The Washington Times

Monday, June 22, 2009

Taliban averts a acks with U.S. equipment

Eli Lake (Contact)

Some Taliban fighters have been able to ward off a acks by U.S. aircra by wearing special infrared patches on their shirts that signal that they are friends rather than foes.

The patches, which can also help suicide bombers get close to U.S. targets, are supposed to be the property of the U.S. government alone, but can be easily purchased over the Internet for about $10 each. Also available online: night-vision goggles and military-grade communications systems like the ones used by the terrorists who a acked the Indian city of Mumbai last year.

While stealing uniforms is as old as warfare itself, the Internet has made purchases of military equipment much easier and increased the risk to U.S. forces in Iraq and Afghanistan.

Some of the patches have been stolen during raids on U.S. resupply convoys in Afghanistan and Pakistan. But they can also be purchased in the United States and sent overseas with li le detection.

In a recent investigation, the U.S. Government Accountability Office (GAO) bought patches using fake names and a front company with only a valid credit card. The patches reveal an American flag when looked at with an infrared light and were designed to avoid friendly fire during nigh ime ba les.

Jonathan Meyer, assistant director of forensic audits and special investigations for the GAO, told The Washington Times, "Based on our conversations with the Department of Defense, terrorists have used U.S. uniforms and the infrared patches to get close to U.S. and allied forces on the ba lefield and at bases. This is more of a potential suicidebomber risk."

Mr. Meyer helped lead the GAO investigation, which concluded that few regulatory controls exist for dual-use and military technology sold domestically.

Rep. Bart Stupak, Michigan Democrat, who chairs the House Energy and Commerce oversight and investigations subcommi ee, said the infrared patches are also made in China.

"It is rather simple technology," he said. "We not only sell this to domestic people here, and they sell them to anybody, but you can get them from China, and the Chinese will sell them to others.

"They have been used by the enemy in the war. It's of grave concern because you don't know who is friendly or not," Mr. Stupak added.

Newsweek magazine first reported in 2007 that 4,800 such patches had been sold inadvertently in 2006 to 23 U.S. and Canadian companies by an Arizona-based company, Government Liquidation. The patches were still sewn onto uniforms that were sent out.

The GAO was able to purchase the patches from a New York-based military-supply dealer, but did not identify the seller's name.

"An enemy fighter wearing these [infrared] flags could potentially pass as a friendly service member during a night combat situation, pu ing U.S. troops at risk," the June 4 report said. "Nevertheless, these items are completely legal to buy and sell within the United States."

The report followed up on a 2008 GAO study that exposed the fact that military-surplus items, such as spare parts for fighter jets, could be purchased on eBay and Craigslist. That same year, an NBC team also was able to procure the infrared patches and have them sent to a mailing address in Amman, Jordan. Earlier, the Associated Press reported that F-14 spare parts had found their

way to Iran from U.S. suppliers a er the Pentagon sold the equipment to military wholesalers.

Rep. Brad Sherman, California Democrat and chairman of the House Foreign Affairs subcommi ee that deals with export controls, said that it may be time to treat the infrared patches as a munition that would need to be controlled through the Arms Export Control Act.

"If there is an item that has only a military use, like the patches, the fact that they are nonlethal doesn't mean we should not treat them as munitions," he said. "The term 'munitions' perhaps should apply to anything that does not have a legitimate civilian use."

However, a retired four-star general, Jack Keane, said the risk had been overstated.

"Since the beginning of warfare, people have been dressing up as the enemy to infiltrate," he said. "We certainly have done this in the past to our enemies, and our enemies have done this to us."

Mr. Keane, who played a key role in developing the counterinsurgency strategy for Iraq, added, "There are other safeguards in addition to [these patches]. A visual identification and other identification is in the soldier's possession. There are multiple things that are being checked. When it comes to the tactical situation, infrared certainly helps identify where we are, but there is also a dialogue that is taking place describing the situation."

But "it would seem to me that something we are using to help identify ourselves should not be available to the general public, and it should be something that is only acquired through military channels," Mr. Keane said.

Lt. Col. Patrick Ryder, a Pentagon spokesman, said the military was reviewing the GAO report.

"The Department of Defense takes force protection very seriously. As a ma er of course, we are concerned any time sensitive equipment has the potential to fall into enemy hands," he said.

Other items acquired from U.S. companies by the GAO included a "triggered spark gap," a specialized medical component the size of a spool of thread that is also a necessary component for detonating a nuclear weapon. The investigators were also able to purchase an oscilloscope and an accelerometer, important gauges for measuring elements of nuclear explosions.

David Albright, president for the Institute for Science and International Security, a Washington think tank, said the triggered spark gap "can be used in a nuclear weapon to fire high explosives and compress the nuclear core." He added that this sensitive item, whose medical use is to dissolve kidney stones, has shown up in the nuclear programs of Pakistan, North Korea and Iran.

The GAO concluded that "sensitive dual-use and military technology can be easily and legally purchased from manufacturers and distributors within the United States and illegally exported without detection."

At issue is a loophole in the U.S. arms-export control regime. Many kinds of dual-use items would require licensing and an end-user certificate - specifying the ultimate purchaser - if sold to a buyer overseas. But no such safeguards exist if the buyer is in the United States. It is also relatively easy to send sensitive equipment purchased in the U.S. to foreign countries through the mail.

Ed Timperlake, a former senior technology official in the Defense Department and an expert on what is known as "defense critical assets," said the loophole for domestic sales of sensitive technology is a counterintelligence risk.

"There are a lot of Chinese espionage agents and others grabbing anything they can, anything they can find. And with our free market they can find a lot," he said.

Mr. Timperlake added, "The GAO report is fair, and everyone I worked with knew their mission had life-and-death consequences, especially for troops in combat. The issue really comes down to more resources" for the FBI and other agencies.

A former U.S. undersecretary of commerce for industry and security, Mario Mancuso, said he did not find it surprising "that many of these items can be easily sold in the U.S."

"It would have been a more balanced report if the GAO had highlighted the many legitimate commercial uses these items have," he said. "This is important because, in my experience, most manufacturers are not trying to equip U.S. adversaries or turn a blind eye to illicit procurement efforts."

A spokesman for the Justice Department's National Security Division, Dean Boyd, said that since October 2007, the U.S. government has created 20 counterproliferation task forces to look at the issue.

Mr. Stupak said, however, that "no one is really taking responsibility" in the U.S. government for dealing with the problem.

The National Security Council, the State Department and the Department of Homeland Security have declined comment on the GAO report.

Ma hew Borman, acting assistant secretary of commerce for export administration, said, "We are currently reviewing the findings in the GAO report, and we are always looking for ways to improve interagency cooperation. We know an effective export-control system requires a combination of domestic and international activities to educate parties on their export-control responsibilities, proactive compliance efforts and the conduct of enforcement investigations. We are commi ed to protecting U.S. national security, foreign-policy and economic interests by ensuring secure trade in high-technology items."