The Police Chief
The Professional Voice of Law Enforcement
December 2014

Advanced Search
SEARCH

HOME SITE MAP CONTACT US FAQS SUBSCRIBE/RENEW/UPDATE IACP

Columns
President's Message
Chief's Counsel
Legislative Alert
Technology Talk
From the Director

Departments
Advances & Applications
Highway Safety Initiatives
IACP News
Line of Duty Deaths
New Members
Products & Services
Product Update
Survivors' Club

Current Issue
Archives Past Issues
Web-Only Articles
About Police Chief
Advertising
Editorial
Subscribe / Renew / Update
Law Enforcement Jobs
Buyers' Guide

send to a friend
printer-friendly

Social Media and the Homegrown Terrorist Threat

By Joseph Kunkle, Office of Security Technology, Transportation Security Administration, U.S. Department of Homeland Security, Washington, D.C.

While social media strategies present new opportunities and are playing historic roles in spreading prodemocracy uprisings across the Middle East, they also are creating new concerns for security agencies dealing in the complex world of extremist ideology. Prominent terrorist groups are adapting tactics and strategically evolving out of necessity because of far-reaching, multinational counterterrorism operations abroad. They are becoming more adept at making the best use of regional operatives, homegrown terrorists, and communication technologies at hand for a long-lasting terror campaign against the West. Today, terrorist groups are recruiting, inspiring, and guiding global strategies not just by Internet operations but through an organized, steady infusion of propaganda videos and call-to-action messages circulated via social media platforms, such as blogs, Facebook, YouTube, and Twitter.

The terrorist's social media framework is targeting disenfranchised youth with convoluted, fictional information and creating grassroots terrorists within the U.S. borders. As a result, foreign jihadists are enhancing their opportunities to attack the United States by means of a hybrid, multimedia *community participant* strategy designed to influence citizen extremists toward violence, orchestrate ideological movements, shape opportunities to recruit within the United States from unfolding world events, and encourage domestic terrorists to set their own goals and take direct action with open-source and open-ended jihad at home.

The strategy of bringing like-minded people together via conversational media to increase radicalism and the collective technical capabilities of jihadists, in concert with greater reliance upon regional criminal activities (for example, committing robberies and selling narcotics for revenue), is significantly changing the domestic threat picture and adding to the complexity of defeating borderless terrorism. This approach has eliminated the need for direct funding from prominent terrorist groups and global supporters because homegrown jihadists are capable of financing their own operations, as recently demonstrated by the disruptive and destructive improvised explosive device (IED) attacks in Stockholm, Sweden; Glasgow, Scotland; London, England; Madrid, Spain; and many thwarted plots in the United States. Of the 32 plots in the United States examined from open-source material, only a few showed evidence of foreign funding. Furthermore, virtual classrooms have lessened the operational impact of eliminating key bomb-making specialists, given that in-depth instruction for building IEDs is accessible through global networks.

Countless terrorists have been captured or killed in the wake of 9/11, including key operational leaders and highly trained bomb makers. These actions have yielded diminished tradecraft in building IEDs and reduced operational depth in planning and carrying out large-scale, deadly, spectacular attacks with far-reaching impacts, such as the Bali bombing in Indonesia, the attack against the USS Cole in the Yemeni port of Aden, and the simultaneous U.S. Embassy bombings in East Africa that killed hundreds of people via truck bomb explosions. Nevertheless, there still remains a prolific use of IEDs around the world, and IEDs continue to be the most widely used weapon by jihadists to kill and wound personnel both inside and outside of war zones. The use of social media tools to communicate openly with target audiences, such as potential recruits in the countries jihadists wish to attack, is contributing to the emerging spread of bomb-building capabilities and IED operations around the globe, including in the United States. This pervasive, asymmetrical threat is proliferating through the use of social media tools; bringing about long-term security challenges for intelligence organizations and domestic law enforcement agencies; and raising the domestic threat of unpredictable, small-scale surgical strikes by homegrown terrorists using vehicle-borne, person-borne, and leave-behind IEDs—the terrorist's weapon of choice.

Earlier this year, al Qaeda's media arm, the Global Islamic Media Front, released an English-translated bomb-making manual over the Internet on various social media sites. The training material in this manual originated from the teachings of Abu Khabbab al Misri, a well-known Egyptian bomb maker in the Explosive Ordnance Disposal (EOD) community who taught in terrorist training camps in Afghanistan and was killed by a U.S. missile strike in Pakistan a few years ago. This new, comprehensive explosives training manual–gone viral—teaches kitchen laboratory operations; general chemistry; in-depth instructions for synthesizing primary, secondary, and improvised explosives from commonplace ingredients; and directions for making detonators and IEDs. This trend of using social media as a learning platform to grow technical capabilities is creating new ways for homegrown jihadists to harness skills in building IEDs and improve operational techniques for launching lethal attacks in the United States. Moreover, social media is providing greater geographical reach for prominent terrorist groups and their widespread affiliates by providing experienced bomb makers and terrorist leaders (leadership is becoming more organic in nature) opportunities to communicate directly to followers and capitalize on homegrown jihadists' willingness to sacrifice life in prison or perform martyrdom operations anywhere in the world, especially in the West.

On the surface, this approach sounds familiar; terrorists have been spreading propaganda and IED instructions over the Internet for years, but the role that social media is playing in today’s means of communications is much more dynamic. For example, one activist in Egypt succinctly tweeted about why digital media was so important to the organization of political unrest: “We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world.”[1] This statement symbolizes the difference between the Internet and social media; social media will *come to* the radical rather than the radical *going to* the Internet and searching for the information.

Law enforcement should be under no illusion that the concept of terrorism and protecting critical infrastructure is very different than what it was one decade ago. Officials continuously face new and unforeseen threats, especially to open and interconnected transportation systems. Never before in history has the statement “anyone can become a terrorist” been more true or easier to attain than with the advent of social media.[2] No longer do traditional media—television, radio, newspapers, and other print publications—control the messages that terrorists seek to deliver to disenfranchise populace in regional or transnational areas. Today, instant-messaging jihadists can communicate with anyone and increase the drumbeat of violence by directly texting extremists in the homeland, linking videos, and editing domestic and foreign news stories to fuel anger and create feelings of self-importance and power. This kind of social media usage is making grassroots radicalization more feasible and is increasing the potential for recruiting operatives or facilitators legally living in targeted countries. This continuous type of exploitation will most likely increase the probability of future IED attacks within U.S. borders since more people than ever before with national, cultural knowledge (that is, integrated citizens and noncitizens able to blend into communities) have access to detailed instructions on producing explosives and making IEDs, support from within immigrant communities, and virtual guidance for carrying out bombing attacks with little to no warning signs for intelligence and law enforcement agencies to detect and disrupt plots.

Although there have been recent failed attempts by homegrown jihadists to carry out bombing attacks in the United States, 18 of 30 terror plots analyzed between 2001 and 2010 included using IEDs.[3] The security community cannot make the error of measuring the lack of understanding of explosives fundamentals and technical knowledge in IED construction as common operational practices of homegrown terrorists. Nor can law enforcement presume that because there were no detonations or causalities in these incidents, the capability to build lethal IEDs and carryout successful attacks in the United States has been perpetually diminished by the pursuit and arrests of terrorists around the world. Most likely, core

IACP Launches Project on Community Policing and Confronting Violent Extremism

There has been a rise in terrorism-related incidents involving homegrown violent extremists (HGVE), particularly in the past two years. In these HGVE cases, the perpetrators were motivated by a violent jihadists will take a long-term view of these botched operations—although not a failure in their eyes—and produce new, more detailed instructions on IED fabrication for social media distribution in an effort to build upon current, low-level technical capabilities. The counter-IED community has previously seen terrorist organizations post good-quality production instructional videos on the Internet for constructing suicide vests, explosively formed projectiles, detonators, and improvised explosives to improve IED tactics in overseas insurgency operations.

The tactic—whether intentionally planned or not—of lone-wolf individuals and self-made terrorists to opportunistically attack symbolic targets anytime or anywhere they discover vulnerabilities is skillfully creating open-source and open-ended warfare within the United States. Moreover, this approach has the potential to infuse uncertainty into future homeland threat analysis frameworks because of the inability to predict with accuracy the level of operational knowledge being shared and the technical capabilities being gained by multidimensional, irregular actors living in the United States. The result of this new threat paradigm is that a *nobody* can become a *somebody* without having to travel to Pakistan, Yemen, or regions in Northern Africa. In today's new reality, aspiring jihadists do not have to leave home to become radicalized or participate in deadly terrorist attacks against the United States. They can become radicalized in small steps without ever having to make the big leap overseas and risk being discovered by intelligence agencies. By logging onto Internet forums of unregulated and unrestricted speech, want-to-be jihadists can personally brand themselves as terrorists (lines between reality and fictional personas blur) and create a resilient virtual terror cell where they can share and spread ideological beliefs, raise funds, justify and create motives for violence, disseminate misinformation, learn and share terrorist tactics from war ideology that they were exposed to in person or via the Internet. Defeating the threat of homegrown terrorism depends on the whole of U.S. society to ensure that violent ideologies do not influence vulnerable communities or individuals. State, local, and tribal law enforcement agencies can lead this effort by leveraging established relationships with community organizations and leaders, developed through established community policing and outreach initiatives.

The IACP launched the Community Policing and Confronting Violent Extremism (CPCVE) project through a grant from the Office of Community Oriented Policing Services (COPS), U.S. Department of Justice. A primary goal of the CPCVE project is to produce resources for law enforcement to increase its capacity to counter violent extremist ideologies. This includes educating the community about how terrorists use the Internet and social media to win support and incite violence. As a result of education, the community will be better positioned to recognize the indicators of violent extremism and work in greater partnership with law enforcement to eliminate the threat.

For more information about the CPCVE project, please contact the program manager, zones, glorify and compare notes on successful and even failed terror operations and plots, inflame public opinion against Western society, and promote a jihad campaign against anyone or anything in the United States.

Sarah Horn, at horn@theiacp.org.

The crossroads of social media and IED operations in the United States creates a web of challenges for security organizations. Terrorists are recognizing social media's resiliency and operational effectiveness. Prominent terrorist groups are demonstrating an understanding that strength lies in numbers, and greater numbers of grassroots terrorists develop a greater capacity to successfully attack the United States from within. Protecting potential and favored targets from a strategy that emanates from behind media platforms with countless people having access to radicalization processes, where emotion obliterates reason and IED capabilities are built at home, is problematic. This evolving threat will require vast resources and varied approaches from federal, state, and local governments to constantly view media sites to become familiar with tactics of interest and watch for growing technical capabilities for carrying out IED attacks within the United States. The natural vulnerability to this method of communication and open-source warfare will most likely lead jihadists to increase their usage of social networking tools and, as a result, transform the framework of terrorism and what law enforcement believes and knows about this global phenomenon.

The lethal and psychological effectiveness of IEDs on a country's population, along with the increased ease of access to IED-building information, will ensure this threat remains for the foreseeable future. The likelihood of homegrown jihadists ascertaining the skills to deploy advanced IEDs in the United States from those who have experience in fighting overseas and who possess the know-how to make vehicle- or person-borne IEDs will test the efficacy of the frontline and the security community's deterrence credibility. An organization's deterrence credibility is measured by the speed at which stakeholders can identify emerging trends—not by actual incidents, but through the intelligence cycle—and design security measures to defeat or delay those evolving threats before they are used in an attack. This is the basis for risk-based, intelligence-driven security approaches, a process that most stewards of homeland security have adopted and implemented successfully. When implementing this security concept, law enforcement must appreciate one important element: seldom is intelligence black and white, and security strategies and operational measures must be made with the best information available, because playing catch-up to intelligence by attacks is never an effective option or a security measure in this war of adapt and overcome.

The multimedia strategy of prominent terrorist groups most likely reflects what they want to become at the start of this, the 21st century: An unpredictable, decentralized, networked, organic, freelance-type organization that introduces risk and uncertainty into the marketplace, draws upon intellectual talents and practical field experiences from personnel across the globe, and takes into account the activities and the contributions of jihadist operations around the world. This approach makes a prolonged strategy that presumes the sum of terrorist attacks in the homelands of Western nations is greater than a major individual attack.

Defeating this resilient, asymmetrical threat will require flexibility in legacy security measures and operations, as well as strategies of creative insights and collective developments of smart security solutions from all stakeholders. This should include developing a far greater depth of knowledge in explosives—especially in improvised and commercial explosives—and in global IED designs, operations, and capability levels and a more comprehensive understanding of the general threat spectrum the world faces. Law enforcement's ability or inability to swiftly respond to the growing use of social media channels and evolving IED tactics around the world will signal to the enemy the depth of U.S. strength in defeating this irregular, unprecedented challenge in the United States.

In closing, for the past couple of years, social media has become a vital operating juncture for allowing jihadists to operate autonomously and to plot attacks in the United States from within. To what extent social media tools are being used to radicalize individuals and plot attacks in the United States is difficult to determine because it is not easy to measure this process. Just as in the private business sector, elements that are unquantifiable are unknowns, unknowns inherently bring risk and uncertainty into operations, and unknowns in homeland security bring susceptibility to attack.

Social media has and continues to play a major role in increasing radicalization and the spread of instructions for IED attacks in the United States. For the near future, law enforcement will most likely continue to see lone extremists deploying low-skill-level IED attacks with a small number of causalities in the United States. While nobody will argue against this scenario, especially the unsuspecting people being targeted or the EOD technicians responding to these attacks, law enforcement cannot allow these types of incidents to deceive its better judgment. At its best, social media has the power to change the status quo; it can facilitate overthrowing authoritarian regimes and educate a society. At its worst, it can teach enough general chemistry, explosives fundamentals, electronics, surveillance operations, and IED operational planning to enable even novices to construct lethal IEDs capable of producing mass murder and destruction in U.S. cities and transportation sectors. In the words of philosopher and poet George Santayana, "We should always remember that those who do not learn from history are doomed to repeat it." History has tragically proven that terrorists exploit new technologies to plan attacks, evolve and learn from their mistakes, and take advantage of law enforcement's misjudgments in their emerging capabilities to carry out deadly attacks. ■

> *The views represented in this paper reflect that of the author and not that of the federal government, the Department of Homeland Security, or the Transportation Security Administration.*

Notes:

[1] Philip N. Howard, "The Arab Spring's Cascading Effects," *Pacific Standard*, February 23, 2011, http://www.miller-mccune.com/politics/the-cascading-effects-of-the-arab-spring-28575/# (accessed April 16,

2012).

[2] General Arjun Ray, in " 'Be a Part of Intelligentsia': A Talk on Countering Terror," January 15, 2009, Indian School of Business, Hyderabad, India, http://www.isb.edu/Media/UsrSiteNewsMgmt.aspx?topicid=494 (accessed April 19, 2012).

[3] New York State Intelligence Center, *The Vigilance Project: An Analysis of 32 Terrorism Cases against the Homeland* (December 2010), http://info.publicintelligence.net/NYSIC-VigilanceProject.pdf (accessed April 16, 2012).

Please cite as:

> Joseph Kunkle, "Social Media and the Homegrown Terrorist Threat," *The Police Chief* 79 (June 2012): 22–28.

Click to view the digital edition.

Top

send to a friend

printer-friendly