Western Jihadist threats to the military

Samuel J. Mullins

University of Wollongong, smullins@uow.edu.au

Publication Details

Western Jihadist threats to the military

Abstract
In a recent high-profile terrorism case in the U.K., a British-born ISIS sympathizer named Junead Khan was convicted for plotting to attack and kill U.S. military personnel stationed in Britain.[1] His plan was to ram into a vehicle carrying American soldiers and then behead the incapacitated victims. Had police intervened at any point, the intention was to detonate a pressure cooker bomb, committing suicide in the process and maximizing the number of casualties. Far from being an isolated case, this is just one of a long list of attacks on military personnel which have been planned and sometimes executed by Western jihadists. Indeed, Khan appears to have been directly inspired by the events of May 22nd, 2013, when an off-duty British soldier, Fusilier Lee Rigby, was run down and hacked to death by two extremists on the streets of Woolwich, east London.[2] Plots and attacks like these understandably grab headlines and result in at least temporarily heightened force-protection measures. However, little effort has been made to systematically analyze Western jihadist threats to the military, which of course are not limited to the U.K. and are both diverse and ongoing. Drawing upon a variety of cases involving Europe, North America and Australia, this article identifies a range of overlapping external and internal threats and discusses implications for military security.

Disciplines
Arts and Humanities | Law

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/lhapapers/2872
Western Jihadist Threats to the Military

By Sam Mullins
Journal Article | May 17 2016 - 9:19am

Western Jihadist Threats to the Military

Sam Mullins

Introduction

In a recent high-profile terrorism case in the U.K., a British-born ISIS sympathizer named Junead Khan was convicted for plotting to attack and kill U.S. military personnel stationed in Britain.[1] His plan was to ram into a vehicle carrying American soldiers and then behead the incapacitated victims. Had police intervened at any point, the intention was to detonate a pressure cooker bomb, committing suicide in the process and maximizing the number of casualties. Far from being an isolated case, this is just one of a long list of attacks on military personnel which have been planned and sometimes executed by Western jihadists. Indeed, Khan appears to have been directly inspired by the events of May 22nd, 2013, when an off-duty British soldier, Fusilier Lee Rigby, was run down and hacked to death by two extremists on the streets of Woolwich, east London.[2] Plots and attacks like these understandably grab headlines and result in at least temporarily heightened force-protection measures. However, little effort has been made to systematically analyze Western jihadist threats to the military, which of course are not limited to the U.K. and are both diverse and ongoing. Drawing upon a variety of cases involving Europe, North America and Australia, this article identifies a range of overlapping external and internal threats and discusses implications for military security.

External Threats

In this context, external threats involve civilian jihadists acting against domestic military targets from outside of the organization. Most notably, this includes planned and/or executed terrorist attacks as well as malicious hacking operations aimed either at defacement, disruption or acquisition of sensitive information. A third type of external threat involves the acquisition of military materials such as manuals, weapons or other items, though not necessarily for use against military targets.

Terrorist Attacks against Domestic Military Targets

Since 2001, there have been at least 38 plots by civilian jihadists to attack domestic military targets in the West, 26 of which were thwarted (see Table 1 below) and 12 of which (i.e. 32%) were actually executed (see Table 2).[3] Among the thwarted attacks, 19 of these (i.e. 73%) occurred after 2008 and the majority occurred either in the U.S. (38%) or U.K. (35%). Twelve plots (46%) were aimed at military bases, with the intention of using bombs and/or firearms to kill personnel inside; another nine (35%) were aimed at soldiers off-base (whether specific individuals named in the media or else anyone identifiable as a member of the armed services); a further two plots (8%) were aimed at recruitment centers; one group was targeting a town, Royal Wootton Bassett in the south of England, due to its role in the repatriation of
British soldiers killed in Afghanistan and Iraq[4] and in the final two remaining cases, the specific target was unidentified.

The intended modus operandi of thwarted attacks has mostly consisted of explosives (38%) and firearms (31%), although knives (in Junead Khan’s case combined with use of a motor vehicle) have become more common from 2014 onwards. Notably, this has occurred after the murder of Lee Rigby in 2013, which suggests a contagion effect. Also of note is the fact that just five plots could be considered operationally capable at the time of arrest, one involving firearms and the rest involving knives. Among thwarted plots, the closest that anyone came to manufacturing viable explosives was the so-called Sauerland Cell in Germany, but security services had swapped the group’s hydrogen-peroxide for a 3% solution that rendered their efforts useless.[5] The Sauerland Cell was also one of just six cases involving support from a foreign terrorist organization (FTO).[6]

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 2001</td>
<td>Belgium</td>
<td>Nizar Trabelsi's plan to attack the Kleine Brogel airbase</td>
</tr>
<tr>
<td>Mar 2005</td>
<td>UK</td>
<td>Plot to assassinate a British soldier</td>
</tr>
<tr>
<td>Jun 2006</td>
<td>Canada</td>
<td>Plot to bomb a military base, CSIS HQ and the Toronto Stock</td>
</tr>
<tr>
<td>Jan 2007</td>
<td>UK</td>
<td>Parviz Khan’s plot to kidnap and behead a Muslim soldier</td>
</tr>
<tr>
<td>May 2007</td>
<td>US</td>
<td>Plan to assault Fort Dix</td>
</tr>
<tr>
<td>Sep 2007</td>
<td>Germany</td>
<td>Sauerland Cell plot to attack Ramstein airbase</td>
</tr>
<tr>
<td>Dec 2008</td>
<td>Italy</td>
<td>2 Moroccans targeting Milan military barracks</td>
</tr>
<tr>
<td>Jul 2009</td>
<td>US</td>
<td>Dylan Boyd and Hysen Shenli plan to attack US military bases in Virginia</td>
</tr>
<tr>
<td>Aug 2009</td>
<td>Australia</td>
<td>Operation Neath: Plot to attack Holsworthy army barracks using firearms</td>
</tr>
<tr>
<td>Oct 2009</td>
<td>France</td>
<td>Nuclear physicist discussed attacks on military targets with AQIM</td>
</tr>
<tr>
<td>Jul 2010</td>
<td>US</td>
<td>Paul Rockwood hitlist, including military personnel</td>
</tr>
<tr>
<td>Dec 2010</td>
<td>US</td>
<td>Antonio Martinez plan to bomb a military recruitment center</td>
</tr>
<tr>
<td>Feb 2011</td>
<td>US</td>
<td>Khalid Aldawsari considered targeting soldiers from Abu Ghaiba</td>
</tr>
<tr>
<td>Jun 2011</td>
<td>US</td>
<td>Plot to attack a Seattle Military Entrance Processing Station</td>
</tr>
<tr>
<td>Oct 2012</td>
<td>UK</td>
<td>Operation Nimrod: Plot to attack a TA base using a remote control car</td>
</tr>
<tr>
<td>Jul 2012</td>
<td>UK</td>
<td>Richard Dart et al plan to attack Royal Wootton Bassett</td>
</tr>
<tr>
<td>May 2013</td>
<td>US</td>
<td>Fazliddin Kurbawan plan to bomb military targets</td>
</tr>
<tr>
<td>Jun 2013</td>
<td>Italy</td>
<td>Anas El A. used Google Maps to surveil Brescia military barracks</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>UK</td>
<td>Brushtom Ziamani plot to emulate the Woolwich attack</td>
</tr>
<tr>
<td>Aug 2014</td>
<td>UK</td>
<td>Kazi Islam attempt to incite a Woolwich-style attack / bombing</td>
</tr>
<tr>
<td>Oct 2014</td>
<td>UK</td>
<td>Tarik Hassane et al plot to do drive-by shootings targeting military/police</td>
</tr>
<tr>
<td>Nov 2014</td>
<td>UK</td>
<td>Nadir Syed et al Remembrance Day plot</td>
</tr>
<tr>
<td>Feb 2015</td>
<td>US</td>
<td>Plot to attack a N. Carolina military base involving minors</td>
</tr>
<tr>
<td>Feb 2015</td>
<td>US</td>
<td>Abdurrahman Sheik Mohamud plot to execute soldiers at a US base</td>
</tr>
<tr>
<td>Apr 2015</td>
<td>US</td>
<td>John Booker plan to bomb Fort Riley, Kansas</td>
</tr>
<tr>
<td>Jul 2015</td>
<td>UK</td>
<td>Junead Khan plan to kill US airmen stationed in Britain</td>
</tr>
</tbody>
</table>

Table 1. List of thwarted terrorist plots involving civilian jihadists in Western countries targeting the military (2001–2015). Cases highlighted in bold involved lone individuals, i.e. no other active accomplices or informants.

Turning our attention to attacks which were actually executed against domestic military targets in Western countries, all twelve of them occurred after 2008. Four attacks took place in France, there were three attacks in Canada and two in the U.S., while Italy, Germany and the U.K. have experienced one apiece.
The majority of attacks (7 out of 12, or 58%) were conducted against soldiers in public places. These include the shooting of two U.S. soldiers at Frankfurt airport in March 2011\[7\]; the assassination of three French soldiers in two separate attacks by Mohamed Merah in Toulouse and Montauban in March 2012\[8\]; the stabbing of a soldier at a train station in Paris in May 2013\[9\]; the killing of two Canadian soldiers in separate incidents in Saint-Jean-sur-Richelieu (using a motor vehicle\[10\]) and Ottawa (firearms\[11\]) in October 2014; and the attempted running over of four soldiers guarding a French mosque in Valence in the southeast of France in January 2016.\[12\] A further three attacks (25%) took place on military installations. The first was an attempted suicide bombing of military barracks in Milan in October 2009\[13\]; the second was the May 2013 stabbing of a French gendarme in Roussillon\[14\]; and the last was the fatal shooting of four U.S. Marines and a sailor at a Navy Reserve Center in Chattanooga, Tennessee in July 2015 (which was preceded by a drive-by shooting at a nearby Armed Forces Career Center\[15\]). Recruitment centers were also attacked on another two occasions; a fatal drive-by shooting in Little Rock, Arkansas in June 2009,\[16\] and the stabbing of two Canadian soldiers in Toronto in March 2016.\[17\]

### Table 2.

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jun 2009</td>
<td>US</td>
<td>Shooting at Little Rock army recruiting centre (1 dead)</td>
</tr>
<tr>
<td>Oct 2009</td>
<td>Italy</td>
<td>Attempted suicide bombing of military barracks, Milan</td>
</tr>
<tr>
<td>Mar 2011</td>
<td>Germany</td>
<td>Frankfurt airport shooting (2 dead)</td>
</tr>
<tr>
<td>Mar 2012</td>
<td>France</td>
<td>Toulouse/Montauban shootings (7 dead)</td>
</tr>
<tr>
<td>May 2013</td>
<td>France</td>
<td>Stabbing of agencie, Roussillon, Iseran</td>
</tr>
<tr>
<td>May 2013</td>
<td>UK</td>
<td>Murder of British soldier, Woolwich, London (1 dead)</td>
</tr>
<tr>
<td>May 2013</td>
<td>France</td>
<td>Stabbing of assolider, Paris</td>
</tr>
<tr>
<td>Oct 2014</td>
<td>Canada</td>
<td>Two Canadian soldiers run over in Quebec (1 dead)</td>
</tr>
<tr>
<td>Oct 2014</td>
<td>Canada</td>
<td>Shooting attack at Parliament Hill, Ottawa (1 dead)</td>
</tr>
<tr>
<td>Jul 2015</td>
<td>US</td>
<td>Chattanooga shooting (5 dead)</td>
</tr>
<tr>
<td>Jan 2016</td>
<td>France</td>
<td>Card runned at French soldiers guardinga mosque, Valence</td>
</tr>
<tr>
<td>Mar 2016</td>
<td>Canada</td>
<td>Stabbing attack at Canadian Forces recruitment center</td>
</tr>
</tbody>
</table>

Five of the above incidents (i.e. 42%) involved firearms; four (33%) involved knives (combined with the use of a motor vehicle in the murder of Lee Rigby); another two attacks (17%) involved vehicles only; while explosives were used (unsuccessfully) on just one occasion. In total, seven of these attacks resulted in fatalities, five of which involved firearms and five of which targeted soldiers while off-base. Just one individual had established links to a FTO – namely Mohammed Merah, who had previously trained with militants in the Afghanistan-Pakistan border region and claimed to be acting on behalf of al-Qaeda (AQ).\[19\]

In light of these developments, it is clear that although Western jihadists still prefer soft, civilian targets, they have increasingly targeted the military –as well as police– since 2009.\[20\] This may be in part because they are regarded as more prestigious and morally defensible by the perpetrators; however there is no obvious reason for the timing of the increase, other than perhaps the aforementioned contagion effect, whereby plotters are inspired by the actions of others. The countries where the military is most likely to be targeted are the U.S., U.K. and France, although it is worth noting that Canada suffered three attacks within a relatively short space of time (which prompted a review of security at all Canadian military installations\[21\]) and of course no country is immune. Based on what we have seen so far, the most likely scenario for an externally-generated attack against domestic military targets involves small, freelance groups or lone-actors who are lacking FTO support, using firearms or other readily-available weapons (vehicles and knives) to ambush soldiers in public places. Nevertheless, in light of the recent, successful
use of triacetone triperoxide (TATP)-based explosives in France and Belgium, more sophisticated attacks of course cannot be ruled out.

Malicious Hacking Attacks

A more recent development, which gathered pace during 2015, has been the use of hacking techniques, either to deface or disrupt military (as well as other government and non-governmental) websites and/or to steal and publish sensitive information online. Two online groups have been particularly active in targeting the military – namely the ‘CyberCaliphate’ (CC) and the ‘Islamic State Hacking Division’ (ISHD). Exactly who and how many individuals have been responsible for these groups is unknown; however, a central figure in both appears to have been Junaid Hussain, a British jihadist who was previously convicted of hacking offences in the U.K. and was eventually killed in a U.S. drone strike in August 2015.[22] Together, the CC and ISHD have been credited with at least eight hacking attacks against Western military targets (although one is disputed and another three apparently utilized open source information rather than hacking), while others have carried out at least five similar operations (see Table 3 below).[23]

The vast majority of these attacks have involved the online publication of personally identifiable information (PII) of military personnel, other government officials and sometimes family members. Details vary but have included names, photographs, physical as well as IP addresses (some accompanied by satellite imagery), phone numbers, email accounts and passwords. Besides generating a sense of fear or unease, causing embarrassment and financial loss, as well as demonstrating the ability to compromise seemingly secure government systems (which no doubt delivers a boost to terrorists’ morale), such operations are clearly intended to incite and facilitate attacks. As the ISHD declared in March 2015, “These kuffar [infidels] that drop bombs over Syria, Iraq, Yemen, Khurasan [Afghanistan] and Somalia are from the same lands that you reside in, so when will you take action? Know that it is wajib [religious obligation] for you to kill these kuffar [infidels]! and now we have made it easy for you by giving you addresses, all you need to do is take the final step, so what are you waiting for? Kill them in their own lands, behead them in their own homes, stab them to death as they walk their streets thinking that they are safe”. [24]
Table 3. Hacking operations against Western military targets, January – May 2016.

<table>
<thead>
<tr>
<th>Date</th>
<th>Perpetrator</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>12-Jan-15</td>
<td>CyberCaliphate</td>
<td>Hacked CENTCOM Youtube and Twitter accounts, defaced accounts, published PII* and sensitive documents</td>
</tr>
<tr>
<td>10-Feb-15</td>
<td>CyberCaliphate</td>
<td>Hacked Military Spouses of Strength Twitter account and made threats</td>
</tr>
<tr>
<td>21-Mar-15</td>
<td>ISHD**</td>
<td>ISHD document containing PII for 100 U.S. military personnel circulated on Twitter and jihadi forums, accompanied by calls for them to be killed***</td>
</tr>
<tr>
<td>8-Apr-15</td>
<td>CyberCaliphate</td>
<td>French TV5Monde network hacked and disrupted, PII of relatives of French soldiers broadcast†</td>
</tr>
<tr>
<td>29-May-15</td>
<td>ISHD</td>
<td>ISHD document containing PII for 10 Italian military personnel circulated on Twitter***</td>
</tr>
<tr>
<td>26-Jul-15</td>
<td>Unspecified</td>
<td>ISIS supporters circulated PII of NATO soldiers on Twitter</td>
</tr>
<tr>
<td>11-Aug-15</td>
<td>ISHD</td>
<td>PII of hundreds of U.S. military personnel and government officials, along with information on RAF bases in the U.K., released via Twitter</td>
</tr>
<tr>
<td>22-Aug-15</td>
<td>Unspecified</td>
<td>ISIS supporters circulate &quot;#Entire IP ranges [of the] #U.S. #government military and #security #bases and #websites&quot; via Twitter</td>
</tr>
<tr>
<td>23-Aug-15</td>
<td>Al-Battar Media</td>
<td>Video released via Twitter featuring PII of U.S., U.K., French, and Italian soldiers and other officials, allegedly collected via hacking of a &quot;UK military website&quot;</td>
</tr>
<tr>
<td>11-Sep-15</td>
<td>ISHD</td>
<td>A second &quot;kill-list&quot; of 100 U.S. military personnel released via Twitter, accompanied by the hashtag #AmericaUnderHacks</td>
</tr>
<tr>
<td>22-Sep-15</td>
<td>Islamic Cyber</td>
<td>PII of 7 U.K. soldiers released via Twitter, accompanied by the hashtag Army #BritainUnderHacks</td>
</tr>
<tr>
<td>21-Dec-15</td>
<td>Caliphate</td>
<td>PII of 14 CIA &quot;leadership personnel&quot; distributed via Twitter</td>
</tr>
<tr>
<td>1-May-16</td>
<td>ISHD</td>
<td>PII of 76 US Air Force personnel distributed via JustePaste.it***</td>
</tr>
</tbody>
</table>

*Personally Identifiable Information, typically including names, addresses, phone numbers, emails
**Islamic State Hacking Division
***Data believed to have been obtained through open sources rather than hacking
† Attack subsequently attributed to a group of Russian hackers called APT28

Fortunately, as of May 2016, there are no indications that military personnel identified in hacking operations have been targeted for physical attacks. Nevertheless, the calls for violence continue. Indeed, the above-quoted ISHD document, along with PII for a hundred U.S. military personnel, was widely circulated online by jihadi sympathizers – most notably Terrence McNeil, a hospital worker from Ohio, who was subsequently charged with soliciting murder.[25] More worrying still, rather than relying on general appeals, hackers have also directly urged specific individuals to act upon the information they have acquired. Prior to his death, Junaid Hussain was in communication with a number of Western jihadists involved in planning/executing attacks, including Junead Khan, whom he offered to provide...
home addresses of British soldiers.\textsuperscript{[26]} Hacking operations have also continued despite Hussain’s demise and are now clearly an established tool in the repertoire of jihadist activity. In light of such persistence, it is entirely possible that hacking techniques will become more sophisticated over time and that the virtual and physical operations of Western jihadists will intersect violently in the future.

\textit{Acquisition of Military Materials}

A third area of concern is where Western, civilian jihadists have tried or successfully obtained military knowledge, expertise, equipment and/or weaponry. Although such materials have not necessarily been intended for use against domestic military targets, they of course raise terrorist capabilities and –depending on the origins of the material– may fall under the military’s overall responsibility. The most common type of activity here involves the acquisition of military training and field manuals. Although these can now easily be found online, it is worth noting that in fact the so-called “al-Qaeda Manual” –recovered from the Manchester home of Abu Anas al-Liby in May 2000\textsuperscript{[27]}– was largely based upon U.S. military training manuals stolen during the 1990s by an Egyptian AQ operative named Ali Mohamed\textsuperscript{[28]} (see more under the heading of “Infiltration” below). Since then, numerous Western jihadists have been found in possession of official military instructional materials, which they often share with associates, although there is little evidence of the knowledge within being applied. In one such case in the U.S., an individual named Barry Bujol Jr. had acquired a number of restricted American military manuals, which he emailed to an informant, whom he believed to be a member of AQ, in the hope that the “brothers” overseas would then be able to overcome American forces\textsuperscript{[29]}

In similar vein, others have acquired a variety of equipment with direct military application in Western countries, which they then supplied to terrorists overseas. For instance, during 2003 and 2004, Mohammed Junaid Babar (an American who worked closely with jihadists from the U.K.) delivered money, “night vision goggles, sleeping bags, water proof socks, water proof ponchos and other military gear” to a senior AQ figure based in South Waziristan\textsuperscript{[30]} Of course, such items can be legally purchased by members of the public, meaning they are unlikely to be acquired from strictly military sources. Of far greater concern is the acquisition of restricted military hardware and weapons. In addition to copious amounts of hydrogen peroxide, the aforementioned Sauerland Cell was in possession of 26 military detonators\textsuperscript{[31]} In September 2012, a pair of French jihadists threw a hand grenade into a Jewish supermarket in Paris\textsuperscript{[32]} while more recently, Islamist terrorists in Europe have proven capable of obtaining military-grade weapons with apparent ease. Most of these, it seems, originate in the Balkans or Eastern Europe and are trafficked to countries like France where anyone with the right connections can buy them\textsuperscript{[33]} However, it is also possible that weapons belonging to Western militaries may end up in the hands of terrorists. In 2002 an Australian Army captain stole ten M72 rocket launchers from a facility just outside of Sydney. The leader of an Islamist terror-cell, Mohamed Ali Elomar, subsequently purchased five of those launchers (which have yet to be recovered) from an organized crime figure named Adnan Darwiche\textsuperscript{[34]} Of course this was a single incident, rather than necessarily being indicative of a broader trend, yet it serves as a reminder that any criminality or corruption within the military may serve as a point of vulnerability that both organized criminals and terrorists alike can potentially exploit. Worryingly, in July 2015 it was reported that around 180 detonators and a dozen blocks of plastic explosive had been stolen from an army base in the south of France\textsuperscript{[35]} and it is not uncommon for both military and law enforcement agencies to “lose” significant amounts of weaponry and related accessories.\textsuperscript{[36]} In light of Western jihadis’ well-established interest in obtaining such materials, there is an obvious need to ensure they are appropriately secured and accounted for.

\textit{Internal Threats}

The manifestation of internal jihadist threats is often similar to external (i.e. civilian) threats – the key
difference being that the perpetrators are current members of the military. They include infiltration, insider attacks and espionage. A fourth type of threat, which is closely related, involves former members of the military who become involved in terrorism after they leave the service.

**Infiltration**

Deliberate infiltration of the military by individuals who are already radicalized blurs the line between external and internal threats. It naturally begins as an external threat but then becomes internal if/when the individual in question succeeds.[37] By far the most successful example of infiltration was by Ali Mohamed, who was an officer in the Egyptian Army before joining the al-Jihad organization in 1981 and thereafter becoming a core member of AQ and one of the principle planners behind the East African embassy bombings of 1998.[38] In 1984 he briefly volunteered as an informant for the CIA, before the agency realized he was up to no good and cut him loose. Remarkably, he went on to serve in the U.S. Army for more than three years, based at Fort Bragg in North Carolina, and gained American citizenship. During that time, he was assigned to teach fellow soldiers about Middle Eastern politics, culture and religion. As noted above, he also used the opportunity to steal a variety of military documents, which he used to create terrorist training manuals for AQ. In his spare time, he provided training to a group of extremists in New York and New Jersey, including some of the first World Trade Center bombers, and in 1988 he even fought against the Soviets in Afghanistan whilst on leave. Although Mohamed left active military service in 1989, he joined the Army Reserve and in 1992 became an informant for the FBI, not long before travelling to Africa to conduct surveillance of potential targets for attack. It was only after those attacks took place that he was eventually arrested and imprisoned.

Contemporary Western jihadists generally lack the skill and sophistication of an operative such as Mohamed, yet some have nevertheless still tried to infiltrate the military as a means of gaining access to training, weaponry and combat zones, and/or to conduct attacks. In October 2008, an individual named Abdel Hameed Shehadeh from New York attempted to enlist in the U.S. Army with the apparent intention of deploying to Iraq where he would then desert and fight against American soldiers.[39] However, his application was denied when it was discovered that he had concealed a previous trip to Pakistan, where he had tried, unsuccessfully, to go and join the Taliban. In another more recent case, John Booker Jr., from Topeka, Kansas, had successfully enrolled in the Army in February 2014 with the intention of committing an insider attack. He was scheduled to report for basic training but was discharged after it was discovered he had expressed a desire for violent jihad and martyrdom on social media. He was then arrested in April 2015 and ultimately pleaded guilty to attempting to bomb the Fort Riley military base.[40]

Both Shehadeh’s and Booker’s efforts were extremely crude and neither really succeeded in infiltrating the armed forces. It is worth noting, however, that Booker had been posting comments in support of violent jihad long before applying to join the military and it was only after the FBI alerted the Army that they became aware and expelled him.[41] Moreover, although there is no evidence to suggest that Islamist extremists are systematically attempting to infiltrate Western militaries, the number of reported incidents has grown. For instance, in 2012 the FBI was said to be tracking approximately a hundred suspected Islamist extremists within the U.S. military (around 12 of whom were believed to be “serious” threats)[42] while more recently, Spanish,[43] French[44] and German[45] authorities have expressed similar concerns. Despite this, there are few concrete examples to be found and reports generally fail to distinguish between deliberate infiltration of the military (i.e. by individuals with a pre-existing extremist mindset and hidden agenda) versus radicalization and expression of extremist beliefs after having joined. Nevertheless, as the above examples illustrate, there are clear incentives for jihadists to try and infiltrate military organizations and the threat is believed to be significant enough to warrant the introduction of additional security measures in some countries. In Germany, for example, there are now plans to perform
background checks on all new recruits, rather than just those working with classified material or in sensitive positions.

**Insider Attacks**

A second internal threat involves the planning and execution of jihadist-inspired attacks by serving members of the military against fellow soldiers. To date, the author is aware of just four such cases, all involving Americans, who appear to have radicalized as individuals *within* the military, rather than infiltrating with the pre-existing intention of conducting an attack (see table 4 below).

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar 2003</td>
<td>Kuwait</td>
<td>Hasan Akbar; grenade/firearms attack on fellow soldiers (2 dead)</td>
</tr>
<tr>
<td>Nov 2009</td>
<td>US</td>
<td>Nidal Hasan; Fort Hood shooting (13 dead)</td>
</tr>
<tr>
<td>Oct-Nov 2010</td>
<td>US</td>
<td>Yonathan Melaku; shootings on Virginia military installations</td>
</tr>
<tr>
<td>Jul 2011</td>
<td>US</td>
<td>Naser Jason Abdo; plot to kill US soldiers near Fort Hood*</td>
</tr>
</tbody>
</table>

*Attack thwarted prior to execution.

Table 4. Insider plots and attacks committed by military members, at least partly motivated by extreme Islamist beliefs. Cases highlighted in bold involved lone individuals, i.e. no other active accomplices or informants.

In the first of these cases, Hasan Karim Akbar, then a sergeant in the Army, launched an attack shortly after 1am at Camp Pennsylvania in Kuwait on March 23, 2003, just a few days before members of the 101st Airborne Division stationed there were due to deploy to Iraq.[46] After throwing grenades into tents where fellow soldiers were sleeping, he opened fire with his rifle, killing two officers. Although there is no evidence to suggest that Akbar was directly inspired by jihadists, the prosecution described his actions as “hate-filled, ideologically driven murder” and his primary goal appears to have been to prevent his victims from killing Muslims in Iraq.[47] Both his actions and his motivations are therefore sufficiently similar to include Akbar’s case in the current analysis, whether or not it is classed as an act of terrorism. In the second case, Major Nidal Malik Hasan, an Army psychiatrist, entered the Soldiers Readiness Processing Center at Fort Hood, Texas in the early afternoon of November 5, 2009.[48] Armed with a handgun, he shouted “Allahu Akbar!” before opening fire on those inside, killing twelve service members and one civilian before being incapacitated by civilian police officers. Although the Department of Defense (DoD) still classifies this as an act of “workplace violence”, Hasan had received ideological advice from Anwar al-Awlaki via email and claimed to be acting in defense of the Taliban within the context of what he perceived was a war against Islam.[49]

In the third insider attack case, there was damage to buildings but no fatalities. Between October and November 2010, a young Marine Corps Reservist, Lance Corporal Yonathan Melaku, conducted a series of five nighttime shootings targeting military installations in Virginia, including the National Museum of the Marine Corps, the Pentagon, and recruitment centers for the Marine Corps and U.S. Coastguard. He was eventually apprehended on June 17, 2011 in Arlington Cemetery – adjacent to Fort Myers – in possession of a backpack containing shell casings, components for an improvised explosive device (IED) and jihadist literature.[50] In the fourth and final case, Private Naser Jason Abdo was arrested at a hotel in Texas on July 27, 2011. In his room was a handgun, precursor materials for making an IED and the now-infamous *Inspire* magazine article, “How to Make a Bomb in the Kitchen of Your Mom”. As Abdo admitted to federal agents, his plan was to bomb a restaurant in the vicinity of Fort Hood which he knew to be frequented by American soldiers, after which he would shoot any survivors. He was thwarted only
because he had aroused the suspicion of an alert sales clerk while purchasing smokeless gunpowder and other materials at a nearby gun store.\[51\]

Although we cannot necessarily generalize from just four cases, each of the perpetrators exhibited some important similarities that may be useful in the identification and prevention of similar attacks in the future. To begin with, they each had histories of problematic conduct and in three of the four cases were underachievers who failed to fit in. Akbar had previously been demoted, was known for falling asleep during meetings and was said to have an “attitude problem”.\[52\] Hasan had been disciplined for unprofessional conduct in 2007 for inappropriate discussion of religion, underperforming in his duties and being overweight.\[53\] Melaku meanwhile had been awarded the National Defense Service medal and Marine Corps Reserve medal;\[54\] however, he was also charged in May 2011 –just a few months prior to his attacks– with two counts of grand larceny (i.e. theft) in relation to a series of motor vehicle break-ins.\[55\] Finally, Abdo was said to have “horrible” rapport with his peers and in the weeks prior to his arrest had gone absent without official leave after being found in possession of child pornography.\[56\]

In addition, for three of these individuals problems had arisen in relation to religion. Akbar had skipped the 1991 Gulf War on religious grounds and had complained of racism and being harassed because of his faith.\[57\] Hasan had given a number of presentations with Islamist themes, including one in 2007 entitled “The Koranic Worldview as it Relates to Muslims in the U.S. Military” in which he declared that “It’s getting harder and harder for Muslims in the service to morally justify being in a military that seems constantly engaged against fellow Muslims.”\[58\] Lastly, Abdo had complained about being unable to properly observe Ramadan and in 2010 refused to deploy to Afghanistan because of his faith, eventually being granted conscientious objector status the following year.\[59\] Impending deployment may also have served as a trigger or catalyst for violence for both Akbar and Hasan.

Of course, refusal to do one’s duty based on religious (or, for that matter, any other) grounds is problematic. In the case of Hasan, his behavior in the years preceding the attack at Fort Hood has since been described as “overt displays of radicalization” and a missed opportunity for earlier intervention.\[60\] However –while preventative action must be pursued whenever possible– it is important to note here that none of these four individuals openly expressed their intention to commit acts of violence. It was later found that Akbar had written about his desire to kill soldiers in his personal diary, but of course this was private.\[61\] A far more significant indicator was Hasan’s communication with Anwar al-Awlaki, who was by that time already a suspected terrorist. As a result, Hasan was briefly investigated by the FBI; however they failed to piece together the extent of his communications and ultimately dismissed them as “research”, given his documented interest in Islamist ideology.\[62\] Contact with known or suspected terrorists should represent a major red flag, yet in this case was overlooked. In the other three remaining cases such connections were absent altogether. Indeed, notwithstanding Hasan’s links to Awlaki, all four inside attackers were lone actor terrorists, which severely limits opportunities for detection. In cases like this, the expression of “extremist” beliefs (in this context, including the perceived incompatibility between faith and military service), must be taken very seriously, especially when accompanied by a history of behavioral and/or mental health problems.\[63\] Such indicators may well stop short of establishing clear terrorist sympathies or violent intent, but they may still provide grounds for some form of intervention. Pending the results of an investigation, this might potentially include restriction of access to firearms, revocation of security clearances, mandatory counselling, voluntary or involuntary discharge or other measures depending on the specific case and tools available. Yet it is also worth bearing in mind that disciplinary or other measures based on low-level potential indicators of radicalization, perhaps including faith-based grievances, may present procedural and even legal difficulties. Ultimately, based on the empirical record, insider attacks by Western military recruits are likely to remain rare, yet cannot be ruled out in future, meaning that clear, preventative policies must nevertheless be in place.
Espionage

A third internal threat involves espionage, i.e. stealing of sensitive information, by service members with a jihadist agenda. There have so far been just two confirmed cases that the author is aware of, both in the U.S., plus one suspected case in France. In the first case, a Navy signalman named Hassan Abu Jihaad (originally Paul Hall) sent classified information about battleship movements to a pair of British jihadists while serving aboard the USS Benfold between August 2000 and September 2001. He was honorably discharged in 2002 and was not arrested until 2007, eventually receiving a sentence of ten years for disclosing national defense information. The second case involved another convert to Islam, a specialist in the National Guard named Ryan Anderson. Between January and February 2004, a few weeks before he was due to serve in Iraq, he attempted to make contact with Islamist extremists online and supplied information—including details of U.S. Army movements, troop strength, tactics and weapons systems—to individuals he believed were members of AQ (in reality the FBI). A military tribunal found him guilty of attempting to provide intelligence to the enemy and sentenced him to life in prison. Finally, in January 2015, French police discovered that a female gendarmerie named Emmanuelle C. –also a convert, who was reportedly in a relationship with a wanted criminal and confederate of French jihadist Amedy Coulibaly—had accessed the “suspect person’s file” more than sixty times without authorization. Although it is unclear exactly what she did with the information that she accessed, she was dismissed from her job and given a year of probation.

In comparison to the insider attack cases described above, the recorded instances of espionage appear to have been even more low-key, with—from what is publicly known—little indication of the perpetrators’ extremist beliefs and no reported history of problematic conduct during their military careers. However, for espionage to occur there must necessarily be some form of contact with external parties, which represents a key point of vulnerability. Neither of the first two offenders were particularly discreet. In the former case, Abu Jihaad used his official Navy email address and it is doubtful that such a case would go undetected for so long in the post-9/11 era (it seems he was eventually discovered only after 9/11 due to the arrest of his contacts in the U.K.). In the latter case, Anderson had a long history of reaching out to others on a variety of online forums and—having turned to extremism—eventually came into contact with an Internet vigilante (someone posing as a jihadist) who then passed his information to the FBI. Less is known about the French case, but she clearly failed to effectively hide her criminal associations. In today’s world, it seems quite unlikely that jihadist “spies” would be so careless. In addition, the widespread availability of encrypted software, now included in day-to-day applications, means that similar, contemporary offenders may find it easier to conceal their communications. As a result, the point of acquisition of sensitive materials and any other suspicious behavior within the workplace become even more important as potential opportunities for detection and intervention.

Military Veterans Involved in Terrorism

Analytically—since military veterans become civilians once they leave active duty—we now come full circle, as internal threats merge back into the external category. Although it has become an issue of increasing concern, there is a long history of former members of Western (as well as other) militaries becoming involved in violent jihad. In the U.S., military veterans were part of the very first jihadist networks that emerged during the late 1980s and early 1990s, with close ties to the New York and New Jersey terror-cells responsible for the first World Trade Center attack and the related plot—overseen by Omar Abdel Rahman—to bomb various New York landmarks. They included individuals such as Ephron Gilmore aka Tahir (allegedly an instructor at AQ’s al-Farooq camp in Afghanistan), Clement Rodney Hampton-El (one of the “landmarks” plotters and an active supporter of the Bosnian mujahideen), Abu Ubaidah Yahya (aka Carl Taylor, who provided training in the U.S. and assisted Hampton-El’s
efforts in the Balkans[71] and “Abu Abdullah” (who led a team of fourteen former American soldiers, again in support of the mujahideen in Bosnia[72]).

Similar examples have continued to come to light. In late 2001, shortly after being discharged from the Australian Army, suffering from post-traumatic stress disorder (PTSD), a former private named Matthew Stewart made his way to Afghanistan where he joined the Taliban and AQ. In October 2015 he resurfaced in Syria as a member of Jabhat al-Nusra (JN), using the name Usama Hamza Australi.[73] Several more American veterans have also tried and occasionally succeeded in joining terrorist organizations overseas, including Craig Baxam,[74] Eric Harroun[75] and Tairod Pugh.[76] According to the German military counterintelligence service, 29 former Bundeswehr soldiers have travelled to Syria and Iraq to join extremist groups[77] and at least ten French soldiers have reportedly deserted and done the same.[78] While the vast majority of these individuals have joined terrorist-insurgencies overseas (becoming so-called foreign fighters), some have also been involved in planning domestic attacks. For instance, in July 2015 it was revealed that a former signalman in the French navy, identified as Djebril A., had been plotting, along with three confederates with links to the so-called Islamic State (IS), to kidnap and behead the commanding officer at Fort Bear on the south coast of France.[79] In a previous case uncovered in 2007, a former cadet in the British Territorial Army, who had been jailed for assaulting a fellow cadet and was suffering from significant mental health problems, was convicted of planning an attack on his old base from within prison.[80] In October 2014, a radicalized US Navy veteran named Zale Thompson took things a step further, assaulting a group of New York City police officers with an axe before being shot and killed.[81]

The overall number of Western military veterans becoming involved in Islamist terrorism appears to be small, yet still significant. It is particularly troubling, given the knowledge and skills that such individuals possess, which can potentially be transferred to organizations like AQ and IS and be put to use in planning and conducting domestic attacks. From the military’s perspective, there is relatively little that can be done once an individual leaves the organization – especially if there are no signs of radicalization beforehand, in which case it essentially comes down to the work of intelligence and law enforcement agencies. However, if a person is identified as a potential violent extremist prior to leaving active duty, steps should be taken to reduce the level of risk if possible and clear policies must be in place to enable the notification of civilian security services and/or support agencies.

**Summary and Concluding Remarks**

Western jihadist threats to the military can be divided into overlapping external and internal categories, depending on the status of the perpetrators. Chief among the external threats are domestic plots and attacks, which have become significantly more frequent in recent years. The plots most likely to come to fruition involve lone actors using firearms, motor vehicles and/or knives to ambush soldiers in public places. Although such attacks are exceptionally difficult to prevent, basic measures such as raising awareness among troops, avoiding wearing uniforms or insignia in public and travelling in groups of two or more, can significantly reduce the likelihood of casualties. As with all of these threats, it is also important to establish lines of communication with relevant civilian law enforcement and intelligence agencies to facilitate timely sharing of information and effective collaboration if and when necessary.

A second external threat that has become increasingly frequent in recent years involves hacking of government computer systems in order to obtain sensitive information – in particular PII for military members and their families, who may then be targeted for attack. Military organizations obviously have a responsibility to maintain adequate security for websites and online databases and efforts must be made to document all relevant breaches of security, to review the techniques that Western jihadi hackers and their allies are employing and to identify the specific vulnerabilities they have so far exploited, in order to
harden online defenses. Individual service members may also contribute by maintaining basic online security – for example, safeguarding personal information on social media and taking steps to avoid falling victim to phishing scams or viruses.

The third and final external threat involves jihadist acquisition of potentially dangerous military materials, ranging from training manuals to weapons and related accessories. Given that it is not uncommon for such materials to go missing and sometimes end up on the black market, it would seem prudent for those responsible to review their security arrangements.

Internal threats are much less common and yet also more troubling when they occur. To date, there have been very few verifiable examples of premeditated infiltration of the armed forces by Western jihadists and recent attempts have been lacking sophistication. Nevertheless, there are clear incentives for trying to infiltrate the military and authorities in a number of countries have expressed concern over this issue. The obvious implication is to ensure adequate background checks for all new recruits (to include reviews of social media, travel patterns, associations and any information held by law enforcement and intelligence agencies).

The most serious internal threats are insider attacks conducted by radicalized individuals against fellow soldiers. Such cases have been mercifully rare and so far have occurred only in the American military. Based on this limited experience, they are most likely to be conducted by lone individuals (though perhaps in communication with known extremists or terrorists) and may display a history of problematic conduct, underachievement and faith-based grievances – most notably the increasingly fervent belief that being a Muslim is incompatible with military service. Some of these individuals may also exhibit mental health problems, although this is by no means guaranteed. Importantly, the inside attackers seen to date (at least those in the West) did not overtly express their intention to commit acts of violence. This means that the threshold for preventative intervention must come earlier, based on the above-noted indicators. The French Defense Security Protection Department (DPSD) has identified the following, additional factors as potential signs of extremism: “changes in dress, recurrent sick leave, [suspicious] travel, or theft of supplies or materiel.” Accessing extremist websites or possession of related propaganda materials may also be added to this list. In reality, indicators of potential extremism may be weak, however, within such highly regulated and fraternal organizations, the chances that insider threats will be identified are increased.

Another internal threat – albeit extremely rare – involves espionage. The cases so far have been amateur and their impact minimal, although more serious instances cannot be ruled out in future. Potential warning signs might include any of the indicators noted above, naturally including contact with known extremists or visitation of related websites or other online platforms. In the absence of specific indications of jihadist tendencies, potential warning signs are likely to be similar to “ordinary” insider threats, which are covered in routine training.

Finally, it is now well-established that small, yet significant numbers of Western military veterans are becoming involved in violent jihad following their departure from the armed services. As noted above, it is important to share information on any suspected extremists with civilian security services as they transition to civilian life (if not before) but in the absence of prior indicators of radicalization there is little that military organizations can do, other than cooperate with subsequent investigations.

In conclusion, Western jihadist threats to the military have grown significantly in recent years. In particular, the most likely threats are external and come in the form of physical and cyber attacks, although it would clearly be a mistake to ignore internal threats, which have produced almost as many fatalities despite being less common. As much as the threat has grown, the overall likelihood and impact
of Western jihadist actions against domestic military organizations remain relatively low. Moreover, the risk of both external and internal threats can be significantly mitigated by way of relatively basic security procedures. Western militaries must remain cognizant of “home-grown” jihadist threats and should certainly review security measures in line with this article. There are no grounds for complacency, yet there is also little reason for panic.

End Notes


[3] Figures based upon databases for the U.S., U.K., Canada and Australia maintained by the author, with additional data for Europe based on Petter Nesser, “Chronology of Jihadism in Western Europe 1994–2007: Planned, Prepared, and Executed Terrorist Attacks” Studies in Conflict and Terrorism, (2008), 31 (10), 924–946; Petter Nesser, “Toward an Increasingly Heterogeneous Threat: A Chronology of Jihadist Terrorism in Europe 2008–2013” Studies in Conflict and Terrorism, (2014), 37 (5), 440–456. A number of additional cases where military targets were mentioned by plotters in passing but were not clearly focused upon are excluded from this analysis. Also excluded are an additional 12 plots targeting police, 10 of which were executed.


[6] An additional six cases involving planned attacks on domestic military targets also had links to FTOs but they were not seemingly involved in the plot.


[18] Note that the French National Gendarmerie falls under the responsibility of the Ministry of Defence. For the purposes of this analysis, gendarmes are therefore included as “military”, while regular police
forces are excluded.


[24] Stalinsky and Sosnow, “Hacking in the Name of the Islamic State (ISIS)”.


[31] Eijkmann, “The German Sauerland Cell Reconsidered”.


[37] Note that Mohamed Merah (cited above) had unsuccessfully applied to join the armed services in France on two separate occasions – once in 2008 and again in 2010. However, there is no evidence that he had ulterior motives at the time.


[39] “Hawaii Resident Charged with Making False Statements in a Matter Involving International


23, 2016.

[52] Roig-Franzia, “Army Soldier Is Convicted in Attack on Fellow Troops”.


[58] Gruen, “The Massacre at Fort Hood”.


[63] Note that only one inside attacker had a documented history of mental health problems – namely Hasan Akbar, who had been diagnosed with depression aged 14, seemingly suffered from sleep apnea as an adult and was also seen talking to himself while on duty (Gruen, “Backgrounder: Sgt. Hasan Akbar”).


[67] “Former Member of U.S. Navy Sentenced to 10 Years in Federal Prison for Disclosing Classified Information”.


[71] Berger, Jihad Joe, 12, 64–69; United States v. Omar Ahmad Ali Abdel Rahman et al.


[74] “Former U.S. Soldier Who Sought to Join Terrorist Group Convicted and Sentenced to Seven Years in Prison


Fischer and Prautsch, “Are Islamists Using the German Military as Training Ground?”

Mamou, “France: Jihad Infecting Army, Police”.


Note that an earlier review of jihadist hacking operations concluded that “the overall impact and sophistication of jihadist hacktivists’ attacks have been relatively low and will likely remain as such in the near term” (Christopher Heffelfinger, “The Risks Posed by Jihadist Hackers” CTC Sentinel, (2013) 6 (7), https://www.ctc.usma.edu/posts/the-risks-posed-by-jihadist-hackers. Accessed October 22, 2015). The successful hacking of government/military websites during 2015 arguably represents an escalation of such operations in terms of the profile and sophistication of the targets, as well as the sensitivity/value of some of the data acquired, it is unclear whether the techniques being used have become more refined.

Mamou, “France: Jihad Infecting Army, Police”.

About the Author

Sam Mullins

Dr. Sam Mullins is a Professor of Counter-Terrorism at the George C. Marshall European Center for Security Studies, Germany and an Honorary Principal Fellow at the University of Wollongong, Australia. He is the author of ‘Home-Grown’ Jihad: Understanding Islamist Terrorism in the US and UK (London: Imperial College Press, 2016). Twitter account: @Sam_J_Mullins.

Available online at: http://smallwarsjournal.com/jrnl/art/western-jihadist-threats-to-the-military

Links:
{1} http://smallwarsjournal.com/author/sam-mullins
{2} http://www.telegraph.co.uk/news/2016/04/01/delivery-driver-guilty-of-isil-plot-to-kill-us-troops-in-uk/
{3} http://www.theguardian.com/uk-news/2013/dec/19/lee-rigby-murder-michael-adebolajo-adebowale-