of encrypted communication then becomes the norm. Very few of our targets are communicating in the open today. These encrypted messages are not only hidden from the public's watchful eye but are also impenetrable by the global law enforcement community. These methods of communication among groups are becoming the norm. For example, in the spring and summer of 2015, we had about a dozen individuals in the United States planning attacks via encrypted channels with members of ISIS.

The challenge we face is to remain agile, specifically in terms of technological advances. As technology evolves, the bad guys adapt. We, too, need to be willing -- and able -- to adapt to the ever-changing threat environment. We have a tendency to fight the last war using yesterday's technology. Much of the time technology is outpacing our workforce's capabilities. So what's the answer? Let's start by digging in further on the topics of volume and encryption.

Let's start with the volume issue. When I started as a case agent we were taught to ask logical investigative questions -- the bad guy's personal information, physical characteristics, and associations. We'd jot the information down in our notebook and run it through the systems to see if we could glean any known connections. We've seen a scaled progression of the standard baseline collection from physical traits to phone numbers, email addresses, and now usernames, making the "standard" even more complex. To add to that, many people don't have just one phone number or one email account. I'm sure many of us in this room have a home phone number, a cell phone, an office number. We also have a personal email account, work email account. Now stop for a moment and think about the online accounts you have and all the different information you entered to create those usernames and accounts. That's a lot to keep track of personally. But now imagine those individuals who intentionally create one account after another to cover their digital bread crumbs and, ultimately, to hide from us. These digital profiles have become equally critical to our investigations.

The size and scope of these digital profiles is transforming the way we do business. Why is that? We need to track down and evaluate all of the associated digital profiles because they may be the only clues we have. To accomplish this task, we must sort through the large volume of social media connections (the noise) to find the digital profiles (the signal) that are part of our terror network. I cannot emphasis this last point too loudly -- the volume of potential contacts can be in the tens of thousands. Think how that compares to the historical volume in identifying physical global networks.

For example, both the November Paris attacks and the December attack in San Bernardino contained multiple subjects with multiple online profiles. During investigations such as these, the online profiles often give insight into the subjects. Sometimes it's obvious, within the profile description or publicly shared content; most times, it's in the digital connections.

In the end, the digital investigation alone can result in an abundance of information. And that's likely an understatement. It could take us weeks to comb through the lines and lines of data and the endless connections enabled by the online world to determine what warrants our attention. This could add up to valuable time spent before we even identify the key connection. The connection, the ties to the subject -- it's in the online world. It's just sitting behind a screen.

The second challenge is encryption. Not only do we face the overwhelming volume of information we've uncovered, the second challenge is the lack of accessible information when the person is using encrypted communications. Encryption takes many forms. Encryption hides stored digital communications; sometimes it masks the trail of communications; and at other times it erases the content.

In the May 2015 shooting outside of the "Draw the Prophet" event in Garland, Texas, one of the shooters communicated with an overseas terrorist associate using an encrypted communications platform -- including more than 100 times on the day of the attack. The

investigation uncovered the shooter intentionally used the end-to-end encryption platform to ensure his communications would remain secure. To this day, we still do not know what the discussions were about.

Encrypted communications quickly eliminate the digital trail. These digital dead ends can be deadly for our communities.

What are we doing to set ourselves up for success in the future? As leaders, we must look at our organizational processes and adapt to the current and emerging threat. Specifically with volume and encryption, we need to look at tools and training for the answers.

It's up to us to arm our teams with the right tools. We will always be behind if we're using yesterday's technology. Resources need to be renewed on a regular basis to ensure we are fighting the war with weapons on par with our opponents. We owe it to our people to invest in tools that will help them do their jobs better and to face the technology overload head on. When I talk about the volume of information being unmanageable at times, using technology to sort or prioritize information could save many man hours. But we need to be smart with technology -- it's not just about spending money. How can we leverage technology -- cloud-based solutions, cognitive computing, commercial products that can be layered on top of our classified databases? I am talking about strategic solutions. Last year we were faced with a few super users who, from safe havens in Syria, spread venomous ideology throughout the online world on behalf of ISIS. These individuals accumulated thousands of followers. For us to fully tackle not only the subjects but also to analyze their reach and identify potential additional actors, it seemed like an impossible task. At one point there were more than 30,000 associates, and the web of connections kept expanding. We learned that smart data crunching programs can help sort through the noise and allow for human analysts to focus on the true bad guys.

Importantly, we need to ensure new tools are coupled with adequate training. Tools are no good unless people know how to use them. When we take a look at our workforce and the collective caseload and think about how it's evolved over the years, how do we adapt? How do we position our people to adapt? It's a culture shift. Throughout history it's been done time and time again. The only difference this time is the speed at which we need to learn and adapt. As I said earlier, new technology comes out fast. Folks, we're not using brick phones or pagers anymore. In fact you can assume if you or I are being introduced to new technology, it's likely already been in the marketplace for some time and our kids have thoroughly mastered it.

The law enforcement and intelligence community has vast experience investigating and identifying individuals once we have resolved a biographic identity. The critical task today is to traverse the identity divide as quickly as possible, going from the anonymity of cyberspace to a live body before subjects can go -- in the world of terrorism -- from flash to bang.

For example, in June 2015 we became aware of an individual known only by an online moniker. This anonymous individual communicated to an overseas terrorist group that planned to conduct an attack in the United States in the coming weeks. But who was it? Male or female? Juvenile or adult? Located in the United States or overseas? Plotting to kill or ready to act? These are questions with answers hidden in an individual's digital footprint. Sometimes the answers are easy to extract, but at other times, they are nearly impossible to find. In this case, the individual provided subtle clues that assisted us in narrowing down the geographic area. This case started like many of our cases today, beginning with an anonymous digital persona, later leading to a physical human being. There is no way to stop the growing identity divide, and technology trends indicate it will only become easier to erect identity barriers to hide a biographic identity. In this case, we resolved to the real person by utilizing a hybrid team consisting of members who had the traditional investigative skills as well as members who had the digital know-how. Without both of these components working in coordination, we would not have been as successful as we were.

It's all about being adaptive in our processes -- pushing our teams to innovate and not be comfortable just because we have always done it that way. In fact, phrases like that and "why fix it if it's not broke" are poisonous declarations if our goal is truly an agile workforce. But what I am describing can be a huge shift for our workforce. Many of us grew up without cellphones and were around long before the Internet. We had to learn how to adjust to the connected lifestyle. We are digital immigrants. We try our best to learn the latest app but it's likely not intuitive. However, much of our younger workforce is just the opposite. We work side-by-side with individuals who have never known life without the Internet, had a cellphone before they started high school, and navigate the online world almost as comfortably as the physical world. They are digital natives.

Digital immigrants are extremely experienced in traditional investigative practices. For digital immigrants, the street holds the answers -- interviews, informants. Digital natives, on the other hand, are our colleagues with so many monitors at their desk that some are turned sideways and who are equally comfortable using Google as a noun, adjective, or verb. But we need both skill sets equally in today's fight against terrorism.

Remember, bad guys are actively looking to put as many barriers between their digital and biographic identities as possible by concealing their IP address, using end-to-end encrypted messaging apps, and registering for social media with spoofed identifiers. A workforce splintered in its approach to navigating between the digital and physical worlds is doomed to fail.

Being adaptive also means looking at how these complex organizations communicate and move. As we have seen in Europe with ISIS external operations, their ability to do both has outpaced Western governments' ability to push actionable intelligence and prevent attacks. In the digital world, it's not sufficient to say information sharing is important. It's now the speed of information sharing that is critical to success. It's the difference between sending a letter

through the U.S. Postal Service for delivery a few days later versus sending a message via email for delivery in a matter of seconds. In both cases the message arrives -- but days is too long a timeframe if a terrorist has struck and killed in the meantime.

We must resist the urge to accept political theater post attack where broad general statements are made that information sharing has improved. We need to allow that information sharing in itself is complex and work with partners to develop robust systems that take into account the type of information to be shared (identifiers, biometrics, analysis) and the form of information to be shared (raw data, finished intelligence). We need to have difficult discussions with intelligence agencies, security agencies, law enforcement, and border control agencies. How is the classified information being used rapidly in a usable format at a speed that is faster than a train ride or flight? It's great that CIA is sharing with MI6, but if a terrorist travels from Heathrow to Dulles undetected who cares? These solutions also require adaptive new models that consider deconfliction, access, privacy, storage, and use.

The coming year will present continued challenges as Western allies continue to squeeze ISIS's operating space. While this is a measure of success, it will bring with it a more dangerous world in 2017 and 2018. Yet the bar remains set very high for us in this line of work: zero terrorist attacks on the homeland. To achieve this standard we need strong leadership. Whether you're in the public sector or private sector fighting, leaders in today's hyper technology-driven world must ignore sayings such as "don't fix it if it ain't broke" and instead lean forward to accepting change as the new norm. The only certainty I can give you is that I cannot predict the global landscape sufficiently to know exactly what the threat will look like. But by instilling a culture of adaptability in our organizations we can meet head on the challenges of 2017 and beyond.

THE WASHINGTON INSTITUTE FOR NEAR EAST POLICY
1111 19TH STREET NW, SUITE 500
WASHINGTON, DC 20036
202-452-0650
202-223-5364 (fax)
www.washingtoninstitute.org