PENNSYLVANIA ACTIONABLE INTELLIGENCE BRIEFING #16

TARGETED ACTIONABLE MONITORING CENTER

4 DECEMBER 2009

******

STRATEGIC ANALYSIS

Communiqué Confirms Jihadist Focus on Infrastructure

In a communiqué made public on 2 December 2009, jihadists from the Islamic Emirate of the Caucasus (IEC) claimed responsibility for the 27 November 2009 double bombing of the Nevsky Express in Russia, which killed around 30 people. In their statement, the IEC reiterates and confirms the worldwide jihadist focus on infrastructure attacks, insofar as such are feasible.

Specifically named targets in the IEC communication include infrastructure assets, economically significant targets, energy assets, mass transit, power lines and energy pipelines, as well as civilians. "Many of the operations are in the process of being prepared," the IEC warned.

The IEC declared that the Nevsky Express attack was part of a larger plan to strike "a number of strategically important assets" in Russia, after "it was decided to transfer the sabotage war to the territories of Russia, along with strong blows to the occupiers infrastructure in the Caucasus." The jihadist group states explicitly, "We will do everything possible to spread jihad even further in the territory of Russia in order to undermine its economy, so that Russia will not have the opportunity to use the Caucasus as its raw material base."

Indeed, one day before the Nevsky attack, a diesel train line in the Caucasus region, south of Makhachkala, was bombed. Earlier that same day, an IED was discovered along a gas pipeline in the Dagestan.

In a previous claim of responsibility, on 25 November 2009, Chechen jihadists of *Muwahidun Al-Rusi* ("The Russian Monotheists") announced that they bombed "the largest subterranean natural gas storage facility in the world" in Stavropol, Russia. The same organization claimed to have sabotaged a major hydroelectric plant in August. Whether or not the claims are true - in some cases the jihadists "claim" accidents for their own portfolio - the targeting focus is abundantly clear.

Cyber-Infrastructure, Too

Commenting on the recent attacks and claims of responsibility, a jihadist communication observed: "Large countries like Russia, that rely on public transportation, are vulnerable to such attacks. Keep cutting the transport links and the economy will wither and die."

Nonetheless, physical infrastructure is only one kind of infrastructure target jihadists have discussed. Much of today's world depends on a virtual infrastructure - which means a "virtual jihad" against those assets as well.

In September 2009, Targeted Actionable Monitoring Center analysts noted a possible scenario implied in jihadist communications involving a coordinated attack by cyber-hackers against an American asset (or assets) that would affect a large portion of the population. Another possibility raised is a hacking attack targeting high-profile systems, such as those of NASA, the Pentagon or infrastructure companies.

Inside Jobs

In its recent communication, the Emirate of the Caucasus also boasts of its covert operations capabilities, again aimed at the same target - the entire economic infrastructure: "This year ... several intelligence-sabotage units were trained and sent deep into Russia to conduct operations on the enemy's territory. ...These operations have caused enormous economic damage to Russia; we will continue to work in this direction."

As noted by the TAM-C in November 09, careful analysis of the recent spate of intelligence sharing communications, as well as previous intercepts, show that jihadists are actively attempting (and in some cases succeeding) to recruit vulnerable individuals from within targeted infrastructure systems.

For example, in September Indonesian investigators revealed that an interrupted bomb plot by jihadists involved smuggling explosives on board an airplane with the assistance of a sympathetic airline technician. More recently, dozens of employees at a nuclear plant in India were apparently deliberately poisoned with tritium in their drinking water. The latter incident has been blamed on disgruntled employees; however, the possibility of a far worse scenario involving radicalized jihadist employees cannot be ruled out.

In addition to spreading terror, destruction and disruption in the short term, such attacks, in the view of the IEC and other Al-Qaeda affiliated terrorist groups worldwide, contribute to the long-term goal of collapsing the Western economy. A seven year strategy laid out by Al-Qaeda many years ago and reiterated in part several times includes sustained, long-term actions aimed at draining the Western economy as a whole.

Not Just the Jihadists

Unfortunately, it is not just jihadists who would like to collapse the Western world's economy. In the summer of 2009, a radical anti-globalist organization known as *Root Force* promoted what it calls "anti-infrastructure" actions.

Root Force seeks to "exploit weak points in the global economy and hasten the system's collapse," the group says, by supporting those fighting the development of highways, railways, ports, dams, mines, oil and gas pipelines, power plants, power lines and telecommunications cables. A specific focus for Root Force is infrastructure that provides access to resources in Latin America, "because the U.S. economy is particularly dependent on ... those resources."

The Root Force online and offline forums serve as a clearinghouse to provide specific targeting information for their supporters within North America. Root Force regularly facilitates intelligence sharing between all autonomous groups "working against infrastructure," as they put it.

In July 2009, TAM-C analysts noted the high significance of a Root Force communication pointing its supporters to a news item from 16 July 2009 about a rail line sabotage in Pennsylvania. The item was meta-tagged by Root Force with the keywords "Actions" and "Transportation," and was accompanied by a picture of a train bearing coal cargo.

SECTOR-SPECIFIC THREATS

Sector: TRANSPORTATION SYSTEMS

Attempted Hijacking in Yemen: Jihadists Are Watching

In a recent incident in Yemen, a man armed with a pistol attempted to board a plane from Yemen to Cairo, Egypt. However, local security officers identified and intercepted him before he could carry out the hijacking.

Of interest is that this incident was noted in jihadist communications - although there was no indication of a nexus to terrorism - indicating that the jihadists are continuously seeking tactical intelligence from world events apparently unrelated to the global jihad.

********ANALYSIS********

In this specific case, the focus on an attempted hijacking dovetails with previous jihadist communications intercepted by TAM-C analysts that involve the targeting of mass transit and aviation.

Reviewing the overflow of recent jihadist intelligence sharing in November, TAM-C analysts noted:

1. Discussion of security methods on airplanes and in airports indicates a continuing prioritizing of attacks on aviation.
2. Communications suggested the return to the use of aircraft in suicide attacks.

Several identified communications suggested the targeting of military bases in zones of conflict; however the tactics mentioned can be used by jihadists anywhere.

Sector: GOVERNMENT FACILITIES

Reaction to the Obama Surge
Initial jihadist reaction to the military "surge" recently decided upon by US President Barack Obama includes a call for Muslims to realize that "jihad is the best solution."

A recent Islamist communication said, in part: "This is a wake-up call for all the jihad warriors to get out of their coma and start jihad actions, because jihad is the best solution."

********ANALYSIS********

TAM-C analysts suggest that the U.S. decision may inspire and motivate further attempts to commit terrorist attacks as a response, or retaliation. Targets would not necessarily be limited to Afghanistan or overseas.

Targets that have been identified in past by Al-Qaeda and its affiliates could become the first targets of a more extensive campaign. TAM-C analysts note that it is significantly easier for jihadist cells - lone-wolf or otherwise - to target police officers or military bases (cf. Ft. Hood) in Western states than it is to fight the Marines in Afghanistan.

National Guards, FEMA Camps, Trains Worry Right-Wing Extremists
Large-scale property thefts at Fort Indiantown Gap last month included the worrying disappearance of around 1,000 gallons of fuel from multiple points. The target of the theft was the 28th Aviation Brigade Armory.

In separate research, TAM-C researchers noted that certain militia groups and conspiracy-minded organizations and individuals have identified Ft. Indiantown Gap as a base for building a New World Order with United Nations forces training there, and what they believe are other indicators. They claim the military is practicing using roadblocks and procedures for detaining "political dissidents" in the Ft. Indiantown Gap area.

********ANALYSIS********

The theft from Ft. Indiantown Gap may be a simple property crime, although a relatively impressive one; however, TAM-C analysts point out the potential uses of the quantity of stolen fuel for explosive devices or in combination terrorist attacks.

TAM-C researchers have identified two "persons of interest" in connection with conspiracy theorists focusing on Ft. Indiantown Gap; however, there are no indicators at this time that either of these two individuals, nor their followers, pose a threat in relation to the 9-11 December 2009 activity planned at Ft. Indiantown Gap.

Adversarial intelligence gathering has included Ft. Indiantown Gap, United Nations forces allegedly training at FIG, as well as "Norfolk Southern Railways in Lebanon" and nearby public transportation. The TAM-C recommends that registration information, driver's licenses and descriptions of vehicles owned by active, hostile members of adversarial groups, should be provided to security personnel as needed at Ft. Indiantown Gap, as well as at Norfolk Southern Railways.

Sectors: GOVERNMENT FACILITIES AND ENERGY

PA Group Announces First 'Direct Action'
Pennsylvania's Keystone Environmental Youth (KEY) Coalition has announced its first "coordinated direct action", as they called it. It is scheduled for 12 December 2009, in line with "an international day of action focused on the climate negotiations in Copenhagen" (7-18 December 2009).

The KEY Coalition sees itself as "educating ourselves and the public on Pennsylvania's contribution to global climate change."

********ANALYSIS********

The Keystone Youth Coalition has a very short history (formed in fall, 2009). Analysts of the Targeted Actionable Monitoring Center (TAM-C) note that, until now, KEY has been part of "Power Shift," a campus educational and advocacy group. Their programs have been aimed at mobilizing university students to pressure law makers into making environmentally sound decisions.

While their brief history points to the use of lawful picketing, it is unknown if any of the self-identified "Keystone Environmental Youth" members have attended (or will attend) such recent training as the climate camps in West Virginia or the current Ruckus Society training in New York (4-6 December 2009). Those KEY members who attend such training will have learned far more radical "direct action" tactics.

As noted in previous Pennsylvania Actionable Intelligence Briefings, targets most likely to see direct actions during the COP15 will be linked to the production and use of carbon-based energy – from the extraction, transportation, and use of coal to the corporations that provide financial support of those industries.

No actionable intelligence at this time for the following sectors:

AGRICULTURE AND FOOD
DEFENSE INDUSTRIAL BASES
HEALTHCARE AND PUBLIC HEALTH
NATIONAL MONUMENTS AND ICONS
WATER
CHEMICAL
COMMERCIAL FACILITIES
CRITICAL MANUFACTURING
DAMS
EMERGENCY SERVICES
NUCLEAR REACTORS, MATERIALS, AND WASTE
INFORMATION TECHNOLOGY
COMMUNICATIONS
POSTAL AND SHIPPING

END-CLASSIFIED-TAM-C-

For additional information, please contact the TAM-C of the Institute of Terrorism Research and Response at: +1.215.922.1080 or info@terrorresponse.org

Working with organizations that refuse to surrender their domestic or international operations to terrorism

Ensure that you always receive the latest information from The Institute of Terrorism Research and Response. Add the e-mail address, "tamc@terrorresponse.org" to your personal address book.

This Intelligence report includes information from open and closed intelligence sources. Not all information is able to be verified; however, the TAM-C is actively evaluating the reporting to establish its accuracy and to determine if it represents a possible link to terrorism. If recipients have any additional or clarifying information, please contact the Targeted Actionable Monitoring Center (TAM-C) at +1.215.922.1080.

Actionable Intelligence Weekly Briefing® A general overview of actionable intelligence (upcoming events) used by directors of security and law enforcement managers to pre-plan their future operations. The Briefing is dispatched on Monday of each week by 1100 GMT to enable early planning of the upcoming weeks.

Threat and Hazard Monitoring (THM) A custom service meeting the needs for each client. With the assistance of our international analysts, this service identifies specific threats, hazards, vulnerabilities, and assets our team of native language speakers researchers and ground resources, are to monitor and forward on to the client.

For additional information regarding the Center's services or specialized customized research and analysis programs, feel free to contact us at: tamc@terrorresponse.org