Homeland Security | Federal Bureau of Investigation

JOINT INTELLIGENCE BULLETIN

(U//FOUO) Use of Small Arms: Examining Lone Shooters and Small-Unit Tactics

16 August 2011

(U) Scope

(U//FOUO) This Joint Intelligence Bulletin (JIB) updates a DHS-FBI joint analytic product of the same title dated 3 September 2010 and is intended to provide warning and perspective regarding the scope of the potential terrorist threats to the United States, specifically towards US persons. This product is provided to support the activities of DHS and FBI and to help federal, state, and local government counterterrorism and law enforcement officials deter, prevent, preempt, or respond to terrorist attacks directed against the United States.

(U) Key Findings

(U//FOUO) The current evolving and diversified homeland threat environment and recent incidents involving small-arms operations in the United States and abroad demonstrate the need for continued vigilance and awareness. Small-arms operations could be employed through a range of tactics from a lone offender—as illustrated by the recent 22 July 2011 lone shooter attack that took place in Norway—to a coordinated small-unit attack involving several operatives.

(U//FOUO) We continue to assess that the scale and complexity of any attack of this type is dependent on a variety of factors, to include the sophistication and training of the attackers, the parameters of their targets, and the local security environment.

(U//FOUO) Threat Posed by Lone Offenders

(U//FOUO) Recent lone offender attacks and plots in the United States and abroad illustrate the effectiveness of the small-arms tactic and the need for continued vigilance and awareness of this tactic. Attacks by lone offenders—which by definition lack co-conspirators, and therefore provide fewer opportunities for detection—may be more difficult for law enforcement and homeland security authorities to disrupt.

- (U) On 27 July 2011, a US Army soldier who was absent without leave was arrested in Killeen, Texas for his alleged plot to target military personnel stationed at the nearby Fort Hood military post. Gunpowder, ammunition, and other items commonly used in the production of improvised explosive devices (IEDs) were found in the soldier's hotel room.

- (U) On 22 July 2011, after detonating a vehicle-borne improvised explosive device (VBIED) in Oslo, Norway, Anders Behring Breivik allegedly utilized small arms to kill 69 people on the island of Utoya, 17 miles outside of Oslo. Breivik is believed to have acted alone and used legal methods to procure the vast majority of materials and weapons needed for his operation, successfully avoiding law enforcement suspicion.

- (U) On 2 March 2011, a lone gunman at Frankfurt Airport in Germany killed two US airmen and seriously wounded two others when he boarded a US Air Force bus bound for Ramstein Air Base and opened fire.

- (U) On 5 November 2009, a US Army officer allegedly opened fire at the Fort Hood military installation's Readiness Center in Killeen, Texas, killing 12 and wounding at least 31. He was armed with two pistols, according to Army officials.

(U//FOUO) Incidents involving lone gunmen in the United States and abroad demonstrate the potential danger, lethality, and effectiveness of an unrehearsed small-arms attack by a single individual with little or no training, and underscore the potentially higher consequences of an assault-style attack involving multiple operatives.

(U//FOUO) Small-Unit Tactics Overseas

(U//FOUO) Terrorist and violent insurgent groups overseas—in many cases operating in nations battling violent civil unrest—have long favored small-unit assault tactics, in which small teams of operatives storm a target using small arms to defeat security. The frequency of these attacks is likely attributable to perceptions of their effectiveness, the prevalence of small-arms instruction at terrorist and militant training camps, and the widespread availability of assault weapons in conflict regions.

- (U) Beginning on 28 June 2011, nine terrorists—several wearing suicide vests and carrying small arms—infiltrated the Intercontinental Hotel in Kabul, Afghanistan. One suicide bomber reportedly detonated his vest at a guarded entrance, allowing other insurgents to enter the hotel kitchen and disperse throughout the building. The attack killed at least 12 people inside the hotel, and wounded 20 others.
- (U) On 24 August 2010, at least two members of the Somalia-based terrorist organization al-Shabaab—a gunman and a suicide bomber—stormed the Muna Hotel in Mogadishu disguised as police officers, killing at least 33 people, including 4 members of the Somali Parliament.
- (U//FOUO) On 21 July 2010, six attackers—probably insurgents from the North Caucasus—used small arms to kill two security guards and gain entry to a Russian hydroelectric plant. Once inside the facility, they detonated IEDs, destroying two of the plant's three hydropower generators.
- (U) In an early July 2010 attack on an international development organization's compound in Kabul, Afghanistan, insurgents breached the front gate with a VBIED. Five operatives armed with assault rifles and small IEDs entered and attacked the facility, killing 5 and injuring more than 20 people.

(U) The 2008 Mumbai Attack

(U//FOUO) The Mumbai attack in November 2008 stands as the most well-known example of a small-unit assault tactic. Ten operatives, who received specialized training from the Pakistan-based terrorist organization Lashkar-e-Tayyiba, formed small teams and infiltrated India by boat. The terrorists used small arms, hand grenades, and IEDs to attack multiple lightly secured facilities, including hotels and a rail station in Mumbai. The teams that stormed the Taj Mahal and Oberoi Trident hotels took hostages, leading to a multi-day standoff with police. Ultimately, 166 people and all but one of the attackers were killed.

(U//FOUO) Homeland Threat Posed by Small-Unit Tactics

(U//FOUO) Given recent events demonstrating the success of small-arms tactics and the evolving, diversified threat faced by the United States from al-Qa'ida and those inspired by its ideology, we assess that transnational terrorist groups and homegrown violent extremists (HVEs) could employ small-unit assault tactics in the United States.*

* (U//FOUO) DHS and FBI define an HVE as a person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

(U) Although we have no information indicating transnational terrorists have attempted to execute a small-unit assault operation in the Homeland, we note that disrupted HVE plots, such as the six individuals found guilty in 2008 of targeting the military base in Fort Dix, New Jersey and, more recently, two men alleged to have targeted a Military Entrance Processing Station in Seattle, Washington planned to employ small arms-based assault tactics.

(U//FOUO) Failure of Homeland IED Attacks May Increase Attractiveness of Small-Unit Assault Tactics

(U//FOUO) Failed bombing attacks targeting the Homeland—a 25 December 2009 attempt by an alleged al-Qa'ida in the Arabian Peninsula operative to detonate an IED on a flight from the Netherlands to Detroit and an unsuccessful VBIED attack in Times Square by a self-confessed Tehrik-e Taliban Pakistan operative—illustrate the complexity of training and deploying a terrorist operative to the Homeland to carry out attacks using explosives.

(U//FOUO) While terrorist organizations almost certainly will continue to attempt future homeland attacks using IEDs, it is also possible that operational planners will incorporate small-arms attacks that do not require mastery of IED construction or risk the failure of a complex bomb design.

(U//FOUO) Importance of Suspicious Activity Reporting

(U//FOUO) We face an increased challenge in detecting terrorist plots underway by individuals or small groups acting independently or with only tenuous ties to foreign handlers. Recent events have illustrated that state, local, tribal, and private sector partners play a critical role in identifying suspicious activities—such as unusual purchases of or inquiries about firearms, gunpowder, or ammunition—and raising the awareness of federal counterterrorism officials.

- (U) The US Army soldier arrested on 27 July 2011 for allegedly planning an attack against military personnel from Fort Hood came to the attention of authorities after a local gun store employee in Killeen, Texas became suspicious when the soldier acted oddly while purchasing smokeless gunpowder, shotgun ammunition, and a semi-automatic pistol and reported the behavior to police.

- (U//FOUO) The men convicted in 2008 for plotting to assault Fort Dix were discovered in 2006 after an attentive store clerk alerted authorities to a videotape of training activities the group attempted to have copied. It is unlikely this type of information would have come to the attention of federal officials unless it had been reported by partners in the private sector and state, local, and tribal government through suspicious activity reporting channels.

(U//FOUO) Recommended Protective Measures

(U//FOUO) Private sector security and law enforcement agencies can use protective measures to help disrupt or mitigate a terrorist attack in multiple phases—during surveillance, target selection, target infiltration, and engagement with security forces.

(U) Surveillance

- (U//FOUO) Train staff to be aware of unusual events or activities, such as individuals loitering for no apparent reason, sketching, or pace counting.

— (U//FOUO) Install and monitor closed-circuit television cameras covering multiple angles and access points.

— (U//FOUO) When possible, establish random security patrols to disrupt potential surveillance efforts.

(U) Target Selection

— (U//FOUO) Establish security at facility access points and potential approach routes.

— (U//FOUO) Know a facility's vendors and, if possible, randomly alter delivery entrances to avoid developing discernable patterns.

— (U//FOUO) Avoid widely distributing site blueprints or schematics and ensure those documents are kept secured.

(U) Target Infiltration

— (U//FOUO) Establish an outer perimeter at target sites to deny access or intercept potential assailants, and ensure security personnel and security measures are in place at all access points.

— (U//FOUO) Establish a credentialing process for facilities.

— (U//FOUO) Conduct background checks on all employees.

(U) Engagement with Security Forces

— (U//FOUO) Encourage local law enforcement to meet with key facility staff to assist in the development and familiarization of emergency evacuation and lock down procedures.

— (U//FOUO) Conduct security sweeps for explosive devices and increase security measures in zones that could be compromised.

— (U//FOUO) Federal, state, and local law enforcement entities should routinely conduct joint training and communication coordination exercises to allow for effective deployment of multiple units in a crisis.

(U) Reporting Notice

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force and the State and Major Urban Area Fusion Center. The FBI's 24/7 Strategic Information and Operations Center can be reached by telephone number 202-323-3300 or by email at SIOC@ic.fbi.gov. The DHS National Operations Center (NOC) can be reached by telephone at (202) 282-9685 or by email at NOC.Fusion@dhs.gov. FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm and Fusion Center information may be obtained at http://www.dhs.gov/contact-fusion-centers. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at (202) 282-9201 or by email at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) Administrative Note: Law Enforcement Response

(U//FOUO) Information contained in this intelligence bulletin is for official use only. No portion of this bulletin should be released to the media, the general public, or over nonsecure Internet servers. Release of this material could adversely affect or jeopardize investigative activities.

(U) For comments or questions related to the content or dissemination of this document, please contact the FBI Counterterrorism Analysis Section (202) 324-3000 or via email at FBI_CTAS@ic.fbi.gov, or I&A Production Branch staff at IA.PM@hq.dhs.gov.

(U) Tracked by: HSEC-8.1, HSEC-8.2.2, HSEC-8.5.1, HSEC-8.6.2.21, HSEC-8.6.3, HSEC-9.1, HSEC-9.2