Hearing before the House Homeland Security Committee
"Terrorism Gone Viral: The Attack in Garland, Texas, and Beyond"
June 3, 2015

John Mulligan
Deputy Director
National Counterterrorism Center

Thank you Chairman McCaul, Ranking Member Thompson, and members of the Committee. I appreciate this opportunity to discuss the potentially tragic event in Garland, Texas, last month, which we thankfully averted. And I want to more broadly address the growing threat of violent extremists' use of social media to our national security. I'm pleased to join my colleagues and close partners from the Department of Homeland Security and the Federal Bureau of Investigation.

Garland Plot

As you already know, last month, two U.S. citizens attacked an art exhibit and cartoon contest in Garland, Texas. The attackers arrived on the last day of the event, exited their car, and opened fire with semi-automatic rifles, injuring a guard on the scene.

Thankfully, our law enforcement partners in the area were aware of the potential for violence and were able to respond quickly to prevent the attack from becoming a greater tragedy.

This event, however, exemplifies the challenge posed by homegrown violent extremists who can be motivated to violence quickly and have the means to attack without warning. It also highlights the growing threat our nation faces from a new generation of terrorists who find like-minded associates on the internet and social media to share their violent extremist ideology.

Garland Attackers' Use of Social Media

Let me explain more about how the Garland attack plans evolved. Less than two weeks before the attack, an online ISIL supporter posted a link on Twitter to a news article with information about the cartoon contest. This supporter's posting also included a message that suggested people should follow in the footsteps of the Charlie Hebdo attackers in Paris.

In addition, one of the Garland attackers reached out to the ISIL supporters and asked to move their communications to private Twitter messages.

Approximately 15 minutes before the attack, the same attacker posted a message on his Twitter feed indicating he had pledged allegiance to ISIL with the accompanying hashtag TexasAttack, which we now know was an indicator of his intent to target Garland.

While ISIL did not claim responsibility for the attack, many of its supporters, including a known ISIL member, praised the Garland attackers and encouraged others to follow suit. The group also highlighted the attack in its most recent edition of its English-language magazine *Dabiq*, in which it praised the attackers for seeking vengeance for the honor of the Prophet Muhammad.

Broader Commentary on ISIL's Use of Social Media

Like every other brand that targets young people, ISIL continually innovates to ensure it is using each new online marketing tool. Consequently, its social media presence—and that of its followers—is more widespread than that of any other terrorist group. In addition to maximizing its spread of terrorist messaging, the group shares guidance on how anyone can support ISIL and connects with like-minded individuals who become potential recruits.

In terms of the group's media efforts, ISIL has published more than 1,700 pieces of official terrorist messaging since the beginning of this year, including videos, pictorial reports, and magazines. These products are often very professional in appearance and continue to improve in quality with each new release, suggesting the group places a high priority on trying to win over the hearts and minds of new followers – including Westerners.

ISIL relies on the internet to send this material outside of Iraq and Syria and has shown a particular affinity for Twitter to disseminate official messaging, probably because the platform allows the group to reach a very broad audience. ISIL supporters also regularly use other platforms, such as Ask.FM and Facebook, to share information related to the self-declared Islamic State, including specific guidance on how to travel to Syria and how to avoid Western authorities.

ISIL supporters use the privacy of Twitter's direct messaging capability and encrypted messaging applications to discuss topics they deem too sensitive to display on their public accounts, such as travel facilitation into Syria or Iraq. We increasingly have seen ISIL supporters publicize their use of encrypted messaging applications on social media to let aspiring violent extremists and terrorists know that there are secure avenues by which they can communicate – after they make public contact online.

The group takes advantage of all the features and functions of social media to ensure widespread distribution of its messages. ISIL supporters on Twitter, for example, have used various tactics to expose its messaging to a more mainstream audience such as hijacking popular hashtags associated with pop culture figures or current events and using commercial applications to automate its tweets to make the group a trending topic.

It's important to be clear, however, that a video or series of pictures probably are not going to radicalize or mobilize to violence individuals who are just beginning to show interest in the group or violent extremist ideologies. Rather, these videos can serve as discussion points,

which enable other ISIL supporters to find one another and discuss their support for the group with like-minded individuals.

During the past few months, numerous statements from senior ISIL leaders have called for lone-offender attacks against the West. We remain highly concerned by numerous people in the Homeland who are buying into ISIL's distorted messaging. While we recognize companies have some initiatives underway to curb terrorist use of their platforms, there is still much work to be done.

Countering Violent Extremism (CVE)

The volume of individuals going abroad as foreign terrorist fighters to Iraq and Syria only emphasizes the importance of prevention. Enduring security against terrorism—and defeat of terrorist organizations like ISIL—rests in significant part on our ability to diminish the appeal of terrorism and to dissuade individuals from joining them in the first place. To this end, we continue to refine and expand the preventive side of counterterrorism. Working in close coordination with the Department of Justice (DOJ), the Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI), the National Counterterrorism Center (NCTC) is engaged in this work all across the country.

We collaborated with DHS to create tools that help build community resilience across the country. Additionally, we have seen a steady spread of proactive community awareness efforts across the US. These efforts aim to give communities both the information and the tools they need to recognize violent extremist ideologies and to intervene before radicalization to violence.

In concert with DOJ, DHS, and FBI, NCTC met with communities in Denver, Sacramento, Buffalo, and Minneapolis to raise community and law enforcement awareness of the terrorist recruitment threat. Our joint presentation, developed in partnership with DHS, addresses the specific issue of foreign fighter recruitment in Syria and Iraq; and we have received a strong demand for more of this outreach.

This is an effort to share information about how members of our communities are being targeted and recruited to join terrorists overseas. This is not a law enforcement-oriented effort designed to collect information. Seen in that light, we have had a remarkably positive reaction from the communities with which we have engaged.

With our DHS colleagues, we have also created—and regularly orchestrate—the Community Resilience Exercise. This is a table-top exercise that assembles local law enforcement and community leadership in tackling a hypothetical violent extremist or foreign fighter-related scenario, including a hypothetical attack. The goal of the exercise is to build capacity within municipalities to mitigate the terrorist threat.

We are also encouraging our local partners to implement models for countering violent extremism similar to existing crime prevention efforts. This approach mirrors the way, for

example, that local partners, including law enforcement, schools, social service providers, and communities, have come together to provide alternative pathways and outlets for people who might be vulnerable to joining a gang. We have found that the more resilient the community, the less likely its members are to join a terrorist group.

Countermessaging

As many community leaders have admirably pushed terrorist narratives out of their public spaces, these narratives have found refuge in virtual spaces. We understand that to truly counter violent extremist narratives, credible voices in communities should be encouraged to create alternative narratives that are attractive to target audiences. The role of these credible voices in communities as front-line responders cannot be overstated. Put plainly, we believe encouraging these community voices is an important and essential strategy.

However, communities best suited for repelling these terrorist narratives have not generally followed terrorist migration into online spaces. Communities whose young people are vulnerable to terrorist messaging have inconsistent capacities when it comes to countering that messaging. We believe this is the result of communities' fear of being associated with violent extremist elements, unfamiliarity with terrorists' online presence and tactics, and a lack of resources to create and disseminate alternative online content. Without confidence-building measures and proper training and resources, these communities will be hard pressed to counter ISIL's dominant messaging.

We are working with our partners and local communities to lessen these obstacles and to identify capacity-building measures. For example, we are connecting community leaders with entertainment industry executives. And we are actively trying to form public-private partnerships. For instance, the Peer2Peer program—a public-private partnership between EdVenture Partners and the Department of State—has empowered university students to create counter narratives to ISIL on social media. With programs like these, we have seen that private sector and community contributors can be much more nimble, creative, and credible online.

It is in everyone's interest to help mitigate this fear and encourage the use of law-abiding measures that communities can employ to confront terrorist narratives in virtual environments. To achieve this objective, we can provide training and information that will enable communities to use social and technical tools in the fight against online violent extremism. We can cultivate relationships between communities, the private sector, and the federal government based on trust and mutual benefit.

Conclusion

In summary, confronting these threats and working with resolve to prevent another terrorist attack remains the counterterrorism community's most important mission. This year, NCTC enters its second decade of service. While the Center has matured tremendously during that period, we are focused on positioning ourselves to be better prepared to address the terrorist threat in the decade to come. We expect this threat will increasingly involve terrorists' use of online platforms.

Chairman McCaul, Ranking Member Thompson, and members of the Committee, thank you for the opportunity to testify before you this morning. I want to assure you that our attention is concentrated on the security crises in Iraq and Syria—and rightly so. But we continue to detect, disrupt, and defeat threats from across the terrorist spectrum.

Thank you all very much, and I look forward to answering your questions.