Penetrating the web of terror networks

Aaron Mannes, R.K. Raghavan, Animesh Roul & V.S. Subrahmanian

A detailed study of the Indian Mujahideen, based on a clinical analysis of curated data, is beginning to pay dividends in understanding when the outfit will launch attacks and who its targets will be

The deadly explosions that struck a Bharatiya Janata Party rally in Patna on October 27 confirmed that terrorism will remain on top of the agenda for an over-stretched Indian police and a heavily burdened Intelligence Bureau (IB). Investigations have revealed the involvement of at least six individuals in the planting of 18 explosives (of which only seven exploded) in Gandhi Maidan. The Indian Mujahideen (IM) is the leading suspect for the daring attack. Its intentions seem clear: convert the rally into a mass fatality event, and spread fear and panic with a blatant message to the security apparatus that the IM is a force to contend with.

To the credit of the Bihar Police, some operatives from the IM's Ranchi cell — one of its newly unearthed field entities — have been arrested in connection with the Patna bombing. Unfortunately, arresting IM operatives does not appear to prevent the outfit from launching terror attacks with relative impunity, and in fact could be a sign that further attacks are in the works.

In the forthcoming book *Indian Mujahideen: Computational Analysis and Public Policy* (Springer 2014), the four writers here were able to use data mining algorithms developed at the University of Maryland to identify broad conditions that were predictive of different types of terror acts carried out by the IM. Over the years, the IM has consistently carried out simultaneous attacks with multiple devices within a few months of the arrests or deaths of its top operatives. Following the arrest of Yasin Bhatkal in late August 2013, this behavioural rule led us to predict that the IM was likely to launch attacks in the last quarter of 2013 — a prediction that has unfortunately come true with the Patna attacks.

The prospect of a renewed IM terror campaign is dismaying because the next few months are going to be dominated by heightened political acrimony related to the general election and the inevitable use of valuable police resources. In contrast, organisations such as the IM and their allies (such as the Lashkar-e-Taiba) and sponsors (such as the Pakistani Inter-Services Intelligence) would remain focussed on creating maximum damage for India's governments.

Soft targets

A striking feature of all IM attacks is the choice of soft targets such as crowded markets. These have caused havoc, killing hundreds of innocent civilians. The IM's trademark has been multi-pronged attacks that maximise casualties. These attacks, such as the near-simultaneous bombing of three courthouses in different cities across Uttar Pradesh in 2007, require substantial coordination and organisational skills. After the U.P. attacks, the IM terrorised India with a string of bombings throughout 2008. In an attack in Ahmedabad in July 2008, the IM set off nearly 20 low-intensity bombs across the city, and when crowds gathered at the City Trauma Centre, it detonated a car bomb, killing dozens. Since then, the outfit has carried out at least 10 forays, including the 2010 attack on the German Bakery in Pune (possibly in conjunction with LeT) that killed 17, a triple bombing in Mumbai in 2011 that killed 27, and in February 2013, a double bombing in Hyderabad that killed 17.

There have been a few significant IM arrests in recent months. In a coup for India's security agencies, two of IM's top operatives, Yasin Bhatkal and Asadullah Akhtar, were captured. Unfortunately, these arrests do not seem to have caused a major dent on the IM, which retains its skill in planning operations with deadly precision and efficiency. The serial blasts in Patna, which were strikingly similar to the twin blasts in Dilsukhnagar (Hyderabad), on February 21, and the July 7 Bodh Gaya blasts this year, illustrate the IM's capabilities. These repeated terrorist successes here and elsewhere can, unfortunately, only help to boost the morale of groups like the IM.

This raises the overarching issue of how to check terrorism in India. It is more than clear that the IM is one of the most active terrorist groups in India. Its achievements have been disproportionate to its actual strength or marginal popular appeal.

Predicting exactly when and where an attack will occur is a task that cannot be consistently done. However, the authors' detailed study of the IM, based on a clinical analysis of carefully curated data, and employing the "big data" analytic techniques (similar to techniques used by the Amazons and eBays of the world), is now starting to pay its first dividends in understanding when the IM will launch attacks and what types of targets it will select.

The study projects an ominous scenario. Periods during which Indian-Pakistani diplomatic relations begin to warm are followed by internal IM conferences and chatter, a month or so later. These high-level internal meetings are seen as necessary to plan the IM's signature multi-pronged bombing campaigns. These meetings are then followed by "ramped up" collaboration with other terrorist groups such as the LeT and the Harkat-ul-Jihad Isami. Pakistani terrorist groups, with the active connivance of Pakistan's ISI, have provided funding, explosives, training and other crucial support, all of which have facilitated the IM's emergence as a deadly terrorist organisation capable in its own right. Shortly after every strike, there are the usual arrests of IM activists. These arrests may be the result of visible IM activity in preparation for an upcoming attack. It is also possible that attacks follow the arrests of IM men, because the IM or its Pakistani allies, LeT and the ISI, want to demonstrate their resolve to carry out further attacks.

Valuable warnings

This sequence of events preceding IM bombings can provide valuable warnings of likely attacks, and highlight points in IM operations that are vulnerable to disruption by security agencies. Specifically, security agencies must subject IM operatives and their networks to extensive covert electronic surveillance. While this is routine in most counter-terror operations, travel intelligence systems must track the movement of IM operatives within India, across India's borders, and even beyond those borders. IM operatives have previously used Indian passports to exit India to friendly neighbouring countries like Pakistan and Bangladesh — from there on, they have used fake Pakistani passports, no doubt supplied by the ISI, to travel to Pakistan and the Gulf.

One of IM's top leaders, Mohammed Sadiq Israr Sheikh, from Azamgarh in Uttar Pradesh, is believed to have travelled from India to Bangladesh in 2000 on a legitimate Indian passport and from there on to Pakistan on a genuine Pakistani passport arranged by the ISI. In Pakistan, he met with LeT commander Azeem Cheema in Bahawalpur and trained at an LeT training camp near Muzaffarabad. At least another 10 people from Azamgarh alone, who travelled to Pakistan through various intermediate countries, have been identified.

Disrupting a network requires understanding it thoroughly in real-time so that attacks can be stopped before they occur. Closer coordination with agencies such as the Federal Bureau of Investigation and other law enforcement agencies will not only help uncover IM's global support network, but also the detailed interlinked relationship among terror, financing, and criminal organisations.

Though it is impossible to predict the exact location and timing of an attack, data mining technology has now come of age. It can predict the types of attacks that terror groups will carry out — and the approximate time-frame (in three-month periods). This provides a valuable input to law-enforcement and intelligence agencies, enabling them to intelligently deploy scarce investigative resources. If this translates into fewer number of IM attacks over the course of a six-month period, we will have brought about a welcome and needed synergy between researchers and law-enforcement at a time when national security demands it.

(Aaron Mannes and V.S. Subrahmanian are researchers at the University of Maryland, where Professor Subrahmanian heads the Center for Digital International Government. R.K. Raghavan served as Director of the Central Bureau of Investigation, while Animesh Roul directs the Society for the Study of Peace & Conflict in Delhi. They have co-authored Indian Mujahideen: Computational Analysis and Public Policy *[Springer 2014])*