Defeating Terrorist Support Structures After Mumbai III

by John Solomon - Global Head of Terrorism Research at World-Check

WORLD-CHECK

This is the third report of a three-part series addressing the terrorist structures involved in the November 2008 Mumbai attacks.

The first report provided an initial summary of the attacks with an emphasis on operational support. The second report examined the structure of Jamaat-ud Dawa (JuD), the non-profit arm of Lashkar e-Tayyiba (LeT), the terrorist group believed to be responsible. This report addresses the vulnerabilities that LeT/JuD exploited in the private and public sectors. In addition, the article assesses whether JuD will survive the ban the UN imposed on it on 10 December 2008.

Private sector

The most obvious vulnerabilities exploited by the LeT terrorist cell involved in the Mumbai attack include telecommunications and hotel security. That the mobile phone has revolutionized the way people interact across cultures, regions and socioeconomic levels is well-known. In South Asia and other parts of the developing world, inadequate fixed line and limited Internet access and computer use make the use of mobile phones even more important than in the developed world. Not shocking then perhaps is the fact that the 20-something terrorists that attacked Mumbai availed themselves of a range of mobile phone and other telecommunications technology. This connected them electronically to their handlers; enabling remote, real-time operational intelligence and instructions to be exchanged during the attack.

The Mumbai cell made use of mobile phones. The terrorists not only stole mobile phones from hostages, they also took steps to acquire SIM (subscriber identity modules) cards anonymously months before the attack. According to media reports, for example, the support network bought at least 37 SIM cards mostly from Kolkata in India using fake identification. The support cell then reportedly sent the SIM cards to Pakistan via Kashmir. The SIM cards carried the fake names of the individuals and also functioned as prepaid phone cards with credits of US$100 authorized. The use of prepaid cards is generally worrisome with regard to terrorist financing because anonymously bought cards may be used to withdraw cash from ATMs.

The terrorist cell's handlers, believed to have been based in Pakistan, also made use of VOIP (voice over Internet protocol) technology to communicate. VOIP enables users to create virtual phone numbers in many countries around the world irrespective of the physical location of the user. The handlers intended to conceal their identities and locations through the use of this technology. In this case, an individual calling himself "Kharak Singh" from India set up a US-based number through Callphonex, a VOIP service, and paid for it with a moneygram, which was probably bought using another fake ID. In addition, Indian investigators have indicated in the government's official dossier that the support cell used Western Union to pay Callphonex approximately US $230 for five Austrian direct dial numbers via an Italian agent. Although Callphonex inquired into why the payee, a purported Indian named Javid Iqbal, would have a Pakistani identification number and residence, it approved the transaction and did not investigate further.

Another vulnerable point within the private sector was the level of security present at the Taj and Trident hotels. Reports, still unverified, indicated that parts of the terrorist cell's support structure had infiltrated the hotels variously as employees and guests. Al-Qaeda's New York City landmarks plot also involved the reconnoitering of targets though infiltration as hotel employees. Since there has been a hardening of security at embassies around the world, softer targets like luxury hotels, which often host diplomats and other VIPs, have become higher value in the eyes of terrorist planners. The September 2008 al-Qaeda attack on the Marriot hotel in Islamabad, Pakistan, that killed more than 50 people and injured 100s more, is another illustration of this trend. In that instance, for example, one of the support cells allegedly checked into the hotel in order to gather intelligence on the security in place. Moreover, like the Taj and Trident hotels, the Marriot in Islamabad constituted an attractive, softer substitute for an embassy because of the high profile diplomats, VIPs and others that frequented it.

Public sector

From an operational perspective, the clearest breaches in the Indian government's security framework took place at sea and

port. The attack planners identified Indian capabilities in maritime and port security as a critical weakness and moved to exploit them. With hardened security procedures at border crossings and airports, the 7500 kilometers of coastline, nearly 200 ports, and inadequate coast guard presence, the maritime entry point seemed the most attractive. The risk of detection may have been perceived to be lower and the ability to access weapons was made easier by a seaborne entry into Mumbai.

The terrorists took a circuitous route, based on the evidence provided by their GPS devices. The terrorists embarked on a 500-mile journey from Karachi, Pakistan's largest port, to Mumbai. The trip entailed changing vessels three times, which included the hijacking of an Indian fishing ship the murder of its crew. The entry to Mumbai was then made via an inflatable boat. Port security was not alerted.

Implications

Much can be said about the need for the private sector to take on a greater share of responsibility for doing its part to create a strategic counterterrorism environment. Banks have undertaken a greatly expanded role in this regard since 9/11, when the UN, the US, the UK and the EU adopted a more robust sanctioning program to address international terrorism. To combat terrorist and its support networks, it is past time for these same regulatory requirements to be had by other critical sectors of the economy. Telecommunications is one such key sector. While hindsight is always 20-20, it is indeed worthwhile to probe why more due diligence was not done on "Javed Iqbal" when the information given did not make sense. The same is true with the hospitality industry. Terrorist movements have selected this industry as a key target and will continue to do so in the months and years ahead; therefore it is necessary for this industry to improve its security policies and to take appropriate countermeasures.

The Indian government undoubtedly recognizes its maritime vulnerabilities as does its neighbor Pakistan. These governments will likely take the right steps in improving their capabilities on this front. While the breaches in the private and public sectors both seem clear, it is equally clear that more needs to be done to not only tactically but also strategically to address the issue of wide terrorist support networks and infrastructure in place. The UN Security Council, therefore, took the correct step in banning JuD, the non-profit wing of LeT that allegedly was the recruitment vehicle for some of the Mumbai terrorists. And credit must be given to the Pakistani government as well for its meaningful response.

The Pakistan government has responded by cracking down on JuD, closing its camps and arresting 100s of its leadership and administrators. The government also took over the organization's headquarters and 75-acre compound known as Markaz-e-Tayyiba in Muridke. Indeed the right sounds are coming from Islamabad, but the Indian government has unsurprisingly indicated that the Pakistani side should do more. Although Pakistan has been responsive to the UN's addition of JuD, the past record of its compliance with bans does not bode well for the prospect of eliminating JuD. There have been reports, for example, that JuD/LeT leader Hafez Saeed, who had been under house arrest, was seen traveling freely from a mosque to his home after the ban had been imposed.

In addition, banned groups - especially non-profit organizations - tend to reopen under different names shortly after they are listed and sanctioned. This pattern has occurred in Pakistan several times. When al-Qaeda-linked al-Rashid Trust was sanctioned, for example, it merely changed its name to al-Ameen, and opened for business shortly thereafter. It would not be shocking if the same were to occur with respect to JuD.