FBI Threat Landscape

Web Forum

On July 31, 2018, Gregory W. Ehrie, Special Agent in Charge of the Newark Field Office, Federal Bureau of Investigation (FBI), provided a briefing and discussion on the current threat landscape from the FBI’s perspective. This document provides a summary of the main insights included in the presentation, as well as the most important issues addressed as part of the discussion with participants.

Introduction

The web forum included an overview of various threats from the perspective of the FBI. In addressing these threats the FBI considers partnerships with the private sector and other agencies to be critical. The discussion focused on three areas: counterterrorism, cyber threats and criminal organizations.

Counterterrorism

Counterterrorism is the top priority at the FBI. There has been an increase in the complexity of threats and a rapid evolution of the speed and agility of actors.

There are thousands of Islamic State related cases in all 50 states of the nation. This threat is not centered in just the big cities. These are homegrown violent extremists. Once a person is on the FBI’s radar for counterterrorism it is difficult to get off because it’s hard to know when that risk will go away.

The threat posed by the Islamic State is very different from al-Qaeda. They’ve revolutionized terrorism and taken it to a different level. There are three prongs related to this threat:

- Attract people to the caliphate
- Propaganda efforts to get people to participate in terrorism, and
- The terrorism diaspora – where will these actors go to, emigrate, move, etc.

There has been a very significant decrease in the number of people going to the Middle East and this is also affecting their propaganda. But there is a lingering phenomenon with individuals that are still inspired. Their propaganda speaks to people who are interested in this issue and it draws them in. This propaganda can be accessed on the Internet.

An important threat is that as the caliphate is defeated, radicalized people who have been trained in fighting are now going back to Western Europe, Southeast Asia or the US.

Homegrown terrorism is defined as people radicalized here who are inspired by jihadism. The challenge is detecting who they communicate with.
With al-Qaeda, the intelligence community was able to intercept a plot and step in, but now individuals are using cars and finding targets, and it’s very difficult to track that.

The intelligence community has been analyzing their propaganda in social media and companies such as Facebook, Google and others are supporting the efforts of the intelligence community in terms of monitoring and suppressing it.

Another challenge of addressing the threat of homegrown terrorism is that there aren’t many commonalities in terms of the individuals that are drawn in. They are across all society. It is not just disaffected people. It also involves wealthy individuals and those who are motivated by ideology. A minority have sought mental health services, but it can be anybody. It is not easy to identify who may turn into an extremist.

Another challenge that the intelligence community faces is too much information. For example, looking at an individual’s contacts on social media and across multiple devices is very resource intensive. These agents are also very sophisticated in terms of the technology they use.

The intelligence community needs to have the right people on board and to constantly replenish human resources and have new ideas. There is also a need for IT specialists to help with the flood of data that is now available.

The FBI also needs to strengthen its partnerships with the private sector. The FBI is about the size of a medium or large police force, with about 13,000 agents. So the FBI needs to work with others like educators, police officers, human resources personnel, since they are likely to be the ones that see the first signs of a person being radicalized.

Information sharing also needs to be much more fluid and the FBI is always looking for partners in this area. This includes participating in task forces, and informing people of the agency’s activities through InfraGard, a partnership between the FBI and members of the private sector.

Another area of collaboration between the FBI and the private sector is by participating in active shooter training exercises. It is good for companies to include their federal partners in these activities.

The FBI also collaborates with the private sector through the Domestic Security Alliance Council (DSAC), an American governmental/corporate alliance that engages in information sharing to protect the interests of the nation.

Q. Is there a potential for the use of drones? Is this a concern?

Yes, the FBI is working with drone manufacturers. People are interested in the positive use of this technology, like deliveries, etc. as proposed by companies such as Amazon. But the FBI also recognizes this as a threat. For example, the use of drones to make drug deliveries or to deliver bombs or weapon parts. It’s a very anonymous technology and they are very difficult to track. They are plug and play, you can use GPS and walk away. The intelligence community hasn’t seen this in the US but it is something of concern and the best partners for the FBI in this area are private sector companies.
Cyber threats

All the threats that concern the FBI manifest themselves as cyber threats. All our sensitive information is in cyber and this is where people are going to try to hurt you. This is an area where the FBI may be a little behind.

**Nation states** are a cyber threat. China, Russia, North Korea and Iran are aggressively attacking the U.S. China’s strategy is for a time frame of 50-100 years.

These nation states have hundreds of hackers and are looking at hospitals, businesses, infrastructure, to understand how they work, and also stealing secrets from the private sector. The FBI can work with the private sector to assess a company’s computer infrastructure. In the past the agency has found passive collection devices from nation states.

**Election security** is a continuing threat with the midterm elections coming up. Nation states like Russia are interested in having access to electoral systems. They seem to be interested in monitoring what happens. They haven’t tried to change the results but they have other ways of exerting influence through social media, etc.

**Ransomware** attacks are another cyber threat. The agency has seen sectors like the medical community be the targets of ransomware with patient records and other information. The FBI asks those affected not to pay a ransom. It’s not going to stop it. If an organization pays the ransom once, it will pay it again. If this issue affects your organization you should contact the FBI. The agency will not make it public. Ransomware is a growing concern.

**Q. Is there anonymized information that the private sector can use to build responses for it?**

Certainly. The FBI doesn’t want to advertise ransomware responses. The actors responsible for ransomware adapt and change the code. DSAC is also a good place for this kind of discussion. The FBI can do one-on-one consultations too.

The FBI is also looking into ways that terrorists could operate in the cyber field. They have not yet been seen going to intrusion and ransomware, but the agency expects this will happen.

The FBI is trying to impose a cost on cyber-crimes. For example, charging Chinese military and Russian officials with cyber espionage charges.

**Criminal Organizations**

In terms of criminal organizations, **MS-13** is the most violent gang and the FBI is watching them very closely. They are very difficult to infiltrate because they kill anyone they suspect of talking to the police. As one hotspot is improved they move somewhere else. The FBI is trying to understand their strategy.

There are multiple gangs with increased activities in NJ and other places and this is a rising trend related to opioids. **Opioids** are immediately addictive and affects individuals across the whole spectrum of
society from wealthy to poor. High level opioids are being distributed by doctors. The strategy is to get as many people addicted to them as possible so they can keep selling these drugs.

With regard to the legalization of marijuana, the FBI is anticipating issues with edibles and the amounts people may consume and how that will affect them. Gummies or squares can be used for medical marijuana but it could lead to unanticipated uses and behavior.

Q&A

Amazon will deliver to your locked car. Is this an issue?

The FBI is concerned about how these technologies could be used for illegal things like anonymous drug deliveries.

With an increasing prison population, will there be more radicalization?

This is an issue, it is a place for radicalization like white supremacy. We don’t see it as much because there are very good intelligence systems built into prisons. The radicalization that concerns the FBI happens in places where the agency doesn’t have an optic to them.

Where do criminal organizations get the money to use tech?

Money typically comes from prostitutions, drugs, robberies and burglaries. The technology piece is also pretty inexpensive. Ransomware is a cheap, effective crime. It’s much more anonymous and difficult to find than something like kidnapping. Another example is obtaining blueprints for 3D printable guns, which may cost $28.

How can a company get in touch with the FBI to get an assessment?

You can call office directly and they will put you in touch with the right people. Let the FBI be your friend before something happens. Give the agency a call and we’ll talk about whatever concerns you.

How active are the African terrorist groups like Boko Haram, etc.?

Not much, they support other major groups but they don’t have the capacity to extend to the US now. They are starting to do more on the cyber realm. But the FBI is not currently seeing an attack from those groups.

Additional Resources:

• Federal Bureau of Investigation (FBI): https://www.fbi.gov/
• FBI Newark Field Office: https://www.fbi.gov/contact-us/field-offices/newark
• FBI New York Office: https://www.fbi.gov/contact-us/field-offices/newyork
• The Domestic Security Alliance Council (DSAC): https://www.dsac.gov/
• InfraGard: https://www.infragard.org/