Copyright 2015 Roll Call, Inc. www.cqrollcall.com
All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of Roll Call. You may not alter or remove any trademark, copyright or other notice from copies of the content.

HOUSE COMMITTEE ON HOMELAND SECURITY HOLDS A HEARING ON TERRORISM IN GARLAND, TEXAS

June 03, 2015

SPEAKERS:

REP. MICHAEL MCCAUL, R-TEXAS.
CHAIRMAN

REP. PETER T. KING, R-N.Y.
REP. LAMAR SMITH, R-TEXAS
REP. MIKE D. ROGERS, R-ALA.
REP. CANDICE S. MILLER, R-MICH.
REP. JEFF DUNCAN, R-S.C.
REP. TOM MARINO, R-PA.
REP. LOU BARLETTA, R-PA.
REP. SCOTT PERRY, R-PA.
REP. CURT CLAWSON, R-FLA.
REP. E.L. "BUDDY" CARTER, R-GA.
REP. WILL HURD, R-TEXAS
REP. JOHN KATKO, R-N.Y.
REP. BARRY LOUDERMILK, R-GA.
REP. MARTHA MCSALLY, R-ARIZ.
REP. JOHN RATCLIFFE, R-TEXAS
REP. MARK WALKER, R-N.C.
REP. PATRICK MEEHAN, R-PA.
REP. DANIEL M. DONOVAN JR., R-N.Y.
REP. PETE SESSIONS, R-TEXAS

REP. BENNIE THOMPSON, D-MISS.
RANKING MEMBER

REP. LORETTA SANCHEZ, D-CALIF.
REP. SHEILA JACKSON LEE, D-TEXAS
REP. BRIAN HIGGINS, D-N.Y.
REP. CEDRIC L. RICHMOND, D-LA.
REP. WILLIAM KEATING, D-MASS.
REP. DONALD M. PAYNE JR., D-N.J.
REP. FILEMON VELA, D-TEXAS
REP. BONNIE WATSON COLEMAN, D-N.J.
REP. KATHLEEN RICE, D-N.Y.
REP. NORMA J. TORRES, D-CALIF.
REP. JIM LANGEVIN, D-R.I.

WITNESSES:

- JOHN MULLIGAN, DEPUTY DIRECTOR, NATIONAL COUNTERTERRORISM CENTER
- FRANCIS TAYLOR, UNDERSECRETARY FOR INTELLIGENCE AND ANALYSIS, DEPARTMENT OF HOMELAND SECURITY
- MICHAEL STEINBACH, ASSISTANT DIRECTOR, COUNTERTERRORISM DIVISION, FBI

MCCAUL: The Committee on Homeland Security will come to order. The purpose of this hearing is to receive testimony regarding the increasing threat from violent Islamic extremists groups, such as ISIS, who use the Internet and social media to recruit fighters, share propaganda and inspire and potentially direct attacks.

And before I recognize myself for an opening statement, I'd like to welcome our newest member of the committee, Congressman Daniel Donovan of New York. We have another -- yet another New Yorker on this committee. Quite a contingency we're building.

But his experience as a district attorney and dedication to public service make him a, I believe, valuable asset to this committee, and we're happy to have you, sir. Appreciate it.

I now recognize -- I yield to the gentleman from New York.

(UNKNOWN): I'd like to join you in welcoming Mr. Donovan. (inaudible) many years. He's an outstanding district attorney, outstanding public servant, and he's going to be able to work across the aisle for the betterment of the country.

So Dan, it's great to have you on board. Thank you.

MCCAUL: Ms. Rice...

RICE: Just it show how bipartisan we are all going to be, as a Democrat, I would like to welcome my former colleague, D.A. -- former D.A. Dan Donovan. Great to have you here, and look forward to working with you.

Thank you, Mr. Chairman.

MCCAUL: Anybody else -- anybody else like to -- Mr. Richmond?

Onto a more serious topic, just yesterday in Boston, reports are emerging that Mr. Raheem was killed by federal law enforcement officers after lunging at them with a knife. He was being investigated by the Boston Joint Terrorism Task Force after communicating with and spreading ISIS propaganda online.

Known associates of Mr. Raheem are also being arrested as we speak. These cases are a reminder of the dangers posed by individuals radicalized through social media.

In Garland, one month ago, Elton Simpson fired off a series of tweets declaring his loyalty to the Islamic State and urged others to do the same. Simpson included a hashtag, texasattack, previewing his decision to terrorize the Prophet Mohammed cartoon contest that Islamists on social media had signalled out as a target.

In his final tweets minutes before the attack, Simpson told his followers to follow Junaid Hussain, also known as al-Britani, a 20- year-old British foreign fighter embedded with ISIS in Syria and one of the group's top recruiters, who has been linked to the CENTCOM Twitter hack in January of this year.

Hussain was quick to praise the Garland attack and issued a warning that same night stating, quote, "The knives have been sharpened. Soon we will come to your streets with death and slaughter."

This attack exemplifies a new era in which terrorism has gone viral. Extremists issued a call to arms to attack an event. A radicalized follower clearly heeded that call, and he took steps to make sure his act of violence would spread and motivate more.

Social-media networks have become an extension of the Islamist terror battlefield overseas, turning home-grown extremists into sleeper operatives and attackers.

The proliferation of jihadist propaganda online has established a new front in our battle against Islamic extremists. We are no longer hunting terrorists living in caves and who only communicate through couriers; we are facing an enemy whose messages and calls to violence are posted and promoted in realtime over the Internet.

For example, last month, the threat level at military bases across the country was elevated after ISIS supporters posted the names of individuals serving in the military online and quickly spread this on social media.

Aspiring fanatics can receive updates from hardcore extremists on the ground in Syria via Twitter, watch ISIS blood lust on YouTube, view jihadi selfies on Instagram, read religious justifications for murder on JustPasteIt and find travel guides to the battlefield on Ask.fm.

Jihadi recruiters are mastering the ability to monitor and prey upon Western youth susceptible to the twisted message of Islamist terror. They seek out curious users who question, -- have questions about Islam or want to know what life is like in the so-called Islamic State. They engage, establish bonds of trust and assess the commitment of their potential recruits.

From there, extremists direct users to continue the conversation on more secure apps, where secure communications hide their messages from our intelligence agencies.

Such communications can include advice for traveling to terror safe havens, contact information for smugglers into Turkey or the membership process for joining ISIS itself.

I know the officials appearing before us here today are disturbed by these trends.

Mobile apps like Kik and WhatsApp as well as data-destroying apps like Wickr and Surespot are allowing extremists to communicate outside of the view of law enforcement. Equally as worrisome are ISIS attempts to use the Dark or Deep Web.

These Web sites hide I.P. addresses and cannot be reached by search engines, giving terrorists another covert means by which they can recruit fighters, share intelligence, raise funds and potentially plot and direct attacks undetected, as we saw yesterday in Boston.

ISIS tailors its message for specific audiences around the globe and in doing so projects power far beyond the safe havens by amplifying its battlefield successes and winning over new converts across the world. Its media sophistication helps legitimize self- proclaimed caliphate in its perverse interpretation of Islam.

This stands in stark contrast to Al Qaeda's past outreach, which relied on tightly controlled, top-down messaging and propaganda more difficult for aspiring jihadists to find.

Today, ISIS is instead taking a grassroots approach to terror, seeding its repressive world view from the ground up. From digital magazines to online videos that glorify barbaric murder, ISIS is using its multi-platform engagement to create a jihadi subculture that supports its violent ideology and encourages attacks against the United States and its allies.

These tactics are a sea change for spreading terror, and they require from us a paradigm shift in our counterterrorism, intelligence and our operations.

For example, we can start doing what FBI Director Comey suggested, shaking the trees more aggressive to quickly identify and engage potential homegrown jihadis.

MCCAUL: But this is a dynamic new front in the war against Islamist terror, and it will require a new approach with a heavy focus on the ideological battlespace.

I'm grateful for the three witnesses we have here today that are dealing first-hand on the front lines with how this terror is going viral. And I look forward to hearing their testimony and recommendations for confronting this new and dangerous challenge.

And with that, I now recognize the ranking member

THOMPSON: Thank you, Mr. Chairman. Thank you for holding today's hearing.

I'd like also to thank the witnesses for appearing today.

On May 3rd, the American Freedom Defense Initiative, which is recognized as a hate group by the Southern Poverty Law Center, organized a Mohammed art exhibit and contest event in Garland, Texas. Two violent extremists, armed with assault rifles and body armor, attacked police that were providing security to the event, resulting in the wounding of a dedicated police officer.

According to the FBI, just hours before the Garland attack, a bulletin was issued to state and local police stating that one of the assailants may have an interest in traveling to the event. Unfortunately, the local police stated that the bulletin was not received in time.

Mr. Chairman, by no means am I saying that this bulletin would have changed the outcome of the situation. But I do think that this illustrates that we need to continue looking into information-sharing with state and local police, and also listening to the boots on the ground on how to recognize and prevent acts of home-grown violent extremism.

In the days following the attack in Garland, supporters of the terrorist group ISIL praised the attack. After the attack, it was discovered that one of the gunmen detailed his plans to leave the country and travel to Syria to join ISIL on Twitter. The assailant's plans were disrupted when the FBI arrested some people that planned to travel with him.

It also came to light that he engaged with other ISIL followers from around the world through Twitter.

Mr. Chairman, we know that the threats from foreign and domestic terrorist groups are not going away overnight. Using the Internet and social media to recruit members, plan attacks and spread ideology is not novel. As the director of the National Counterterrorism Center pointed out in a hearing in this committee in February, ISIL's exploitation of social media plays a prominent role in the group's ability to recruit fighters from around the world.

But as we look at social media and how violent extremist propaganda is spread, we must look at ways to counter-message. Both sides of the aisle are engaged in an examination of the president's countering violent extremism strategy. The department has a vital role to play in carrying out that strategy, as evidenced by the fact that there is a dedicated CVE coordinator, David Gernstein (ph), working.

Mr. Chairman, at this time, I request that this committee have an open oversight hearing where we can take testimony from DHS's CVE coordinator about the department's role in implementing the CVE strategy.

Furthermore, we know that more work remains to ensure that our foreign partners are willing to and able to stop and identify foreign fighters at their borders. Last Friday, the U.N. Council issued an unprecedented statement urging countries to enforce border controls that allow suspected terrorists to travel across international borders. The director of the NCTC also stated at our February hearing that there was work to be done in this area.

I know that the committee has a task force that is examining this issue and we should be receiving their recommendations soon.

Mr. Chairman, as I stated in our last hearing on this issue, we all have to -- a stake to prevent terrorist attacks against Americans and on American soil. Accordingly, I encourage this committee to continuous -- continue serious discussions on how to counter violent extremist messages, while protecting constitutional rights.

As we consider this threat, we need to foster greater information sharing among the diverse partners and seek new ways to work together to pursue effective and promising approaches to violent extremism.

With that, Mr. Chairman, I yield back.

MCCAUL: I thank the ranking member.

First, I ask unanimous consent that the gentleman from Texas, Mr. Sessions, the chairman of the Rules Committee, also represents Garland, Texas, be allowed to sit on the dais and participate in today's hearing.

Without objection, so ordered.

The gentleman from Texas is recognized.

SMITH: Mr. Chairman, I'd like to ask unanimous consent to be recognized out of order for two minutes.

MCCAUL: Without objection.

SMITH: And Mr. Chairman, I appreciate your and the ranking member's indulgence. And I'll yield my two minutes to the gentleman from Texas, the chairman of the Rules Committee, Pete Sessions.

MCCAUL: Mr. Sessions is recognized.

SESSIONS: Mr. Chairman, thank you very much.

And my thanks to Chairman Lamar Smith, my colleague from San Antonio, for kindly yielding time to me. And I also want to thank the young chairman of the Homeland Security Committee, the gentleman from Austin, Michael McCaul, as well as the ranking member, my good friend, Bennie Thompson, and members of the committee.

Thank you for inviting me to participate in today's hearing to discuss the ISIS-inspired terrorist attack in Garland, Texas. As the proud representative of the 32nd Congressional District of Texas, I'm pleased to notify each and every one of you that all of North Texas is committed to fighting terrorism. Specifically, the city of Garland, Texas is a diverse, all-American city that continues to attract families and businesses with its thriving economy and growing opportunities.

Since 1891, this city has grown from a small cotton farming community to a thriving metropolitan area outside of Dallas, with almost a quarter-million people that call Garland, Texas home.

The mayor of Garland, Texas, Doug Athas, is a friend of mine and he works closely with his city managers, William Dollar and Brian Bradford, as well as the police chief, Mitch Bates, and local officials including the school board and other community leaders, to ensure that Garland is a great, safe city to live in.

On Sunday, March 3rd -- May 3rd, 2015, a courageous Garland police officer swiftly acted to protect the people of Garland from what could have been a devastating situation. I would like to commend the police officer and all members of local law enforcement who stood in the face of terrorism and protected countless innocent lives.

I remain committed to working with each of my colleagues in the House, local leaders and local law enforcement, to uphold our duty as elected officials to protect the people who we serve. It is my sincere hope that today's hearing that we can learn positive lessons so that other cities and communities can be as prepared as Garland, Texas if an event were to happen in their local community.

Mr. Chairman, thank you very much. I yield back my time.

MCCAUL: I thank the gentleman from Texas.

Other members of the committee are reminded that opening statements may be submitted for the record.

I'm pleased to have a distinguished panel of witnesses before us today on this important topic. The first, John Mulligan, joined the National Counterterrorism Center in March 2015 as deputy director. Previously, he served as associate deputy director for counterterrorism at the National Security Agency.

Next, we have Mr. Francis Taylor, assumed his post as undersecretary for intelligence and analysis at the Department of Homeland Security in April of 2014. Previously, he served as assistant secretary of state for diplomatic security and director of the Office of Foreign Missions.

And finally, we have Mr. Michael Steinbach, who was appointed by FBI Director James Comey as the assistant director of the Counterterrorism Division in July of 2014. Prior to assuming his current position, he served as deputy assistant director of the Counterterrorism Division and the acting section chief of the FBI's International Terrorism Operations Center.

I want to thank all of you for being here today.

The chair now recognizes Deputy Director Mulligan to testify.

MULLIGAN: Thank you, Chairman McCaul, Ranking Member Thompson, and members of the committee. I greatly appreciate the opportunity to discuss some of the recent events of interest to the committee and the growing threat of extremists' use of social media to national security.

I'm pleased to join my colleagues from Homeland Security and the Federal Bureau of Investigation. As you already know, we work closely every day as part of the counterterrorism community, and that interagency partnership is one of the keystones of our homeland defense.

This morning, I will speak briefly to you about the recent attempted attack in Garland, Texas and the role of violent extremist social media in that event. Then I will transition to broader remarks on ISIL's use of social media before concluding by sharing some of the efforts NCTC and our partners across the federal government are pursuing to counter that avenue of threat.

MULLIGAN: As has already been described, last month, two U.S. citizens attacked an art exhibit and cartoon contest in Garland, Texas. The attackers arrived on the day of the events, exited their car, and opened fire with semiautomatic rifles, injuring a guard on the scene.

Thankfully, local law enforcement partners in the area were aware of the potential for violence and were able to respond quickly to prevent the attack from injuring or killing others. This event highlights the growing threat our nation faces from a new generation of terrorists, often operating

from afar, who use social media to find like-minded associates within our borders who can be motivated to violence, attacking with little or no warning.

As was indicated in this case, an online ISIL supporter on Twitter posted a link to an article with information about the cartoon contest a few weeks beforehand. This supporter's posting also included a message suggesting extremists should follow in the footsteps of the Charlie Hebdo attack in Paris.

Days later, one of the Garland attackers reached out to ISIL supporters and asked to move their communications to private Twitter messaging. This same individual also urged Twitter users to follow the account of a known ISIL member who had been trying to incite ISIL supporters to conduct attacks in the West.

Just hours before the attack, the same attacker posted a message on his Twitter feed indicating he had pledged allegiance to ISIL with the accompanying hashtag, Texas attack.

ISIL did not claim responsibility for directing or managing the attack, but ISIL operators praised the attackers and encouraged others to follow suit. The group also highlighted the attack in the most recent edition of its online magazine, which it publishes in several languages.

As we examine ISIL's broader efforts in social media, like any brand that seeks to target young people, ISIL continually innovates its online marketing to ensure it is developing effectively crafted messages. Using well known U.S.-based platforms such as YouTube, Facebook or Twitter, ISIL works to ensure its media releases reach audiences far and wide through reposting, regeneration of follow-on (ph) links, and translations into multiple languages.

ISIL also employs marketing tradecraft, attaching its messages to trending topics in order to gain additional readership. Consequently, its social media presence is more widespread than any other terrorist group.

Since the beginning of this year, ISIL has published more than 1,700 pieces of terrorist messaging. These include videos, pictorial reports and online magazines. These products are often very professional in their presentation and timely in their delivery, underscoring ISIL's commitment to master multiple social media tools in order to advance their extremist objectives.

As the Committee already knows, ISIL has often shaped its media content to amplify the effect of its violent operations and activities. They do so in an attempt to project an image of power and intimidation. They also employ a complementary approach to enhance recruitment, a projection of the self-described caliphate as an idealized family-friendly environment in which ideological, religious or personal fulfillment can be realized. This narrative has successfully induced large numbers of young people to make their way to the combat zones of Syria and Iraq.

During the past few months, ISIL social media operators have more aggressively pursued a new line of effort. Following statements from senior ISIL leaders encouraging lone-actor attacks against the West, these operators are now practicing online recruitment and provisioning of terrorist instruction intended to precipitate civilian attacks within the U.S. and other nations.

Sadly, as we have seen, some individuals have embraced the messaging and have sought to commit acts of violence on this basis.

When it comes to countering the spread of ISIL's violent messaging, several social media platforms have taken the initiative to close down accounts advocating terrorism and violent acts. They do this upon detection. However, energetic efforts to prohibit the propagation of violent messaging has not been universal. And there is still much work to be done to encourage greater vigilance and a broader sense of corporate responsibility to address this threat to public safety.

For our part, we are employing the knowledge that we have developed -- that has been developed by the U.S. counterterrorism community to refine and expand our prevention efforts. We've seen a steady proliferation of more proactive and more engaged community awareness initiatives across the United States, all working with the goal of giving communities information and tools they need to identify the threats posed by violent extremist online recruitment and to effectively engage it before it manifests in violence.

With our DHS colleagues, we have created and regularly deliver a community resilience exercise program, a tabletop exercise that brings together law enforcement and community leaders to run through a hypothetical scenario and potential responses.

In summary, we need multi-level partnership efforts to enable local U.S. communities to build the dual capabilities of addressing radicalization and ensuring resilient responses when an individual moves from radical ideology to radical violence.

We must continue to develop our knowledge of evolving terrorist online tactics, and we need to communicate that knowledge so that it can be used to minimize the application of terrorist online tactics against our citizens.

I'll stop there, Mr. Chairman. Thank you again for the opportunity to address the community.

MCCAUL: Thank you, Mr. Mulligan.

The chair now recognizes Undersecretary Taylor to testify.

TAYLOR: Chairman -- excuse me -- Chairman McCaul, Ranking Member Thompson, members of the Committee, thank you for the opportunity to appear with my colleagues to discuss the homegrown violent extremist threat to our country.

The terrorist threat today is more decentralized and complex. It is not constrained to one group, race, ethnicity, national origin, religion, or geographic location.

ISIL, Al Qaida and other like-minded terrorist organizations have expanded their efforts to recruit individuals for violent action at home and to continue to be effective -- and continue to be effective in recruiting foreign fighters from Western countries to travel to Syria and Iraq.

Core Al Qaida and its affiliates remain a major concern for DHS. The group and its affiliates maintain the intent, and in some cases, the capability to facilitate and conduct attacks against U.S. citizens and facilities. Their attack planning continues despite our persistent efforts to -- to disrupt them.

Through their sophisticated messaging capability, as Mr. Mulligan has mentioned, ISIL has been able to quickly reach a global audience and encourage acts of violence, inspiring U.S. citizens to travel to Syria, to recruit and radicalize to balance (ph) Western homegrown violent extremists here at home. This is concerning because mobilized lone offenders present law enforcement with limited opportunities for detection and to disrupt their plots.

The recent attack in Garland, Texas reinforced the importance of close collaboration and information sharing between DHS, the FBI, other federal, state, local and private sector partners.

Prior to the attack, the FBI and DHS shared with the Texas fusion center and local law enforcement warnings that the event was at risk of being targeted for violent extremism. These warnings led to the preparation taken by the Garland P.D. that helped thwart the attack.

Our top priority to counter this evolving threat is information and intelligence sharing with our partners. DHS, INA and the National Programs Protection Division field personnel are instrumental in this effort, and anticipate -- to anticipate potential terrorist actions and to propose protective security measures to help build resilience in our communities across the country.

As an example of close coordination intelligence sharing between DHS, INA and our state and local partners was the protests last week in Phoenix, Arizona this past weekend.

We proactively contacted our partners on the ground and shared intelligence from the FBI and DHS sources in real time to help ensure local leadership and law enforcement have the necessary information to protect their communities and their citizens.

Additionally, we reached out to the faith community in Phoenix to provide information regarding the potential violent activities so that they could take preventive actions in their communities.

It is important that we continue to build these partnerships with state and local enforcement in a way that enhanced community relationships and builds resilience to violent extremist recruitment.

DHS now has a senior executive, the DHS Coordinator for Countering Violent Extremism whose sole role is to coordinate and improve the Department's C.V. efforts.

The new DHS CVE strategy emphasizes the strength of local communities and the premise that well informed and well equipped families, communities and front-line personnel represent the best defense against violent extremism.

TAYLOR: DHS will continue to work with our international counterparts and our colleagues within the FBI, NCTC, the State Department and across CIC to identify potential threats to our security, both at home and abroad.

Chairman McCaul, Ranking Member Thompson and distinguished members of the committee, thank you for the opportunity to appear before you today and I look forward to your questions.

MCCAUL: Thank you -- thank you, Secretary Terry -- Taylor.

The chair now recognizes Assistant Director Steinbach.

STEINBACH: Good morning, Chairman McCaul, Ranking Member Thompson and members of the committee, thank you for the opportunity to appear before you today to discuss the recent terrorist influence, which transcends geographic boundaries like never before.

Terrorists' use of technology has aided in the dissemination of rhetoric encouraging attacks on U.S. interests in the homeland and abroad.

As the threat to harm Western interests evolves, we must adapt and confront the challenges. This includes working closely with our federal, state, local and international partners since the threat persists in all of our communities.

We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of ISIL and also those homegrown violent extremists who may aspire to attack the United States from within.

Conflicts in Syria and Iraq continue to entice Western-based extremists who wish in engage in violence. We estimate upwards of 200 Americans have traveled or attempted to travel to Syria to join extremist groups.

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. These threats remain among the highest priorities for the FBI and the intelligence community as a whole.

ISIL has proven relentless; through their skillfully crafted messaging, the group continues to attract like-minded extremists, including Westerners. Unlike other groups, ISIL has constructed a narrative that is appealing to individuals from many different walks of life. It is seen by many who click through the Internet every day, receive social media push notifications and participate in social networks.

In recent months, ISIL, via social media, has advocated for attacks against military personnel, law enforcement and intelligence community members. ISIL has gone so far as to post the names, addresses and photos of U.S. military personnel to the Internet, which quickly went viral.

We should also understand community and world events may entice an individual to act. As we've seen recently with highly publicized events, including the attack in Garland, the events will attract media attention and inspire copycat attacks.

The targeting of the Muhammad art exhibit and contest exemplifies the call to arms approach encouraged by ISIL, along with the power of viral messaging.

As I've stated in previous opportunities I've had to testify before this committee, there is no set profile for the consumer of this propaganda.

However, one trend continues to rise: the inspired youth. We've seen children and young adults drawing deeper into the ISIL narrative. These generations are often comfortable with virtual communication platforms, especially social media networks.

Some of these conversations occur in publicly accessed social media 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 equipped 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 the terrorists.

Social media is yet the latest tool exploited by terrorists. With its widespread distribution model and encrypted communications, it has afforded a free zone by which to recruit, radicalize, plot and plan.

We need to urgently assess the laws applicable in these matters and work with private industry toward technology solutions. To correct the narrative, this is not a conversation about national security at the expense of privacy or about weakening legitimate security of communication products through creation of technological back doors.

We are looking to be fully transparent with legal process showing evidence of a crime to gain access through the front door with full knowledge of those companies. The FBI seeks to ensure no one is above the law. So the bad guys can not walk away leaving victims in search of justice.

There is certainly a balance between security and privacy. We seek that proper balance and one in which security enhances liberty. The FBI in partnership with DHS and NCTC is utilizing all investigative techniques and methods to combat the threats these individuals 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.

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.

Chairman McCaul, Ranking Member Thompson and committee members, I thank you for the opportunity to testify concerning ISIL's persistent threat to the United States. I'm happy to answer any questions you may have.

MCCAUL: Thank you, Director Steinbach.

I now recognize myself for five minutes.

I want to first pull up on the screen what I consider to be an Internet conspiracy to conduct a terrorist attack. I was a federal prosecutor, worked on drug cases, organized crime; there are a lot of similarities.

But this one is conducted completely on the Internet. And let me first commend -- I want to commend the FBI, Homeland Security and the joint terrorism task forces for their textbook model case efforts in both the Garland attack and most recently in Boston. That's the way it's supposed to work.

Unfortunately, you have to get it right every time. And they just have to get it right once. But this kind of shows what we're dealing with, the threat gone viral.

You have this guy, Miskey (ph) the ISIS follower in Somalia, directing attacks against the cartoonist art competition, to Mr. Simpson, who responds. And as the attack is being conducted, we have the infamous Mr. Al Britani, who has become one of the chief ISIS recruiters, hackers, directors for terrorist attacks, congratulating them, basically saying that the knives have been sharpened; soon we will come to your streets with death and slaughter.

And I guess my first question is to Director Steinbach, this is just a microcosm of the conspiracy in the Internet we're looking at and the threat that we're looking at on the Internet.

How many potential recruiters do you think we have sitting in Syria and Somalia and Northern Africa, actively recruiting acts of terrorism globally?

STEINBACH: That's a good question, sir.

So I think you can refer to the Brookings Institute study on terrorist use of social media -- in particular, Twitter -- and gives you an idea of what we're dealing with.

So when you look at the volume of social media and its social -- and its ability to spread horizontally, you probably look at a -- in the neighborhood of a couple thousand core users, propagandists, that are pushing that message out.

And then probably in the neighborhood of 50,000, based on the study that's in open source, of individuals retweeting that message. And then again upwards of 200,000, say, for instance, receiving that message.

So that's our pool with which to start. And those are just, you know, ballpark numbers. So unfortunately, social media is a great tool for the public, but it also allows for this horizontal distribution, which is very difficult to follow. So those are baseline the numbers that we start with.

MCCAUL: Baseline, you start with. You said -- and it's been reported over as many as 200,000 pro-ISIS tweets per day occur on the Internet.

Is that correct?

STEINBACH: So I couldn't give you the exact numbers; it's a large volume.

And that's the trick, right?

What is somebody's individual right to tweet and say what they want to say versus somebody who is going down a different road, a more nefarious road/

So that's our starting point, is those thousands that you talk about and trying to cull through that and to find out who, amongst those individuals, are up to no good, who amongst those individuals are potentially plotting an attack on Western interests?

MCCAUL: And that is the great challenge that the FBI and Homeland has, is to try to, you know, monitor, to the extent you can, these communications.

STEINBACH: It's usually -- it's usually problematic. So the -- social media's great; it's out there. It's open source, but the volume is immense. And that, of course, I'm talking about the open side of social media. I'm not talking about the encrypted direct messaging, which is also a very problematic issue for us.

MCCAUL: And how many of those followers are actually in the United States in your estimate?

STEINBACH: So I think Director Comey stated it last -- there's hundreds, maybe thousands. It's a -- it's a challenge to get a full understanding of just how many of those passive followers are taking action.

MCCAUL: And I've read some of these Twitter accounts and tweets. They have thousands of followers and thousands following, which means they're actively communicating and pinging each other.

And then they go into, "Let's go into messaging." And then they go into a more secure space that if we have coverage, we can pick that communication. But, as you suggested in your testimony, then they have the ability to go into what's called "dark space," to another platform that is securecom that we don't have the ability to monitor these communications. Is that correct?

STEINBACH: That is correct, sir.

MCCAUL: To me, that's one of greatest concerns I have. Do we have any idea how many communications are taking place in the dark space?

STEINBACH: No, we don't. And that's the problem. We're past going dark in certain instances. We are dark. The ability to know what they're saying in these encrypted communication situations is troubling.

MCCAUL: I think it's a tremendous threat to the homeland. And do you have any recommendations for the Congress?

STEINBACH: I think we need to have an honest conversation, get past the rhetoric of what we're talking about. We're not talking about large-scale surveillance techniques. We're talking about going before the court, whether the criminal court or the national security court, with evidence, a burden of proof, probable cause, suggesting a crime has been committed or, in our case, that there's a terrorist. And showing that burden of proof, having the court sign off on it, and then going to those providers and requesting access to either that stored information or that communications that's ongoing.

And so, we're not looking at going through a back door or being nefarious. We're talking about going to the company and asking for their assistance. So, we suggest, and we are imploring, Congress to help us seek legal remedies towards that as well as asking the companies to provide technological solutions to help that.

We understand privacy. Privacy, above all other things, including safety and freedom from terrorism, is not where we want to go.

MCCAUL: Well, and I think this committee should be looking at this very important issue.

Finally, if you can comment on the most recent Boston case, it's been reported that this was a ISIS-inspired event over the Internet. And it took to behead police officers. We know that a lot of their commands and call to arms are to attack military installations and attack police officers. And I know it's an active investigation, but to the extent you can comment on this, would you please do so?

STEINBACH: The investigation's early on, post-event, so there's not a lot I could say on the intelligence side.

You're right, sir, we know that ISIL has put out a message to attack the West, specifically law enforcement, military. We know that they have been looking at those target sets. So we are very careful in where we're at.

The targets that are out there, the counterterrorism subjects, we are monitoring them very closely for any type of action, any type of overt steps, any mobilization factors. And when we see those, we're not taking the chance.

MCCAUL: I appreciate that. And we, again, commend your efforts in this most recent threat.

With that, the chair recognizes the ranking member.

THOMPSON: Thank you, Mr. Chairman.

Mr. Steinbach, you went into great detail, the challenge of social media and other things. Do you, at this point, see the challenge, also resources or the authority to do your job?

STEINBACH: I don't feel we have a challenge resourcewise. We've done an effective job, identifying, prioritizing and working through the JTTFs, the state, locals, to focus the target set.

And so, I would say that, of course, we always have to prioritize resources, but it's more so the challenge for me is the technological challenge, to get over that hurdle.

THOMPSON: When you say technological, is it -- just explain that a little bit for me, please.

STEINBACH: So, when a company, a communications company or a ISP or social media company elects to build in its software encryption, end (ph) encryption, and leaves no ability for even the company to access that, we don't have the means by which to see the content. When we intercept it, we intercept encrypted communications.

So that's the challenge. Working with those companies to build technological solutions to prevent encryption above all else.

THOMPSON: So there's nothing from a congressional standpoint authority you need from us to make that happen?

STEINBACH: Well, I think a number of years ago Congress passed CALEA, which was a law that was put in place that required telecommunication providers to provide assistance to law enforcement. I would suggest that that's a starting point, that we need to expand who is -- who is bound by that law, telecommunication providers is just a small subset of the companies that are out there that provide communication services these days. So I think as a starting point, that would be helpful.

THOMPSON: So, can you provide the committee with -- beyond the starting point -- in terms of where the department think we should be going in this -- in this direction?

STEINBACH: Sir, I could. I think more appropriately, the FBI's OTD, the Operational Technology Division, has the lead on that. And they could -- I'm sure they'd be happy to come here and kind of lay out for you step by step where they need to go.

THOMPSON: I think, Mr. Chairman, we ought to try to make that part of what we do.

MCCAUL: I agree.]

THOMPSON: OK.

Mr. Mulligan, according to your testimony, videos, tweets and messages are probably not enough to radicalize individuals who are beginning to show these tendencies. They serve as discussion points.

Showing interest and having online discussions are not criminal in nature. So what do we do about all of these online portals that kind of start this -- people down this slope, so to speak?

MULLIGAN: Sir, as my colleague mentioned, so it is part of a dialogue. They start out by trying to gain your interest. It's marketing and advertising. And as Michael indicated, a lot of it is there's followers.

And, you know, as you frequently start out as following someone, and following the trail, or you're subscribing to one of their channels, and then it progresses beyond that into a dialogue.

So what we really need to be doing is helping educate a lot of the members of the public about this process. And we've been trying to do that with DHS so that, like, as Michael also said, family members are aware that if their children are spending a lot of time on this, they need to be able to counter that. They need to be able to execute some degree of measures.

These individuals are very savvy in their understanding of the gradual nature of recruitment and operationalization. And so, what they try to do is create a series of images that are attractive and then they try and broaden that into a further discussion. I

So it does require, again, a much more active, interventionist approach.

THOMPSON: General Taylor, can you kind of tell us where the DHS fits in this space, in terms of trying to do the community engagement and some other kinds of things that can help what Mr. Mulligan is talking about?

TAYLOR: Yes, sir, certainly. As my colleagues on both sides had mentioned, it starts with the intelligence to understand the tactics, techniques and procedures that our adversaries are using to reach into our communities.

And we go out with NCTC, with the FBI, with the Department of Justice, to conduct community resilience exercises, to teach communities about the tactics, techniques and procedures, what to look for, how to spot it, who to -- whom they may report to about that activity, so that they can intervene at the earliest possible stage.

And we've done that across the country. Secretary Johnson has done six of them so far this year. He's actually out, doing one this afternoon. It is a clear part of our strategy to ensure that communities understand this threat and how it's being manifested.

And, in my mind, it's almost like what we do with predatory behavior, with child molesters and that. We've got to inform parents of what is happening on the Internet so that they can go and monitor what their children are doing and seeing on a continuous basis.

THOMPSON: Last question: Do parents who are monitoring, do they have enough options out there? You know, I think if a parent suspects that my child might be engaged in this behavior, you know, if -- who do I call? Do I call the local law enforcement? Do I call the FBI? Or have I really put my child in a situation where I'm labeling that child for life?

Do we have anything in between law enforcement and -- and a parent that can help mitigate some of these circumstances?

TAYLOR: Well, certainly, I think the opportunity is to -- for the community to engage, for the schools to engage before it gets to a radical action that requires law enforcement involvement.

So what we try to get communities to understand is that they are part of the solution and it's not just a law enforcement solution that we're looking. We're looking for communities to be engaged, to understand and to intervene when these events occur.

There was a recent case we had where a father in New England -- his -- his daughter went missing, and he went to the airport in his state and said, "I think my daughter's leaving."

And we were able to find his daughter. She wasn't at that airport; she was at another airport before she got on a plane to go to -- overseas.

That happens almost everyday with somebody having that sort of challenge, and it's not a law enforcement response; it's helping parents be good parents and helping their children not make bad mistakes.

THOMPSON: Thank you, Mr. Chairman. Yield back.

MCCAUL: Mr. King is recognized.

KING: Thank you, Mr. Chairman.

Let me thank all of the witnesses for the testimony today and for the tremendous service they've given our country. Thank you very much.

I'd like to expand on something or maybe slightly disagree with something the ranking member said, and maybe it's more for the point of clarification about whether or not ISIS' use of the social media can, by itself, cause someone to carry out violent action.

I know many cases may be part of a long process, but we had two recent cases in New York where there was a man in Jamaica, Queens who attacked two police officers with a hatchet. It doesn't appear as if there was a long process of radicalization there; he was responding to a -- in effect, a director from ISIS.

And then we had two women -- now, this may -- somewhat longer process -- also in Queens, with IEDs in their apartment. And they both seemed to -- primarily, their means of radicalization was the ISIS use of social media.

Am I correct in that or -- I'm not trying to disagree with the ranking member; I just wanted to add onto that.

MULLIGAN: I would suggest, Congressman, that you are absolutely correct in their -- in their -- they believe they are able to operationalize people solely through social media. They believe that they can enter into the dialogue I referred to earlier and provide the tools, and they're not getting into very complex tools.

What they're telling them is, "Here are tactics and procedures you should use. Here is some easily available, readily available information online that you can exploit."

In other words, they believe that they can provide them everything that they will need to undertake some kind of lone actor attack.

STEINBACH: Let me add to that, sir.

So I think you -- you also hit on an important point, and that's the diversity of the threat. You've got a slow burn, but you also have individuals who are flash to bang, which is very quick. We've seen more of this flash to bank with ISIL and their online efforts.

Again, it's not just going some place on the Internet and looking it up; the social-media push is coming right to your -- your pocket via your smartphone; there's it's a diversity of threat.

So you're right in that it all depends on the individual. But we have to be prepared for both types of situations.

KING: I think you were very, all of you, eloquent as far as some of the dark areas where you just can't go right now. And it would seem to me that, in those instances, it's more important to have human sources on the ground that can fill in those gaps.

I would just say -- maybe this is rhetorical on my part, but with the constant criticism of law enforcement and the constant talk of snooping and spying, for instance, to me, it makes it harder to recruit people on the ground.

Like in Boston, if this had been two days ago and the Associated Press, New York times uncovered the fact that the Boston police were following those alleged terrorists, that would have been snooping and spying. Well, now it turns out after the fact it was effective surveillance.

And I just think that the use of those terms really are doing a tremendous disservice as far as enabling law enforcement to recruit people on the ground. You said you wanted to work with the community, and you do. But at the same time, this onslaught coming from the media and from certain people in politics constantly talking about snooping, spying, harassment, to me, undoes a lot of the good that you're trying to do.

So I don't know if you want to comment or not. Again, maybe I was just making a rhetorical point. But if anyone wishes to comment, fine. If not, I'll just...

STEINBACH: I agree with you, sir. You have to have a multitude of tripwires, both online and in person. And we try to insert sources in situations where there's a predicated investigation, but it's a challenge.

KING: Thank you.

TAYLOR: Sir, I would add to what Mr. Steinbach had said and indicate that this is a total team fight. It takes (inaudible). It takes (inaudible). It takes what I call transaction and looking at travel patterns and those sort of things to -- to come to this.

And certainly, in communities, communities sometimes feel, well, you're looking at us too much as opposed to another community, and our response is generally, "The bad guys are trying to recruit your kids. That's why we're talking to you. It's not because of your religion, but it's what the bad guys are try doing, and that's why we're here talking to you about strategies to defend yourself."

KING: My time is running out. Just -- if you can comment on this.

ISIS, one thing they have been doing, it appears, is encouraging use of hoax threats. Are you in a position to say yet whether (inaudible) what happened on Memorial Day, where there was going to be 10 different hoax threats were called in to the airlines and again this weekend when they were called in, if that is any response to ISIS, are these lone wolves, or is it just a person carrying out a hoax?

STEINBACH: So I would say we don't have any credibility information that there are threats to aviation right now. So yes, the ones so far appear to be hoaxes. Tracking those back to an individual or group is still an ongoing process.

KING: But ISIS has said that the use of the hoax itself is an effective means of attack.

STEINBACH: Correct.

KING: Thank you.

I yield back. Thank you, Mr. Chairman. Thank you for your testimony.

MCCAUL: Mr. Richmond's recognized.

RICHMOND: And I guess I'll start with Mr. Taylor or maybe even Mr. Mulligan.

You mentioned that there were about 1,700 messages sent out by ISIL. How many -- if you had to estimate, about how many people did that reach?

MULLIGAN: Certainly tens of thousands. 1,700 separate publications, be it a video release or an online magazine release but certainly in the thousands to tens of thousands.

RICHMOND: And the people who start to follow and engage in the social media, even if it's on the front, we're not seeing any similarities or any consistent traits across the board in the people that start to engage, or are we?

MULLIGAN: Well, sir, it's partly about what the actual publication is or the video is about or what they're trying to incite.

In some instances, as you know, we're particularly concerned when we see someone who is -- let's say a Twitter feed that's being followed and they are really strongly advocating violence, then I think the FBI is paying particular attention to those.

It's important to also note that in some instances, a lot of the followers are just -- I mean, they're paying attention. The media's paying attention to some entities on a lot of video releases. Obviously, they're tracking and reporting on it.

And I would also like to posit that in many instances, they're also trying to generate buzz themselves. So we've seen multiple instances in which they have, if you will, collaborators who will retweet messages to try to in crease the numbers so that it makes it look like they've got a yes very large number of followers.

The bottom line is they're effective at using social media and they're effective at, if you will, manipulating social media.

RICHMOND: Well, knowing that they're experts at manipulating social media and using social media, are there things that we can do or things that we should encourage others to do or not to do to protect themselves?

And I guess now, I'm going to get into the sensitive area of -- you know, I'm not commenting (ph) whether it's their First Amendment right to have a contest to depict or make fun of Islam, but in my mind, I encourage my mother not to walk down dark streets at night, because it's dangerous. I would get upset if someone drew cartoons of Jesus or called Mary a slut. I mean, that's just my faith.

RICHMOND: So if you know they're social-media experts and they're good at using social media to get their message out, are we inciting some of this with our -- or some people's hatred towards their religion and other things? I mean, are we fueling some of this fire?

TAYLOR: Sir, I think I would answer that question simply by saying, the Constitution of the United States of America and our rights and freedoms are something that stands in the way of our enemies' effort to create a global caliphate.

So I don't think any one event fuels this. I think it's coming at our system of government, our freedoms, is what they're trying to undermine. They are in the news cycle.

RICHMOND: So, you don't see any spike in people following after events look this or any rise in social media conversations when you have a contest like that going on?

TAYLOR: Of course you do. But...

RICHMOND: Well, I guess that's my question, then.

TAYLOR: But again, in America, those kinds of conversations happen every day as a -- as a part of our constitutional rights in this country. And so, saying that we should stop doing something here would cause them to stop doing it there, they'll find somewhere else to look for a reason to, you know, to attack America.

RICHMOND: No, and I agree with that.

But I guess my question is, and I think that a guy that's gonna rob a lady walking down a dark alley is gonna rob somebody, but I'm gonna encourage my mother not to walk down that alley so it won't be her, so that it's not easy prey.

And I -- and I guess, you know, it's our constitutional right to say whatever you want, but I promise you, if you call my mother a bad name, there are going to be some consequences and repercussions. And I just don't think that we're having that honest conversation when we're talking about young people, we're talking about angry people, we're talking about people who feel picked on

If you -- I mean if, you know, there are some words that will trigger a response, but you have the absolute First Amendment right to say it. And then it's up to me whether I want to exercise my discipline or hit you in the mouth.

So, the question becomes, how often are we gonna get hit in the mouth before we realize that we may be playing into it unnecessarily by just being callus and cruel, I think, in some instances.

So thank you for your questions.

And thank you, Mr. Chairman.

MCCAUL: I thank the gentleman.

Mr. Perry's recognized.

PERRY: Thank you, Mr. Chairman.

And thank you, gentlemen, for being here. This is a -- I think this is a difficult subject trying to find the line between privacy and security, as we've found out and I think everybody's alluded to.

Let me ask you this. There are folks that might wear their heart on their sleeve regarding this circumstance, radical Islam, attacks and so on and so forth, and they might be having a conversation openly on the -- on social media where they espouse their opinions, which might lead them to be a target for some of these individuals, if you know what I mean, and maybe even

some of the folks in the building, that -- somebody that has a -- somebody that's having this hearing today or somebody that's asking questions like this.

Do you folks have any way or do the platforms have any way of monitoring traffic about those individuals that might have had a conversation with a friend, openly on open source, online, about their disdain for radical Islam, for attacks, and might have been disparaging about it, or, you know, did they become a target? Does that individual become a target? Is there any way that the social platforms have a way of monitoring it? Do any of you folks have a way of monitoring it. Do you collaborate on that? And is that a -- is that a chill, is there a chilling effect for free speech if people feel like they might be targeted because of their thoughts posted openly on social media?

STEINBACH: So I'm not sure that I fully understand the question. So I think that social media platforms usually abide by the terms of service agreement. They've got small compliance departments. So, for the most part, the answer to the first part, no, I don't think social media companies are doing anything along the lines that you speak.

As far as the intelligence community or law enforcement, monitoring those individuals who are exercising expressions of freedom and then become targets, we don't have a mechanism in place to track them. We would track it from the other side, is if we see threats coming toward them but not necessarily -- is that the question you're asking, sir?

PERRY: Essentially, yes. (inaudible)

STEINBACH: We are not tracking it from the other end. Now, if somebody comes to us and says, hey, I feel threatened, of course we will look into that. But, as far as a data pool of some type of large scale to look at that, no.

PERRY: Are there -- is there -- go ahead.

MULLIGAN: If I could offer another bit of context to what Mike said. When you're operating on social media, particularly some of the broadly available public platforms, you're in open space. So you can be monitored by any entity out there, by commercial entities, by educational institutions, by the media, anyone can be looking at that.

That's one of the challenges that I think people are often concerned about, going back to this point that you made. Frequently, within this country, we are trying to -- I mean, trying to encourage credible voices to contest the ideological extremism that is being advocated, and those folks are often reluctant to do so because they're concerned that they will either, as you said, become a potential target of violence, become an intelligence target, become a law enforcement target.

And I think what we've been trying to do collectively as a community is trying to change that environment, at least from the perception of the U.S. government's monitoring of their activities.

But I do believe that, again, it is open space, so any person that enters into that space needs to understand that.

PERRY: So, when you talk about -- several of you talked about encrypted direct messages and dark space, can you give me some examples, is it essentially just texting, would that be considered off-limits to monitoring by the United States government, even in cases where there might be an imminent planning and plotting?

Is there any way -- and if this is classified, that's fine, too, but I'm just wondering from that perspective, you know, if it's not on Facebook, if it's not on Twitter, do we have the capability, other -- the federal -- the federal government, do they have the capability and/or do the providers have the capability, and are there algorithms that pick this type of stuff up, or processes that pick this stuff up ?

STEINBACH: The answer is no. There are -- there are 200-plus social media companies. Some of these companies build their business model around end-to-end encryption. There is no ability currently for us to see that. So, if we intercept the communication, all we see is encrypted communication.

PERRY: Anybody else? Some examples? Are we talking just straight texting? Like I know of a program called Cyber Dust, right? So, once you send it and it's received, it disappears. And that would be -- is that an example of the dark space, or is that just encrypted direct communications? What that is?

STEINBACH: So dark space is a general term. So, yes, there's lots of models out there. There's models, social media that go point to point, and then, once you read it, it disappears, it's not saved.

Some companies can set -- you can set how long a text is saved. Some of them are encrypted from the start. Most of them are text-type direct forms, some of them are photographs that send. There's all kinds of different models. And it's just a -- some of them are more like bulletin board formats. There's lots and lots of formats out there.

PERRY: And all of that is off-limits right now with the federal government as far as -- as far as you're...

STEINBACH: It's not that it's off-limits. It's there are more and more of these companies are building their platforms that don't allow us. We will still seek to go to those companies and serve them legal process, but if the company's built a model that even they can't decrypt, then it doesn't do us any good.

PERRY: Thank you, Mr. Chairman. I yield back.

MCCAUL: Ms. Watson Coleman's recognized.

WATSON COLEMAN: Thank you very much, Mr. Chairman.

And thank you very much, gentlemen, for your information sharing here.

I think I want to tag on a little bit to Congressman Richmond's questions, because I want to get at something that I've not heard a lot about.

I'm reading that there really is no sort of common denominator here, not any religious zealot. Individuals who are being radicalized don't even necessarily know what the Islam religion is all about.

It's not socioeconomic, it's not racial or ethnic, so I'm trying to figure out what exactly is it. What is enticing about beheadings and violence and this just very angry assault that our young people are being exposed to? What is tripping them and their attention to that -- to that kind of radicalization? What is it about ISIL?

MULLIGAN: So, ma'am, if I can just give you a little bit of context on that. You're right to describe, and I think one of my colleagues described earlier, the range of, how can I say it, experiences and, if you will, ideological knowledge, religious knowledge varies incredibly widely.

What there seems to be is, they are appealing in some instances to -- if there is a sense of victimization -- that they are the individuals who are -- those who, you know, will conquer those who have been the victimizers. And so it appeals to that -- to that underdog nature. They really do an effective job in communicating that sense.

And as I said in my remarks, they couple that with an ability to present "Here is the idealized vision of what our religion presents. And if you really want to leave the trappings of all the challenges and troubles you're having in your current life and join us, we will offer you more direction and more means." And so that is how they seem to be succeeding.

COLEMAN: So they seem to be attracting young people. Are we talking about middle school age? Are we talking -- what ages are we talking about? When we say "youth," just how young are these people -- young people being (ph)?

MULLIGAN: I would say any -- I would say we are seeing ages in the teens, probably upper teens into twenties. And it's also important -- you know, we've deemed this a new generation of terrorists because as -- as General Taylor was saying, a lot of them are extremely conversant in a lot of social media. I mean, they've grown up with it.

COLEMAN: Yes.

MULLIGAN: So this is the means by which they use to reach that generation.

COLEMAN: I can understand that. What I don't understand is what is enticing them. I mean, what -- what -- what appeals to you when you see someone beheaded, or you see these nasty threats, or you see this -- this violence? The victimization is something I'd like to just carry on a little bit.

I don't -- one of my favorite programs was about the FBI profiler. And so I'm wondering, is -- was that a real thing? I know that there's police profiling I've got to be concerned about. But do we -- is there such a thing as psychological profiling? Are we looking at those kinds of things? Are we identifying some traits that have nothing to do with ethnicity or socio-economic, or whatever, but other traits? And are we able to, like, identify any sort of red flags in the -- in the children and the young people in school and in college? Because I just wonder whether or not we're expending enough energy and resources in trying to identify early on in intervening.

STEINBACH: So, yes, the FBI does have a behavioral analysis unit. And there is a -- within the National Center for the Analysis of Violent Crime, there is a unit dedicated to terrorists. And it spends a lot of time looking at the parts of radicalization and mobilization. What attracts folks. But like Mr. Mulligan said, it's a very complicated piece. And, quite frankly, what we've seen as far as a profile is the lack of a profile. There's just so many reasons. You know, we don't -- we don't see disaffected, we see some disaffected. We don't see well-to-do, we see some well-to-do. Victimization is certainly a common theme. Younger and younger individuals are drawn into this messaging.

I would say that ISIL has done an effective message versus Al Qaida, and that they have said publicly, "Hey, the caliphate is here today. You can come now to a -- a country where Sharia law rules. Bring your family." And they've really messaged it across a spectrum through -- to a wide walk of individuals.

COLEMAN: Let me just ask this last question, if I might. Should we be engaging the Department of Education -- higher education -- in identifying programs and approaches and sort of learning devices that would be able to anticipate and deal with our younger people who are affected by whatever it is that's turning them on here?

Thank you.

TAYLOR: Yes, ma'am, we should, and we are beginning to work with the Department of Education on these kinds of issues. Because it's a whole of community effort. It's not just the police, not just the churches, but it's education. It's civic organizations, as well.

COLEMAN: Thank you, Mr. Chairman. At some point, I really would like for us to explore what more can be done proactively in identifying and sort of intervening at earlier stage.

Thank you for your indulgence.

MCCAUL: Thank you.

Mr. Hurd's recognized.

HURD: Thank you, Mr. Chairman and Ranking Member for holding this -- this hearing. I think a number of these issues -- we can talk all day long about that. And so we're packing a lot in in a very short period of time. And my first question is to Mr. Mulligan and Ambassador Taylor.

You know, talk about the community engagement exercises and engaging credible voices throughout these communities. How do we blow that up? How do we -- how do we make it bigger? How do we -- how do we accelerate those projects?

MULLIGAN: So we've been developing a partnership community awareness briefing. And we've just been moving it out fairly slowly initially to ensure that we're having a degree of success. But we have had some success in that. And now we're trying to train the trainer so that we can get into a situation where we're propagating it more broadly across the communities. Because, going back to some of the other observations that have been made, it really is at the community level that we need to have this success. And also, we need to have, I think as the ranking member said, levels between government and local. In a lot of instances, particularly with family members, as you know, people are reluctant to engage any sort of authorities, and we need to try and find that middle ground.

HURD: And I appreciate that, because we need to be thinking about this in terms of weeks, not years. Because that's -- that's the speed at which we need to counter this -- this threat.

Ambassador Taylor, do you have any remarks for that?

TAYLOR: I -- and it's a global phenomenon.

HURD: Mm-hmm.

TAYLOR: So our outreach internationally has been important, as well. I'm leading a delegation to Australia next week to further our communication with our FBI's (ph) partners about this phenomenon and how we can engage communities really across the world to better -- so that they better understand what this risk and threat are.

HURD: Yeah. Because in order to make the FBI's job a lot easier, this lone wolf idea -- the way we're going to stop that is by countering that violent, you know, ideology and extremist ideology. And -- and that's going to take a whole of government effort. Who in the government is responsible for this? The CVE activity?

TAYLOR: Well, it's actually a shared responsibility between Justice, the intelligence community, DHS and the FBI. And our deputies meet regularly to formulate those strategies and to implement those strategies within the -- within the U.S.

HURD: My suggestion there would be looking at unity of commands. Because when you have three people in charge of something, nobody's in charge of it. I think that's something that we're plagued with in the federal government on a number of occasions.

And my next set of questions is to Mr. -- Mr. Steinbach.

The cannon out there on counterterrorism is clear. Terrorists are trying to do two things. They're trying to kill a lot of people and they're trying to elicit counterterrorism responses in a government to upset a population to foment discord, all right? And so with that as -- as the

background -- that's why I'm a little bit nervous when we -- when we start talking about CALEA expansion and all these kinds of things, I get nervous because of the privacy aspect.

So my question -- and not to get too technical -- does end-to-end encryption that's provided by many U.S. companies prevent your ability to do attribution?

STEINBACH: In some cases, yes.

HURD: But not in all cases?

STEINBACH: Not in all cases.

HURD: All right. So are you suggesting that when you have a court order on someone connected to terrorism, that there are companies that aren't cooperating with helping to -- to get as much information as they can about that individual?

STEINBACH: No, what I'm suggesting is, the companies have built a product that doesn't allow them to help.

HURD: But if you're saying it doesn't prevent attribution and -- because the key here is to try to find as much information so that you can -- you know, to exhibit the success that you all had in Boston. You know, you were able to identify someone and use other tools to track him in order -- and, you know -- and stop -- and prevent this from happening. And that's -- you know, it's a difficult task. Don't get me wrong. I know how hard you guys are working. Maintaining the operational pace that you all have maintained since September 11th is unprecedented. And your -- the men and women in the FBI should be patted on the back and heralded. But we also got to make sure that we're protecting our civil liberties and our borders at the same time.

And when you talk about reviewing applicable laws around the technology -- the technology challenges that you are facing in CALEA expansion, I just want to be clear. You're not talking about putting a back door in software, are you?

STEINBACH: No. Like I said in my prepared statements, we are (ph) talking about full transparency. I'm talking about going to the companies who then could help us get the unencrypted information. And the attribution piece -- it's important to understand that, depending on the technology involved, this -- and this requires, quite frankly, a technology discussion -- there are tokens that are used that do not allow for attribution. So it's not quite as simple as just using other techniques or attribution. Sometimes that attribution is not there.

And I'd be happy to discuss in a classified setting in more detail just exactly what we're talking about.

HURD: I would love that. And thank you.

And one of the things -- we've been talking a lot about the use of social media and digital tools and how it's made it easier for ISIS to recruit people. But it also gives us an opportunity to do double- agent operations against them to penetrate, you know, their ability.

When chasing Al Qaida, you know, 10 years ago, if you were anything close to an American, you would have got your throat slit. Now we have these new tools in order to penetrate them.

And, again, I know -- I've run out of time, and I yield back that to the chairman.

HURD: Thank you.

MCCAUL: If I could just briefly -- we led a delegation on investigating foreign fighters to the Middle East and Europe, and we found that there is a counter-narrative out there. This is more not online, but foreign fighters who have left the region. Some return inspired and more radicalized, and some return very disillusioned from the experience.

And I think that narrative, and this may be more of a State Department issue, the more we can get that narrative out there, the better off we're going to be.

So, the chair recognizes Ms. Rice.

RICE: Thank you, Mr. Chairman.

Mr. Steinbach, I just want to ask you a couple of questions. How does the intelligence community qualify an elevated threat from online-inspired terrorists? So, you know, we all know how that -- you know, when they raise the threat level. But specifically with this online communications, how do you rate what the -- what level the communication, how it rises to something that you really are worried about?

STEINBACH: So, it's a I think a simple question with a complicated answer. There's lots of pieces -- the volume, the specificity, whether or not they've identified willing sympathizers who will do something. It's a lot of pieces that go into it. And many of those factors are present now.

RICE: So, are there any difficulty -- what's the biggest difficulty in terms of being accurate when you are trying to rate the level of a threat?

STEINBACH: So, as Mr. Hurd stated previously, the social media is great because it's out there -- social media -- it's voluminous, but it's volume. So, there is -- trying to week through the thousands and thousands of individuals on social media and find the -- all the signals out -- all the noise out there identifying the signal. So it's a volume piece. You know, looking at social media requires a different business process that we do things with in -- in going from there to finding a credible threat.

It's -- it's a very difficult process.

RICE: Yeah, I mean, it seems like it would be.

We've been talking this whole time about online communications, online radicalization. Is there any physical presence of either ISIL or Al Qaida doing face-to-face recruiting here in this country?

STEINBACH: So, I would say we don't -- we have, of course, a number -- a small number of returned foreign fighters. We have individuals who have been overseas and returned to the U.S. Where they are and who they are is probably an intelligence (inaudible). I would say our best estimates are we don't have ISIL sitting in the United States. We've got individuals who have taken up the call to arms based on ISIL's messaging.

RICE: Yeah, but not everyone who has gone and come back becomes a recruiter. So I'm just curious as to whether there are people who don't go anywhere, aren't on the Internet, and are actually in physical -- a physical place actually doing, you know, whether in tandem with the online recruitment, actual face-to-face recruiting.

STEINBACH: So, you're trying -- you're talking about a classical home-grown violent extremist -- the lone wolf. There are a number of factors that would cause somebody to radicalize. It doesn't have to be online. It could be a friend, an associate. Other factors may cause that person to become radicalized. Online just happens to be when you look at the spectrum, the -- by volume, the highest percentage.

RICE: OK.

STEINBACH: If you're asking, do we have core Al Qaida coming to the U.S. and sitting here, or core ISIL, I think we look to that -- look at that intelligence gap all the time. But I would say for the most part, no.

RICE: OK. Thank you.

I yield back my time. Thank you, Mr. Chairman.

MCCAUL: Mr. Duncan is recognized.

DUNCAN: Thank you, Mr. Chairman.

Al Qaida led the way with Inspire magazine, I think, which was an online publication. Are we still seeing Inspire as prevalent as it was? Has ISIL adopted that -- that media? And is there a way to track? You know, if you've got a website platform like Inspire, is there a way for you guys to track who visits that page? You know, who -- who takes it and forwards that information? If you could answer that for me.

MULLIGAN: Sir, to answer your question, Inspire still comes out periodically. It has been -- that model has been successfully copied by another -- by several of the other affiliates and other terrorist- related entities. They see that whole process of like an online magazine as being an effective model.

It's been -- it's been adapted by ISIL. They have a publication called The Beak (ph). It is a variation on that. They put out their information. They put it out in multiple languages.

To answer your question about our ability to track its propagation, it's not -- we're not really able to do that. They put multiple links to it. It appears -- I mean, as you can imagine, once something starts to propagate on the Internet, it's there. It can be -- it can reside in a number of places.

So, that model does exist. It continues. They're continuing to employ it. And again, it's extremely difficult -- impossible to track.

DUNCAN: For the freshmen members and people that have just started following this issue, I'd recommend you get the Inspire magazine; take a look at what some of the information that's being provided. I've never seen the information you're talking about at ISIL or others. If there's a way to share that with the committee, even if it's a classified setting, we're glad to take a look at that. Personally, I'd like to do that.

I'm very interested in the foreign fighter flow. I went last year to Europe to really delve into these foreign fighters coming off the battlefield from Syria, whether they transited through Turkey. And when I was there, or right before I got to Brussels, a foreign fighter actually came back, shot up the museum there -- the Jewish Museum; killed three or four people, and tried to flee to North Africa through France.

And so, the timeliness of my travels, but this was the very beginning. You didn't hear about ISIS as much in May and June of last year, not like you hear about them now and at least over the last 12 months.

At the time, that foreign fighter that shot up the museum in Brussels, Germany knew, apparently knew about it, and failed to let the Belgians know or the French know because they were suspicious of U.S. intelligence gathering through monitoring phone calls and all that's come out after Snowden.

So, what are some of the challenges of tracking these foreign fighters? You talk about core Al Qaida and core ISIL. I'm talking about the fringe guys that go over and get -- maybe get radicalized on the battlefield and decide, "You know what? I can do this back home."

How do we track those guys? And how successful have we been?

MULLIGAN: So, that's been -- ironically, that's been an incredibly unifying factor among the counterterrorism community across the globe. A lot of our Western partners, so, I mean, they've got substantial foreign fighter flow issues. You know, as Mike indicated, ours are about...

DUNCAN: I mean, Schengen region in Europe. I mean, it's -- you get there...

MULLIGAN: Yes, sir. And that's, again, something that they're trying to confront in Europe with regard to how do they manage this with the Schengen flows right now. We have been sharing a

lot of information back and forth with some of the means and processes that we're trying to employ to track foreign fighters.

What's also very clear to us is it needs to be, particularly with -- with our foreign partners, a whole-of-government approach. We're trying to share with them the benefits that we have experienced by ensuring that the free flow of information among the interagency. In many instances, we'll develop an effective relationship with a foreign partner, only to discover that the partner flow within their own nation is not optimized to try and ensure that appropriate law enforcement authorities have been alerted to that foreign fighter flow.

DUNCAN: Right.

MULLIGAN: But the bottom line is things are trending positively in the information sharing.

DUNCAN: In the bilateral trade...

MULLIGAN: Multilateral -- multilateral, sir.

(CROSSTALK)

MULLIGAN: But the -- but the other challenges, again, so we estimate there have been about 4,000 in total foreign fighters flowing from the West. But what we've seen is, again, there are foreign fighters from over 100 countries. And some of our other partners closer in that region have developed very effective mechanisms for both tracking the foreign fighters and developing rehabilitation programs.

So going back to some points that the gentlemen made earlier, we really need to do a lot of information sharing about their experiences at rehabilitation, their experiences at tracking, and incorporating them into some of our own processes.

DUNCAN: In the interests of time, North Africans are trying to get across the Med into Italy and Spain. And once they do, they've got pretty much free travel throughout Europe. So, how do you target those? I mean, these are migrants that are getting on boats and coming across. We don't know about them.

MULLIGAN: Interestingly, some of the direction that's been given lately by -- lately -- you know, over the last several months -- by ISIL leadership is they're urging a lot of these fighters to remain in place. To -- as you know, they've been trying to establish branches of the caliphate in other countries. And so they are trying to say, "Hey, don't move -- you don't need to move across North Africa; stay in Libya and work with our branch there."

So, that is one other part of their strategy. That's how they're trying to offset that limitation.

TAYLOR: Sir, if I might add, we are working very closely with our European partners on that flow from Italy and into the northern parts of Europe. It is a very big concern for us, not only

from a counterterrorism perspective, because eventually some of these people might end up applying for visas in our country.

So it is a high priority for our intelligence exchanges with our partners in Europe in terms of getting our arms around that particular flow.

DUNCAN: All right. Well, thank you. I'm out of time.

Mr. Chairman, I would ask that we delve into the effectiveness of JTTFs with regard to some of this, and that might have to be in a classified setting. But I yield back.

MCCAUL: Yes. And let me just say for the benefit of the members, we do have classified briefs with FBI and Homeland, and social media monitoring and on encryption challenges. JTTFs would be right.

The other flaw I noticed in my travels is that European partners don't screen E.U. citizens past any watch list as they fly from, say, Istanbul back into Europe, and I think that's a big security gap. And we urge them to change that. I know the E.U. parliament is addressing a change in their law.

TAYLOR: It's in work. It's not moving as fast as we would like it to move. But there are some glimmers of hope that, based upon the recent activity threats and actions in Europe, that the Europeans understand the importance of PNR and other sorts of data tracking of citizens internal to the E.U. So we have some hope that there will be a light at the end of the tunnel going forward on that.

MCCAUL: Yes. I did, as well.

Mr. Langevin.

LANGEVIN: Thank you, Mr. Chairman.

I want to thank our panel for the testimony here today. And I apologize if any of the questions I'm going to touch on have already been asked. I had to leave briefly to take a call from our commanding general in Afghanistan to get an update and a briefing from current status of things over there, in my Armed Services Committee role.

If I could on -- begin with this, as some of you may know, I spent a lot of time and are very concerned about cyber security issues particularly as they relate to critical infrastructure.

Can you tell me, in your role and with respect to seeing this stepped-up effort in using social media, in recruitment and using cyber as a tool, what you're seeing in terms of recruitment or efforts to use cyber weapons to attract -- to attack critical infrastructure?

And can you also describe what measures, if any, that are also different when combating the threat of a homegrown terrorist interested in cyber terrorism rather than more traditional physical attacks?

STEINBACH: So I think it's a great question. I think, first of all, we're seeing more and more a blended threat, the cyber intrusion piece with the counterterrorism piece.

Where we're at now, we do see those same counterterrorist actors -- or terrorist actors, using cyber intrusion as a tool. And they're experimenting with it, seeing how effective they are. We've seen most recently in the last -- less than a year, them becoming more and more adept at cyber intrusion type activities.

TAYLOR: And, sir, I would add to Mr. Steinbach's comments by saying that this is a very high priority concern for the Department of Homeland Security, our national programs and protection division work with the critical infrastructure community every day across this country about the cyber threat in general and specifically about the threat from terrorist actors so that they are prepared for and understand the potential for that threat and have means of mitigating those sorts of attempts within our critical infrastructure.

LANGEVIN: Mr. Mulligan, do you have anything to add?

MULLIGAN: Yes, sir. I mean, I would agree with those points. I would also posit again, it seems that it is inevitable kind of trend they would move into that realm. They would move into that realm because, again, it is a means by which they could effect damage in a very cost-efficient way.

And they are operating largely -- they have a high degree of maneuverability in cyber space. So it seems quite logical that they would attempt to pursue that and we need to be developing mechanisms for detection of those activities, sir.

LANGEVIN: OK.

Have you seen those stepped-up efforts to specifically focus on that as a -- as a tool right now to be used to go operational?

MULLIGAN: Yes, we have seen stepped up efforts.

LANGEVIN: OK. Thank you.

Mr. Mulligan, if I could turn to you, I'm very supportive of efforts to incorporate countermeasuring into CVE strategies and the use of public-private partnerships, such as the peer-to-peer program that you mentioned in your testimony to ensure that these messages are heard.

At the same time, central to any effective countermessaging strategy, though, is the -- is the credibility of the messenger, which can be greatly undermined if government is involved.

So how can we assure that there are independent voices that can counter extremists' messages without compromising the independence that gives their statements weight?

MULLIGAN: Sir, that's exactly some of the outreach efforts that we're trying to make with regard to the community advising piece.

It is also -- I mean, it's a question of establishing processes by which people will be able to feel free that they are able to have the tools to do that kind of countermessaging.

The challenges that we have, again, is there are still trust deficits that need to be overcome. And we all -- as you said, we need to find those intermediaries who are willing to take up that effort.

LANGEVIN: Thank you.

For the panel, and before my time runs out, social media platforms play a prominent role in all of your testimony.

Obviously, can you describe the relationships that each of your agencies has with the private operators of these networks?

And are these relationships institutional or more based on personal relationships?

And what kinds of requests do you make of these companies?

STEINBACH: So, I won't get into specifics, sir. I would say that we have relationships with every company that's in that environment, because we have to. We have to serve them process.

It's based on personal relationships as a starting point, but we develop more than that. But I think each company is different. And I don't think it's appropriate in this setting to talk about those particulars with that company.

TAYLOR: Sir, I would add that homeland security in our cybersecurity role has relationships with all these companies and, as Mr. Steinbach mentioned, we probably want to have that -- this conversation in a classified environment.

LANGEVIN: Well, hopefully we can perhaps follow up on that, Mr. Chairman, at a later date, then.

MCCAUL: Yes. If I could just quickly follow up. A lot of people asked me why don't we conduct a cyber offensive attack to shut down these -- in the social media program. I guess the two problems with that is they, well, you know, once that's done, they'll open up another account rather quickly.

And, number two, I guess our intelligence gathering capability goes down quite a bit.

You don't have to comment on that.

But the chair now recognizes Mr. Ratcliff.

RATCLIFF: Thank you, Mr. Chairman. I want to thank you and the ranking member for holding this critically important hearing.

And of course I thank all the witnesses for being here and for all the important work that you do every day to serve our country.

This attack in Garland really seems to underscore and demonstrate the unique challenges that ISIS is posing today. In Garland, we saw two dead terrorists and no civilian casualties, and we saw law enforcement do exactly what they should have done, which is protect the public.

And yet we're living in unprecedented times, where a failed attack by ISIS in that regard is still spun as a win, where a failed attempt still plays into the narrative that they want to sell.

As a former terrorism prosecutor, who handled the number of matters involving Al Qaeda, I've noticed something that appears to me to be an important difference. And I want to ask you about that.

You know, Al Qaeda and ISIS have both been encouraging lone wolf attacks, but Al Qaeda's been doing it for years with very little success. And it would -- it seems to me that ISIS has been very effective in this regard in just a matter of months.

We're at a situation, it appears to me, that ISIS' sophisticated use of social media is essentially having a cascading effect, if you will, where it's become a terrorism multiplier of sorts, one where lone wolf attackers like Mr. Simpson or Mr. Soofi (ph) or Mr. Rahim (ph) can essentially use the ISIS brand without having to join ISIS.

And in that regard, it concerns me that it would appear that ISIS has essentially created a terror franchise. And so I want to very quickly ask you each whether you think I'm accurate in that assessment.

MULLIGAN: Congressman, I think that's an excellent characterization. I would agree with you, that is precisely they have very effectively leveraged that capability. They have exceptional capabilities and they claim they are making maximum use of every opportunity to amplify effect.

You've seen them using it in terms of representing their victories on the battlefield and the way that they have obviously treated our hostages. They attempt to squeeze every bit of, if you will, perceptual power out of social media.

TAYLOR: I would agree with Mr. Mulligan in that regard. I have been doing this for a long time, about 45 years. I've never seen a terrorist organization with the kind of public-relations savvy that I've seen with ISIL globally, and they've been very effective in using it.

STEINBACH: Yeah, I think my colleagues hit the -- the main points.

I would just add to it, in addition to that, it's a focus on a Western audience. When you look at the social-media tweets in English versus Al Qaeda or others, they are at a much higher rate.

So it's a great propaganda message. It's a propaganda message that's focused on a Western English-speaking audience.

RATCLIFFE: So we're talking a lot about the effect of their message. I want to focus a little bit more on the cause.

And Director Steinbach, you and the deputy director both talked about this, this sort of unique narrative that ISIS has created, a false narrative, one that involves a sense of community, a sense of adventure, maybe the ability to find a spouse.

We all know how ridiculous these claims are, but for those that are susceptible to radicalization, it seems to be an increasingly successful narrative from their standpoint.

I'm curious, since ISIS grew out of Al Qaeda in Iraq, why did ISIS suddenly become effective at crafting this -- this message when Al Qaeda and other terrorist organizations really hadn't been previously? We have any insight into that?

MULLIGAN: I don't want to oversimplify it, but I would point out the demographic. They have attracted a younger generation of fighters who are much more conversant.

They are in a situation where they have initially occupied territory in which there was fairly advanced infrastructure that could then be leveraged. So, I mean, if you think over time, as you know, Al Qaeda has, in some instances -- they were not occupying optimal areas to leverage that infrastructure, whereas ISIS did position itself very, very well.

And also I think they have a fundamental orientation to action that kind of dominates a lot of their psyche and how they move.

TAYLOR: I think the other difference, sir, is that social media wasn't as robust when Al Qaeda started, as it has been since -- actually since 2010, the Arab Spring, and how social media was used in those events and how it's propagated its use -- use by -- by other groups since that time.

STEINBACH: Just to -- just to further clarify what Frank said, he's absolutely right.

So when you look at the Internet four, five, six years ago, it was anonymous, but you still -- the bad guy, the individual living in the U.S. still had to reach to a forum, identify that forum, go into that forum. With social media, it's pushed to you. It's so far advanced in comparison to the anonymous Internet.

RICHMOND: My time's expired. I hope the chairman'll indulge me to ask one additional question, because I think what's important here is I want to find out what the -- you know, we've talked about their effective messaging and the fact that they've created essentially a winning brand that is a drawing -- that is drawing the disaffected and disenfranchised to them.

What are we doing to counter that message? What can we do besides -- in other words, to create a losing brand for them? And I realize that part of that is kinetic military operations on the ground and -- but from a social-media standpoint, is there a counter strategy?

MULLIGAN: So I would posit to you that there is basically a three-prong strategy.

We're trying to counter them on the battlefield because of the fact that we're trying to negate this image of the caliphate, which they're successfully representing. So if we can -- I mean, that's kind of their center of gravity.

The second piece, as you described, is the whole cyber online media piece. And going back just very quickly to what Frank said, the range of options of over-the-top applications that they are able to employ -- I mean going back -- I mean, what were the options that were available to Al Qaeda? Not so great.

Now we're in -- in another universe of -- of operational activity. But nevertheless, because they are operating in public space, they have vulnerabilities there, and we should move aggressively to counter that.

Finally, the third area is this ideological space that we talked about in terms of finding those voices, those credible voices that can contest the ideological message.

We need to work against all three of those lines of effort.

RICHMOND: Thank you, gentlemen. I yield back. Appreciate it, Mr. Chairman.

MCCAUL: Thank you.

Ms. Torres is recognized.

TORRES: Thank you, Mr. Chairman.

Mr. Steinbach, I am looking forward to reading that Brooklyn Institute study on terrorism and social media. I took a sneak peek at it while we were in this session.

I understand that as of October of last year, there were 42,000 identified Twitter accounts, if the report is correct, and thousands have been disabled.

In some ways, I kind of think that, you know, it's good to be able to view, you know, what is being said and what is being planned. It's -- it's one way that we can try to prepare and prevent.

Mr. Taylor, there's been a lot of talk about community outreach programs. There's been a lot of talk of community awareness, community policing. This is nothing new.

We've known that there have been a lot of issues in the past that need to be addressed from a neighborhood level. But somehow we have not been able to translate that want to do neighborhood community awareness to actually doing it.

And we've seen a lot of tensions arise between our local law enforcement groups and -- and our community groups. This is nothing recent; this has been ongoing.

So what have we changed? What does community policing look like, you know, in my neighborhood versus, you know, the northern part of California?

TAYLOR: Ma'am, your -- your -- your question is -- is a good question.

I think community policing is community policing. I don't think it -- it's about relationships with the communities that we serve. It hasn't changed in 20 years that -- that I've been involved in community policing.

It's the outreach that happens with people who are from the community so that you build partnerships. That's what community policing is all about, and I dare say it happens in diverse communities, it happens in majorities, but it has to happen the same way. You have to build a relationship.

And part of...

TORRES: You have to have the trust.

TAYLOR: And the trust.

And part of -- Secretary Johnson has spoken eloquently about this. When he goes out to do these community engagements, he's met with skepticism. He receives complaints about profiling and other sorts of concerns the community has, but you have to have that discussion, too, to build the trust, that we are talking about things the community needs to know that the community can do to protect themselves.

TORRES: Thank you.

Mr. Steinbeck, I know that -- well, I want you to know that I represent the Ontario Airport, which is, you know, to our demise, is controlled and managed by LAX.

I would like to hear more about the FBI's Joint Terrorism Task Force in Los Angeles and how they are working with my local police department in Ontario to ensure that training is happening, not only for those officers at LAX or LAPD but it is also happening for those officers who would be the first responders, should an incident happen.

STEINBACH: L.A.'s -- the L.A. FBI Joint Terrorism Task Force is a very large task force. It does not just include LAX; it includes all the major airports -- Orange county, Ontario.

And -- and I would suggest that you make an appointment to go out and tour that. I'm sure the office out there -- Dave Bowdich runs that office. He'd be happy to provide a tour view and give you firsthand an understanding of just how robust that task force is.

It is a -- I was just out there a couple of weeks ago discussing with him and -- and meeting some of the folks in his task force. But I would encourage you to go out there and -- and see firsthand.

TORRES: Right. I'd like to continue this discussion with you off the record here to bring to your attention -- my staff recently went on a tour, and I was saddened to have discovered that while training is happening among other agencies, Ontario Police Department has not been invited to participate in many of that -- or much of that.

STEINBACH: I'd be happy to have that conversation with you, and I'd also be happy to bring those concerns to Mr. Bowdich's attention.

TORRES: Tahnk you.

TAYLOR: Ma'am, if I might as well, in our community outreach role in DHS, we certainly are working very hard with police agencies throughout California.

So if there's a deficit of training and there's something that DHS might be able to help in Ontario, we're more than happy to -- to have that discussion and ensure that the training that is available in counterterrorism is available to Ontario.

TORRES: Thank you.

MCCAUL: Thank you.

Mr. Katko

MORE

XXX secure -- security even on the exterior of the European Union borders, and how that's not moving the way it should as quickly as it should. And even the technical support that we offer as a country to some of these countries as to how to deal with it is not being utilized.

KEATING: So I want to ask on a couple of fronts. Number one, I still think we can work together with countries, even if the European Union isn't moving. I want you to comment on how we're dealing with that information sharing -- local, state, federal -- and with those individuals countries. Because we also found that some countries are more receptive and moving faster than others in terms of information sharing that'll make us all safer, not just here and not just when Americans travel abroad in Europe, but here at home, too.

And the other thing is, the -- the idea that, you know, we're doing a good job swatting mosquitoes here at home when it comes to the Internet, but we're not drying up the swamp as much as we can. And can you comment on what we're doing for counter-messaging? Not just

enforcement or trying to find out what's going on, but in counter- messaging through the Internet to try and have competing messages, and what you think more could be done.

So those are the two questions. And anyone that wants to address those.

MULLIGAN: So I'll jump in on the first piece with regard to -- and, again, my colleagues are more conversant on pushing the information to the locals. But from a national perspective, we are very consciously trying to push the intelligence and the knowledge that has been gleaned from our assessments down to the locals so that they are more fully informed. That is definitely -- and we need to do more and we have to keep pushing that.

On the international piece that you described, it does become at times very unwieldy when you make it a multilateral issue. So we have established a number of very close bilateral relationships in terms of information sharing that's been very, very positive.

But the challenge is, if you really are going to try and address these challenges in a time efficient way, you need to ensure that a broader range is -- that you have the equipment that you can be passing information effectively. So that's a longer-term objective in that regard.

In terms of the overall counter-messaging, the government -- our government -- our federal government has an inter-agency process involved in which we're all moving to do counter-messaging. That counter-messaging works at the speed of government. It is -- well, as you understand, it has constraints in that. I think the real secret is going to be to broaden that overall counter-messaging and include those folks outside of the government so that they can...

KEATING: Oh, yeah.

MULLIGAN: ... participate in that process.

TAYLOR: I would make two comments here. First, this Committee has been very clear to me in my role as the undersecretary for Intelligence and Analysis that the core customer for the intelligence that we do is state and locals. And we have worked very hard from last year to try to transform how we approach the dissemination of data and information to our state and local partners, with our I.C. colleagues, with the FBI and with others in NCTC. But specifically focusing on getting relevant information out quickly to our state and local partners.

I -- I don't know how many joint intelligence bulletins we've done this year, but I think it's a record over last year. So that is our commitment to move this information and get into the hands of our first responders at the state, local, federal, travel and private sector -- and private sector.

When we talk about our foreign partners -- you mentioned the E.U. -- the E.U. is, in some cases, reluctant to -- to use PNR (ph) across all the E.U. We do have individual dialogues with members of the E.U. where certain countries are moving forward to do that within their own country.

I think -- I was just on the -- in New York at the U.N. with Secretary Johnson. We talked about U.N. Security Council Resolution 1267. I think there's more pressure on those communities to do that. And we'll continue to press to get those kinds of laws passed in those countries for that kind of information.

I would also emphasize that all of the visa waiver countries -- and that's most of the E.U. -- have independent bilateral agreements with us on information sharing. That may be through the intelligence service, it may be through the FBI or law enforcement. Those are very robust agreements that we're continuing to -- to press for the exchange of that kind of information. So it's not -- it's not a perfect scene (ph) yet, but the information exchange, both within our country to our state and local partners and also with our foreign partners continues to improve on daily basis.

MCCAUL: Now Mr. Loudermilk is recognized.

LOUDERMILK: Thank you, Mr. Chairman. And thank you all for being here. This is -- of all the hearings that we've had, in my opinion, this has been one of the most productive and informative that I've sat in on.

And one of the things that we're going to be doing in my office in the coming weeks is visiting with local law enforcement, our fusion centers within the district. Because what I'm seeing with these lone -- lone wolf attacks, the cause for attackers that are already in the U.S., is going to be a reliance on local law enforcement.

And with the recent attacks, it is a reminder to me, and I think to all of us, that these attacks are not against us as individuals. They're not against us as citizens. They're attacks -- they're attacks by those who are threatened or diametrically opposed to what we are as a people and what we have, which is freedom. You know, our freedom of thought, freedom of ideas, freedom of religion. And in the case of Garland, Texas was the freedom of speech. That was really what was being attacked.

With -- with that in mind, the American Freedom Defense Initiative and their -- their contest seems to be, as some have said, incited these attacks. And understanding it and knowing what happened with Charlie Hebdo in Paris, with which I was there just a few weeks ago in Paris with this codel (ph) -- it would leave us to believe that this is a potential target.

The first question -- what -- how far in advance of the event did our I.C. or counterterrorism know that this event was happening? And how do we find that out? Was there coordination with them? Or did this come from local law enforcement?

STEINBACH: WE knew about it several weeks in advance. And more specifically, I would say in this event, and the event in Phoenix last Friday, and in every event like this, we do go to those organizers and those individuals and lay out the threat and the potential. We, of course, don't try to talk them out of it, but we explain to them...

LOUDERMILK: Right.

STEINBACH: ... but we explain to them, "Hey, if you do X, this may happen." So we knew several weeks in advance.

LOUDERMILK: OK. So you know that these are coming. And how much interface do you have with the local law enforcement going into these?

STEINBACH: It's multifaceted. So, you know, we put out a -- a joint intelligence bulletin, which lays out, in this case -- Garland -- weeks -- a week in advance, it kind of laid out the event and the threat to the event. And this particular case and in many events like it, we do -- we push out a communication tool called the collection emphasis message. That collection emphasis message asks agencies, federal state and local, to collect intelligence on the event and the threat.

We put out tactical reports. We have, in many cases, depending on the size of the event, we have preparatory meetings with state and local, identifying who's going to have lead for crowd control, emergency response, tactical resources. It's a multilayered approach that we take with every special event.

LOUDERMILK: Now, I know Ms. Rice asked one of the questions I was getting at, which is, we -- we have 15 years of tracking terrorism -- terrorists and their activities, their threats through all the chatter. And so we've -- we've kind of got to where we can filter through what's just chatter and what's a valid threat.

Is how responsive our local law enforcement to the threats that we're laying out -- do -- do they tend to -- to take them seriously?

STEINBACH: Yes, we spend a lot of time, DHS, NCTC and the FBI -- pushing that message at the local level through the field officers, as well as at the executive level. Just two weeks ago, we had a video teleconference that was led by the director of the FBI and the director of Homeland Security, where we laid out again the threat -- the current threat. We do that periodically.

So there's multiple levels of engagement. Today I'm going to be talking to major city chiefs on this same topic.

TAYLOR: I would add, sir, that the -- we've created a network in our fusion centers with JTTFs across this country. Whenever an event occurs, there's someone up on the net saying, "What's the impact in my community?" And that's done over the Homeland Security intelligence network, or it's done over the law enforcement network of the FBI.

Our local law enforcement partners understand their primary responsibility to protect their communities. They understand these risks threaten their communities, and they are hungry for information to help them prepare. And that's -- what we've tried to design is a system that...

LOUDERMILK: Right.

TAYLOR: ... gets that information out to them. And once they get it, as they did in Garland, they take the appropriate action.

LOUDERMILK: Now, the -- and if -- if some of this -- these questions are more of a classified nature, we can -- we can respond to those later. Because I understand and appreciate, being in the intelligence community in the past. But of the -- the communications that we know that happened between the attackers and other bad players, how much of that did we know before the attack versus forensic information, and how much of that played into the -- the warning that -- that we sent to the -- to the local.

STEINBACH: I'd be happy to answer that but not in this setting.

LOUDERMILK: OK. I appreciate that.

And -- and the -- the last one is the reverse flow. Do we have good channels of communications for intelligence gathering from local law enforcement, who are the boots on the ground in the community?

Because, you know, this was a national event, per se, because it's -- it was an organization out of New York. But you may have a local event that could be a high-threat target.

Do we have a flow of information from the locals?

TAYLOR: Sir, it's a great question, and again, under the direction from this committee, we've worked to expand the amount of local intelligence that's gathered and reported into the I.C., that's relevant to the I.C., not only working with the FBI but working independently with our fusion centers in the field.

We've created a new process, what we call field activity reporting, where fusion centers working with DHS and the FBI will do reports from a field -- state-level perspective on threats and risks in the community. So I think we've created that opportunity for the local -- state and local partners to -- to report up, for us to report down and for all of us to share information on a continuous basis.

LOUDERMILK: Are they actively reporting up?

TAYLOR: Absolutely, sir.

STEINBACH: Let me highlight that a little bit more, sir.

So, I mean, the reason we are pushing information out is to make use of the 400,000 state, local and tribal law enforcement officers around the country.

They are our first response. They're the ones doing the car stop. They're the ones going into the house as first responders. They're seeing it well before any of us here see it.

It's incumbent we have the guardian process that allows for reporting -- the -- the eGuardian process that allows for reporting of information quickly into the fusion center and the JTTF model to act on that.

So that's -- that's the crux, and that's really at the foundation of this process.

LOUDERMILK: Thank you very much.

Mr. Chairman?

MCCAUL: Ms. McSally's recognized.

MCSALLY: Thank you, Mr. Chairman.

And thank you, gentlemen, for your testimony, and appreciate as part of our Task Force on Combating Terrorism and Foreign Fighter Flow, we've had some other conversations in classified settings. And so I appreciate all the work that you're doing.

The question I have today is about -- the first one is about the recruitment of women and girls from our country. It seems that jihadi women in Syria are actively recruiting or -- not just women -- recruiting Western girls.

I, you know, can't imagine what the draw would be except, of course, they're being lied to, like most of the recruits. But here, we have American girls that are being recruited to potentially flow over there for a life of rape and slavery and so specifically (inaudible) -- I think you said there's 200 that we know of, Americans that have -- have flowed over to the region.

How many of them are women and girls, and are there specific targeting efforts that we're doing community-wide, or others, in order to address specifically what's going on with targeting of women and girls?

STEINBACH: So I won't get into specific numbers, but, you know, when you look five, six years ago, the number of female recruits was almost nil.

So right now, it's -- it's -- 10 percent, I think, is probably a good ballpark. So it's -- it's a minority, but the fact that it went from zero to where it's at now is a significant uptick for us.

So yes, we look at the reasons why individuals are recruited, the specifics, young adult males, young adult females, what's drawing them. That's part of our process to understand it, what the motivations for radicalization.

We find a wide variety. It's not just the classic you see on TV, jihadi; there are other reasons that are motivating these young women to -- to take a chance and go overseas.

MCSALLY: So -- and as part of the countering of it and engaging with communities, actually, do we have messages of, "No, you are going to be in slavery and repeatedly raped when you get over there," and actually countering that and, you know, the graphic realities of what they're going to get recruited into, to include, potentially, testimonies of individuals that have experienced this?

I mean, that -- the way you counter a message is with a stronger message.

STEINBACH: Absolutely.

MCSALLY: And so we're doing some of that?

STEINBACH: Absolutely.

MCSALLY: At the local level as well?

STEINBACH: Yes. Through the JTTF, through the fusion centers, as part of the (inaudible) narrative, we are reaching out, you know, pushing the message out to the communities, to the schools, having conversations about the dangers of being online, not just online because of pedophiles and because of cyber criminals but online for fear of recruitment and enticement.

MCSALLY: Right. OK, great. Thanks.

My next question is about the use of social media for fundraising, and I wonder if you could comment on how ISIS is using social media in order to raise funds through crowdsourcing and other, you know, attempts to raise funds using social media, and are you working with the Department of Treasury, specific, Offices of Asset Forfeiture, FINCEN and -- and OFAC?

Specifically, how successful have they been, and how are we countering fundraising?

MULLIGAN: I would characterize it for you as it's a very arduous process to rebuild -- or build our understanding of the financial processes that ISIS and ISIL is employing currently.

I would also point out, as you're probably very well-aware, that they are -- in their expansion of the caliphate, they are literally taking possession of a number of resources and then exploiting that.

So to a large extent, they've been able to draw on a lot of those resources for a lot of their financing and funding. But nevertheless, it's a long -- because of the fact that they are an extended organization, they have to manage that financial infrastructure.

That's an intelligence effort that's underway. We're working aggressively with the Treasury Department and other states.

MCSALLY: So their online fundraising is minuscule compared to how -- I mean, I know black market and all the stuff they're doing in the region that they have and the ransoms and all the things that we're focusing on, but -- but specifically the online fundraising?

MULLIGAN: I would qualify it by saying I don't think that we're seeing the same degree of online fundraising that we probably have seen in the past by other entities.

(UNKNOWN): I would concur with that.

MCSALLY: Yeah. OK. Great.

And my last question, really quickly, is we know ISIS has been trying to motivate people to attack military bases or attack military members. Obviously, you know, I was in the military. Those are some of our most secure areas. There's, you know, certainly softer targets that they could go after.

But if they would recruit somebody who has access to a base, Major Hasan as an example, you know, we could have a major impact from an insider threat.

Have you seen ISIS attempting to recruit military members or those who have access to bases, and are you working with the Department of Defense in order to counter that threat?

TAYLOR: Well, as the chairman mentioned in his opening remarks, the Department of Defense takes this threat very seriously. They work very closely with the FBI and the I.C. and DHS around how those risks are -- might manifest themselves within the country.

Your point earlier, it's a pretty secure place, but they've even identified people by addresses, and we've worked with the military on strategies for those individuals to protect themselves at this point.

MCSALLY: Good. Any other comments?

MULLIGAN: Wanted to just offer the fact that it's very reasonable to expect a very aggressive effort by ISIS to be trying to derive military targets, because part of their overall narrative is the fact they want to draw linkages, they want to make those correlations.

So we have to be particularly vigilant with regard to military members.

MCSALLY: Great. Thank you. My time's expired.

Thank you, Mr. Chairman.

MCCAUL: Let me thank the witnesses for your testimony and your service to our country.

The members may have additional questions in writing. Pursuant to Committee Rule 7(c), the hearing will be open -- record open for 10 days.

Without objection, the committee stands adjourned.

END

Jun 03, 2015 19:26 ET .EOF