

# TRANSNATIONAL THREATS UPDATE

Volume 7 • Number 9 • Holiday Issue (November–December 2009)

*“Globalization has broadened the number of threats and challenges facing the United States...The nation requires more from our Intelligence Community than ever before and consequently we need to do our business better, both internally, through greater collaboration across disciplines and externally, by engaging more of the expertise available outside the Intelligence Community.”*

—The Honorable J. Michael McConnell, Director of National Intelligence, Statement for the Record to the Senate Select Committee on Intelligence, February 27, 2008

<b>CONTENTS</b>	
<b>Terrorism</b> .....	<b>1</b>
<b>Illicit Trafficking</b> .....	<b>3</b>
<b>Organized Crime</b> .....	<b>4</b>
<b>Technology</b> .....	<b>5</b>

## Terrorism

### Domestic Radicalization Gaining Ground?

“[T]hey know that 15 young Saudi males are not going to get into the United States on one-way visas to do flight training...What they need are people who are not going to arouse any suspicion when they arrive at JFK, or LAX or Washington-Dulles.”<sup>1</sup> So says former CIA officer Bruce Riedel, commenting on the enhanced security in the United States following the 9/11 attacks. Unfortunately, there is a way around even the most stringent screening measures of foreign nationals entering the United States: have a green card or, better yet, an American passport.

This threat has manifested itself as a possibility in more than 20 cases since 9/11, and at least a dozen in the past year. Afghan immigrant and legal U.S. resident Najibullah Zazi, Palestinian-American Major Nidal Hasan, and 14 Somali-Americans in Minnesota were the most worrisome stories of the first three quarters of 2009, and now they are joined by a new name: David Coleman Headley.

Headley combines elements of all three cases. Like Zazi, the Pakistani-American Headley is South Asian

(not Arab). Like Hasan, he was born in the United States, making him a full American citizen. He then moved to Pakistan where he was educated in a military academy. And like the Somali-Americans, Headley is accused of plotting attacks outside, not within, the United States. This curious combination represents a nightmare for Western authorities. Although Headley’s particular plots were foiled, and even Major Hasan’s attack was not particularly deadly compared to other events in the sordid history of terrorism, this unique threat could be orders of magnitude worse in the future.

As Riedel explains, ““We’ve known for several years that Al-Qaeda and its allies like Lashkar-e-Taiba (LeT) have put a high priority on recruiting assets in the Pakistani communities in the United States, the United Kingdom, and the rest of the world.” It is easy to see why. Headley, who changed his name from Daood Sayed Gilani in 2006, was able to “travel freely” in and out of the United States more than a dozen times, according to the *Wall Street Journal*. *Time* magazine reports that he cased the Danish newspaper *Jyllands-Posten* (publisher of the controversial cartoons of the Prophet Muhammad in 2005 and 2006) for an attack that never materialized, but his primary contribution was the thorough reconnaissance he provided in Mumbai. Crisscrossing the city without arousing suspicion during 2006–2008, Headley scouted and videotaped the targets that were attacked last November and landing sites for the infiltrators’ boat. This took place before LeT leaders had assembled or trained the actual assailants, ensuring that Headley and the attackers would be insulated from one another in case of a security breach. Although this attack took place outside the United States, there is no reason why a U.S. passport holder would not be able to play a similar role

with regard to American targets. And as the article below will detail, there is evidence that LeT is attempting to ensure that there are more David Headleys in the future.

### **Russian Terrorism**

On November 27, the Russian luxury train the *Nevsky Express* was attacked by terrorists for the second time in two years while traveling from Moscow to St. Petersburg. A bomb planted under the train tracks detonated, resulting in 27 deaths and about 100 injuries. The following day, a second bomb was detonated at the site of the derailment, but was far less powerful. No injuries were reported following the second attack.

The incident was immediately treated as an act of terrorism even before it became apparent that the derailment was caused by bombs, due its similarity to the previous attack two years before. Bomb experts found that the second device was remote control-activated and targeted the investigators at the scene of the derailment. However, an unknown malfunction appeared to have occurred, as none of the numerous officials in the vicinity were injured.

Several groups jumped to take credit for the attacks. A far-right terrorist group known as Combat 18 claimed responsibility on one of their Web sites, but after the details emerged about the sophistication of the bombs, they were quickly written off. An official from the Federal Security Service of Russia (known as the FSB) official said that Combat 18 simply did not have the capacity to create an attack of this caliber. The most likely perpetrators are the Northern Caucasus Islamist insurgents known as Caucasian Mujahadeen. Members of their group were recently found guilty for the nearly identical bombing of the same train line two years before. The Caucasian Mujahadeen claimed that this assault was one in a number of systematic attacks on Russian infrastructure.

Experts note that because of the clientele (mostly high-ranking government officials and businessmen), this line is strategically significant for insurgents. Indeed, several of the 25 people killed were government officials, executives, or chairmen of major energy and infrastructure companies.

The Russian government has responded with a full-fledged investigation. Several criminal cases have been opened, and a widespread manhunt has begun for the

four main suspects in the case. A kilometer of train tracks had to be replaced and four cars were damaged.

### **Saudi Arabia Brings the Heat to Yemen**

In early November, the Saudi military began a campaign against Houthi fighters in northern Yemen. According to Human Rights Watch, Riyadh upped its involvement following cross-border raids by the Houthis on November 3. The Saudis retaliated that day with ground and aerial attacks and have continued their offensive since. Deteriorating conditions in southern Yemen and alleged Iranian involvement in the north appear to exacerbate the chaotic situation. Meanwhile, increased international attention has brought the focus onto the al Qaeda hotbed. The effect of the Saudi presence in the north has yet to be determined.

Despite Iranian and Houthi claims that the Saudi military has been actively involved in the conflict for months, official reports show that Saudi Arabia started monitoring its southern neighbor after the Houthi separatist movement in northern Yemen turned violent in 2004. However, in October, tensions heightened when several Saudis were killed along the border while attempting to smuggle suicide vests and other goods across the border. Then, in the aforementioned thrust in early November, the Houthis tried to occupy two Saudi villages and killed a Saudi border guard. That was impetus enough for the Saudis.

At the beginning of the offensive, thousands of Saudi villagers were warned to evacuate the region. By November 14, 240 villages were told to evacuate as the fighting spilled over into Saudi Arabia. Similarly, the Saudi forces appear to have attempted to evacuate Yemeni villages before they began their assault on the embedded Houthi fighters. There have been no updates on the number of internally displaced Saudis, but up to 125,000 Yemenis have been displaced since the beginning of the Houthi insurgency.

### **Lashkar-e-Taiba Goes Global**

The November 2008 Mumbai terror attacks vaulted the Pakistani militant group Lashkar-e-Taiba (LeT) into the global spotlight. At the time, LeT's activities were focused almost entirely on its operations in India, Kashmir, and Pakistan. The State Department's 2008 report on terrorist organizations described LeT exclusively in South Asian terms, and a Reuters profile from December 2008 says only that the group "made its name fighting Indian rule in Kashmir...[and seeks to]

Islamicise South Asia and to end Indian rule of Muslims in Kashmir.” LeT’s reputation seems to be evolving, however, as a growing chorus of analysts now describe the group as “going global.”

Terrorism analyst Evan Kohlmann has described LeT as a “stepping stone” to global jihad, noting that abundant training facilities, English-speaking recruiters, and links to militants worldwide make LeT “the best way for emerging jihadists to get trained.” Juan Zarate, the former deputy national security adviser on combating terrorism in the Bush administration and senior adviser at CSIS, says the United States is concerned about “LeT having a global platform” and now recognizes that the group is “no longer just India’s problem.” Former French investigative magistrate Jean-Louis Bruguiere goes the furthest, telling Reuters that “Lashkar-e-Taiba is no longer a Pakistani movement with only a Kashmir political or military agenda. Lashkar-e-Taiba is a member of al Qaeda. Lashkar-e-Taiba has decided to expand violence worldwide.”

LeT denies the accusation that it is targeting the West, and there is no unclassified evidence of specific plots against America. In fact, while there is significant proof of LeT operations in the United States, the majority of the evidence seems to point to recruitment efforts to send Westerners abroad to carry out LeT attacks. Still, it is indisputably a dangerous development that, according to national security expert Noah Schachtman of *Wired* magazine, “Since 2003, at least five U.S. citizens have been convicted in federal court of conspiring to provide material support to Lashkar-e-Taiba. At least nine more men, considered to be in the same larger circle, have been convicted of firearms violations and other felonies.” At a bare minimum, these men could exploit their American passports, like David Headley, to conduct more effective operations in India than would otherwise be possible. This would undermine U.S. interests even if it does not threaten the United States directly. Moreover, there is certainly no logical reason that Americans who trained with LeT could not attack the U.S. mainland if they so chose. Being forced to rely on the good graces of a group accused of murdering hundreds of civilians in cold blood is hardly reassuring.

### **Political Violence in the Philippines**

Elections in the Philippines are notoriously violent. To combat the political violence that has already exploded across some parts of the country, the government has issued a gun ban ahead of the May 10 elections. The ban states that only uniformed police officers are allowed to

carry firearms. In fact, the first arrest made under the gun law was of an off-duty policeman. To implement the gun ban, hundreds of check points have been created around the country, are manned by thousands of police officers.

This gun ban is the result of a scramble by officials to bolster security after a massacre of a political entourage. On November 23, a convoy of about 60 political activists from an opposition party and journalists were surrounded by about 100 gunmen in the Maguindanao province. Reports initially announced that 21 people were brutally tortured and murdered. The toll would later rise to 57. Among the dead were 34 journalists and the wife, aunt, and sister of Deputy Mayor Ismael Mangudadatu of Buluan Township. The wife of the deputy mayor called him to say that their bus had been pulled over by 100 uniformed guards, which led Mr. Mangudadatu to accuse Governor Andal Ampatuan Sr. of responsibility for the brutal attacks. On December 1, 2009, Governor Ampatuan was arrested with several counts of murder and for his role in the massacre.

In the chaos that followed, President Macapagal-Arroyo declared a state of emergency for the province from November 24 to December 13. During that time, three members of the Ampatuan clan were removed from public office, and several of their armories were raided. Andal Ampatuan Jr. was arrested with 57 counts of murder and his personal warehouse revealed a daunting stockpile of weapons, including 330,000 rounds of live ammunition, armored military vehicles, and enough weapons to arm an estimated 500 people.

The Philippines have suffered under a great deal of political violence for several decades. The south, although recently given more autonomy, is filled with strife from several competing clans. There is also an Islamist insurgency that has claimed the lives of almost 120,000 people in the past few decades. Now that the Ampatuan clan has had their leadership structure decapitated and their grip on the southern government drastically weakened, the elections could lead to an even greater upheaval in coming months.

## **Illicit Trafficking**

### **Thai Authorities Make Arms Trade Bust**

On December 12, Thai authorities acted on a tip from U.S. intelligence officials and impounded a plane in Bangkok that arrived from North Korea. The crew was detained when 12 crates of weapons weighing roughly

35 tons were found in the cargo. They were formally arrested and charged with possession of weapons and ammunition without a license. The crew maintains that they were unaware of the contents of their cargo, yet the suspicious details surrounding them and their activities imply otherwise.

The plane left the Ukraine on December 8 and landed in Pyongyang after refueling in Bangkok. By December 11, authorities were tipped off that it would be once again refueling in Bangkok on its return trip. The flight's next leg would have been Colombo, Sri Lanka, then on to the United Arab Emirates. The pilot, Mikhail Petukhov, said that the plane was to be off-loaded in the Ukraine again. However, the Ukraine is still not necessarily the final destination for the weaponry. Some officials believe that the flight pattern may have been intentionally misleading, with Sri Lanka, the Middle East, or even Iran as possible unloading points.

Adding further complexity to the situation is the plane and flight crew. The plane was from Kazakhstan, but was sold to a Georgian private airline company, Air West Georgia. The Georgian company is claiming that the plane was leased to a company in New Zealand. The crew is made up of four Kazakhs and a Belarusian. The Kazakhs all apparently work for a Kazakh airline but were on leave without pay. The crew insists that they were under the impression that the cargo was just oil refinery equipment and refused to provide information on the buyers. One crew member likened their situation to truck drivers not necessarily knowing the contents of their cargo. Petukhov admitted to having made this trip three or four times.

Although the exact contents of the shipment have been kept quiet, Lt. Gen. Thangai Prasajaksattru of Thailand stated, "There were a lot of weapons such as rocket-propelled grenades, missiles and other war weapons."

The shipment confirms a widely speculated source of income for North Korea. The CIA *World Factbook* puts military products as the hermit nation's main industrial output. Despite UN sanctions, experts estimate that the arms trade brings in about a billion dollars a year for North Korea, likely funding its nuclear weapons program. However, because the weapons trade is illicit, North Korea's clientele remains a mystery. This is the second shipment since August to be captured containing North Korean weapons. Dubai intercepted a shipment of detonators and ammunition destined for Iran.

Incidentally, those freights were also labeled as drilling equipment.

## **AQIM Runs Drugs to Europe**

Three arrests in Ghana have brought the convergence of the War on Drugs and the War on Terror. Oumar Issa, Harouna Toure, and Idriss Abelrahman—all nationals of Mali believed to be in their 30s—are being called the first clear link between al Qaeda and transnational drug trafficking by the U.S. Drug Enforcement Administration (DEA). Prosecutors in New York accuse the men of offering to protect South American drug shipments from the Revolutionary Armed Forces of Colombia (FARC) as they transit western and northern Africa on their way to Europe. The men planned to use the revenue from their cut of the shipment to fund operations for both al Qaeda in the Islamic Maghreb (AQIM) and al Qaeda central. West Africa has been under increasing scrutiny for its role as a transit point for Europe-bound drugs since a UN Office on Drugs and Crime (UNODC) report in 2007. CSIS wrote about these issues in the June 2009 TNT Update and in a November piece for the Africa program.

According to the criminal complaint recently filed against the men, Harouna Toure told an FBI confidential source posing as a Lebanese anti-American radical with connections to FARC that "[Toure's] assistance would be needed to secure safe passage from Mali to Morocco." Toure went on to say that he and his men have a "strong relationship" with other al Qaeda groups in North Africa, and that they had jointly engaged in smuggling Bangladeshis, Pakistanis, and Indians to Europe, in addition to drugs.

The men are being charged with "Narco-Terrorism Conspiracy" and "Conspiracy to Provide Material Support to a Foreign Terrorist Organization."

## **Organized Crime**

### **Kingpin's Death Leaves Wake of Violence**

The leader of one of the most powerful Mexican drug cartels was killed during a police raid on December 16. Marcos Beltran Leyva, known as the "boss of bosses" or "the ghost" throughout Mexico, was considered the kingpin of the Beltran Leyva cartel. He was one of the five brothers running the cartel, which controls a significant smuggling route up the west coast of Mexico.

According to a Stratfor study, the Beltran Leyva cartel is one of the most sophisticated criminal organizations in Mexico. The report said that it had managed to infiltrate all levels of the Mexican government. U.S. officials have stated that the cartel has smuggled in millions of dollars worth of cocaine and heroin into the United States. The cartel has also carried out notorious assassinations and acts of brutality. In one particularly vicious instance, 15 men with machine guns killed the son of a rival drug lord in the middle of a shopping center in broad daylight.

The Beltran Leyva cartel gained much of its power through strategic relationships and by moving in on territory lost by dismantled or weakened cartels. Now that Marcos is dead and three of his five brothers have been arrested, the remaining brother, Hector, is the only remaining head of the cartel.

Due to the power grabbing expected in the coming days and weeks, Mexican authorities were preparing for increased violence. However, they were unprepared for the drastic spike in murders and violence. By January 10, 2010, Mexican sources reported that 283 people had been killed by drug-related violence since the start of the year, more than twice the number of killings during that same period in 2009.

## Technology

### Drone Disaster?

The Pentagon has been forced to acknowledge a major security breach after the *Wall Street Journal* reported that militants battling U.S. forces in Iraq and Afghanistan have been intercepting videos transmitted between American drone and U.S. ground forces in the two theaters. Although the exact details have yet to emerge, defense officials told the *Journal* that captured Iraqis had been found to have "days and days and hours and hours of [footage]" from U.S. aircraft on their laptops.

This baffling problem is rooted in the networked nature of modern warfare. The ballyhooed technological Revolution in Military Affairs (RMA), which reached a fever pitch during the Rumsfeld era, leveraged advances in computers, information technology (IT), and satellites to enhance the way the U.S. Armed Forces fight. New technologies have made ordnance more accurate (smart bombs), shown U.S. forces almost exact locations for themselves and adversaries (using GPS), and beamed

real-time intelligence across the globe from an increasingly diverse array of platforms.

This particular scandal centers around pilotless aircraft called Unmanned Aerial Vehicles (UAVs), often referred to as drones. They have been providing high-resolution, real-time surveillance to senior commanders for years, and recent technological innovations have brought their images directly to the frontlines. Through a hand-held device called the "Remotely Operated Video Enhanced Receiver," or ROVER, ground combat units and fighter, bomber, and helicopter pilots can now view the same video feeds that drone operators and headquarters staff can see. Unfortunately, because the data links that transmitted the information from the air to the ground are not encrypted, America's adversaries seem to have been benefitting from the information as well. It seems America's enemies from Iraq to Afghanistan were watching the same video that U.S. troops were, thanks to \$25.95 programs "such as SkyGrabber, from Russian company SkySoftware... developed to intercept music, photos, video, programs and other content that other users download from the Internet." *Wired* magazine's national security blog *Danger Room* compares these electronic intercepts to eavesdropping on police communications with a radio scanner. Smaller aircraft are especially vulnerable, as they "broadcast their surveillance footage constantly and in every direction," unlike some larger aircraft that can turn their feeds on and off. This allows anyone within "line of sight" of the aircraft to listen in on their unsecured networks with even rudimentary electronic scanners.

The fallout from this developing story is only beginning to emerge, but this scandal will have far-reaching implications. Already there is talk of multimillion dollar security upgrades that will take years to install, and that occurs against a backdrop of Pentagon denials that any serious harm resulted from this breach.

### Did Citibank Get Hacked by the Russian Mafia?

The *Wall Street Journal* reported last month that the Federal Bureau of Investigation (FBI) and Citigroup were working together to combat the hacking spree that cost the bank tens of millions of dollars. While many details of the investigation are vague, all signs point to a Russian cyber crime syndicate named Russian Business Network (RBN) being responsible for the robbery.

Multiple sources point to a specific piece of software known as Black Energy that was developed by a Russian

hacker. Black Energy is specifically designed to steal account log-on data and bank credentials and create denial-of-service attacks. In one known case where a man was robbed of more than \$1 million, the software was Citibank-specific.

In that case, all the funds were siphoned to Latvia and the Ukraine. The *Journal* pointed out that similar disruptive attacks that used Black Energy were launched against Georgian banks and firms during the 2008 conflict and against a political opponent to Putin while he was president.

RBN allegedly fell off the radar around 2007. However, the group appears to have reemerged smaller but with the same malicious goals as before: to hack businesses, banks, and any opposition Web site. These activities appear to earn up to \$150 million per year, and RBN even offers its services at a low cost of \$600 per month. The group appears to be based out of Riga, Latvia. Web sites monitoring RBN claim that one of the leaders of the group is related to a high-ranking Russian politician, leading some to believe that the attacks on Georgia and the politician weren't hacktivism, but rather contracted aggression.

---

**This update is produced by the Transnational Threats Project at the Center for Strategic and International Studies (CSIS) and provides monthly news on terrorism, drug trafficking, organized crime, money laundering, and other transnational threats. The *TNT Update* draws primarily on international media sources, including the Associated Press, ITAR-TASS, Agence France Presse, Reuters, Xinhua News Agency, World Tribune, Afghan News, and others.**

**CSIS does not take specific public policy positions; accordingly, all views, positions, and conclusions in this publication should be understood to be solely those of the author(s).**

**© 2010 by the Center for Strategic and International Studies. All rights reserved.**

---