PENNSYLVANIA ACTIONABLE INTELLIGENCE BULLETIN #20

TARGETED ACTIONABLE MONITORING CENTER

14 DECEMBER 2009

******

ACTIONABLE DATE REMINDERS

- **Current-18 December 2009:** The 2009 United Nations Climate Change Conference in Copenhagen. Climate activists are gearing up to stage protests across the globe. (Reported in 18 Nov 2009 PAIB)

- **Current-19 December 2009:** Jews worldwide are celebrating the holiday of Hanukkah. Jewish communal gatherings pose a high-priority jihadist target. (Reported in 11 December PAIB)

- **18 December 2009:** Muslims worldwide mark the first of Muharram, the Islamic New Year.

- **19 December 2009:** Protest and vigil calling for the closing of the Army Experience Center (AEC) at the Franklin Mills Mall in Northeast Philadelphia.

- **25-27 December 2009:** Salafi institution based in Philadelphia that published an article justifying death to those who criticize Islam, hosts its “Deen Intensive” (deen in Arabic means “religion”) event featuring a speech by a Damascus-based cleric. (Reported in 13 Nov 2009 PAIB)

SECTOR-SPECIFIC THREATS

Sectors: ENERGY; CRITICAL MANUFACTURING; TRANSPORTATION SYSTEMS; WATER; GOVERNMENT FACILITIES; INFORMATION TECHNOLOGY

Suspected Serial Sabotage Points to SCADA Vulnerability

A series of as-yet unexplained major railway disruptions have taken place in Queensland, Australia, in recent weeks. Hundreds of thousands of passengers were stranded due to computer malfunctions that changed signals across the rail network to safe mode, forcing train service to essentially come to a halt.

Police have been called in to investigate the cause of the disruptions, with speculation regarding the possibility of sabotage due to a labor struggle against privatization on the Queensland lines. The Rail, Tram and Bus Union called claims of sabotage "absolute nonsense" and blamed over-zealous safety regulations compromising maintenance schedules.

An internal investigation is being undertaken by the Queensland railway authority to examine the computer control room, its software and other vulnerabilities.

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

The Queensland incident points to the serious vulnerability to both computer hacking and insider sabotage in heavily centralized supervisory control and data acquisition (SCADA) systems, such as those used in many national infrastructure projects and in communication-based train control (CBTC).

For example, commuter and freight rail service was seriously disrupted on 21 August 2003 when a virus disabled the computer systems at the freight rail headquarters in Jacksonville, Florida. In October 2006, the SCADA system at a water plant in Pennsylvania was reportedly accessed through an employee's laptop via the Internet. In June 2008 an IT security company released an advisory identifying a buffer overflow vulnerability found in control systems for power and water utilities. One month earlier, an IT security magazine reported a vulnerability in SCADA systems in as many as one-third of the world's industrial plants.

TAM-C analysts believe that, while hostile elements - from jihadists to ethnic separatists to anti-globalist Anarchists - have carried out many physical attacks disrupting rail service in various countries, many such groups are also seeking ways to do serious damage to major infrastructure remotely and without immediate risk to the perpetrators. [Only the investigation will verify whether the Queensland disruptions were a case of outside penetration or insider involvement.]

In one recent incident in India, disgruntled employees were suspected of being behind a case of radioactive poisoning in a nuclear power plant. In another case, a former employee of an Australian sewer control plant was convicted of accessing the plant's SCADA system through his laptop in order to release 264,000 gallons of sewage into national waterways. While these cases implicated employees with personal motivations, the TAM-C notes that both jihadists and other terror groups have repeatedly recruited or intimidated infrastructure insiders to assist in their plans.

Specific insider threats to mass transit SCADA systems include the exploitation of access and network vulnerabilities to send "power off" messages to targeted equipment (suspected in the Queensland incident), to prevent communication between the control center and SCADA-linked devices on the rails, or to alter the information reaching human operators in the SCADA-based control center.

As necessitated by complicated modern infrastructure systems, SCADA networks are in use in many Pennsylvania facilities, including mass transit, energy and water.

Sectors: GOVERNMENT FACILITIES

Update From Egypt

A vehicle belonging to "a non-profit organization that helps the population" was attacked with live fire in northern Sinai on Friday. The organization was identified as an American NGO. Three NGO personnel were in the car along with their driver, but there were no casualties.

The car was on its way out of Cairo, on their way to El-Arish, allegedly to meet a police commander. Initial reports are that the vehicle was first physically blocked by the attackers, who opened fire when the driver managed to execute evasive maneuvers.

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

Most local reports have described the above event as a criminal incident. However, TAM-C analysts note a level of cooperation between jihadist groups and those elements involved in lucrative criminal enterprises (smuggling, narcotics, counterfeiting, piracy, kidnapping for ransom, etc.). Therefore, foreigners in Egypt may be singled out by criminal elements in collaboration with terrorist elements.

As stated in PAIB no. 18 (9 December 2009), TAM-C analysis indicates the potential for terror activity in Egypt - especially against high-visibility government offices, tourist sites and in the Sinai – is increased at this time. Pennsylvania students attending the American University in Cairo, Egypt (BEG) should be advised of the current increased danger of terrorist activity. Also vulnerable as targets for abduction or attack are those who travel in vehicles with markings indicating Western companies or organizations.

Sectors: ENERGY; CRITICAL MANUFACTURING

Learning to Apply 'Direct Action' Against the Coal Industry

Aggressive environmentalists will be attending what they are calling a Winter Action Camp in Rock Creek, West Virginia from 4-25 January 2010. The camp will permit 30 "campers" to learn the skills of aggressive environmentalism, including: "direct action" (which can include vandalism, obstruction of public and private venues, arson, threats of violence, assault, etc.); handling the media; legal support; action planning; and "other skills relevant for this campaign and future actions."

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

The immediate target of the Winter Action Camp training is the West Virginia coal mining industry. However, Targeted Actionable Monitoring Center (TAM-C) analysts point out that attendees at the camp and others who learn from them in the field will likely apply the skills and lessons learned in "actions" targeting coal operations in Pennsylvania, as well.

Sectors: DEFENSE INDUSTRIAL BASES; EMERGENCY SERVICES

'Civil Disobedience' at Lockheed Martin

The Brandywine Peace Community has announced a protest on Monday, 18 January 2009 (Martin Luther King Day) at the facilities of the Lockheed Martin Corporation in Valley Forge, behind the King of Prussia Mall. The group is opposed to defense industry companies such as Lockheed Martin.

Calling for "nonviolent resistance" and "nonviolent action", the organization is also promoting "civil disobedience" at the Lockheed Martin protest.

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

Analysts of the Targeted Actionable Monitoring Center (TAM-C) note that the Brandywine Peace Community is best known for the use of legal non-violent tactics. However, the above planned protest is being discussed in a more strident fashion than usual. Additionally, the organization appears to be seeking volunteers “interested in participating in the civil disobedience.”

TAM-C analysts advise local law enforcement and Lockheed Martin security personnel to be prepared for behavior that intentionally creates a confrontational environment. Expected unlawful behaviors may include the throwing of red paint or blood, trespassing on company property, and the attempted blocking of the facility’s gates.

.

No actionable intelligence at this time for the following sectors:

AGRICULTURE AND FOOD
HEALTHCARE AND PUBLIC HEALTH
NATIONAL MONUMENTS AND ICONS
BANKING AND FINANCE
CHEMICAL
COMMERCIAL FACILITIES
DAMS
NUCLEAR REACTORS, MATERIALS, AND WASTE
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