

# Mumbai attacks: One year on

**Richard Bingley** looks at how counter terrorism in India has evolved since the Mumbai attacks claimed 173 lives

**ONE YEAR ON, A SERIES OF** security conferences will take place across India, bringing together practitioners in business resilience, including our team at CSARN. But the question on everybody's lips, including overseas investors, will be: what has happened to counter terrorism in India since then?

Recently the US National Counter-Terrorism Center calculated that more than 1,000 Indians lost their lives to domestic terrorism during 2007. A clear upswing in Jihadist terrorism within India has occurred since 2006, and a web of spiralling lethality, delivered via multiple attacks on crowded places and railway networks, has been spun ever more ferociously since the dispatch of DVDs to news agencies by Al-Qaeda affiliates, declaring war on India in June 2007.

But the reality facing India's security planners at national, state and local level is that – alongside the threat from armed Islamic extremists – most cities and more remote critical national infrastructure face sustained threats of attack from a wide-ranging network of violent 'political' groups including: Maoists/Communist Party of India; Hindu extremists; and resurgent Sikh militants in Kashmir, Punjab and Rajasthan.

## GEOGRAPHY

Attacks upon mosques in Malegaon in 2006 (by Hindu militants as a reprisal for earlier Mumbai commuter train bombings) and Hyderabad in May 2007 (which purportedly led to the attack of the city centre by Islamic terrorists months later), have left India's 150 million Muslims feeling just as vulnerable to political violence as any other citizen.

Rightly proud of its secular police and military services, the world's largest democracy may feel culturally munificent and luxuriously spacious to a tourist. But its vast and awkward geography creates a headache for homeland security planners, as do bilateral incursions and battle-tank diplomacy, fuelled by mutual mistrust between Pakistan and India over Kashmir and terrorism.

In the words of Brigadier Pradeep Sharma, founder of India's National Security Guard: "Central government was alive to the threat," and some work had already been scoped



domestically to knit together component parts into an holistic counter terrorism strategy. However, the nature and target shift of the 2008 Jaipur, Delhi and Mumbai attacks have acted as a catalyst for India's security planners to carry out a complete systemic overhaul.

Human and technological intelligence have been upgraded, and staff numbers bolstered dramatically (as in the US and UK after 9/11), with orders to agencies to network information sharing more closely.

Home Minister P Chidambaram has prioritised the creation of a Coastal Command; a tightening of anti-terror laws (repealed for being too stringent in 2004); and regional National Security Guard hubs near major commercial centres (it took almost nine hours, from the time of the first attacks in Mumbai at the Leopold Cafe, for the rapid response team to arrive from Kashmir).

Around 20 counter-insurgency and anti-terrorism schools are to be established. Two Indian reserve battalions are being trained for action as special commando units. Funds are being streamed into technological innovation. The *Information Technology Act* has been tightened to deal with data security, identity theft, fraud and cyber terrorism. The Railway Police is also forming

commando units based in major cities.

Nevertheless, although the national economy is buoyant and some political traction exists at national level because of a relatively decisive election win for Congress, it is important to realise that a 'statist' or public-sector (top down) approach to counter-terrorism is noble, but possibly doomed to reap limited success.

Business security and staff safety – especially within commercial centres that are becoming regular targets – need to be brought to the table with police, NSG and public authority security planners. Business security planners should be actively encouraged by public officials and their own chief executives to form resilience networks themselves. They should be made privy to fast-time emergency incident alerts, authorised threat assessments, accessible government-funded emergency preparedness and crisis response guidance, tabletop and evacuation exercises. They should also have in-house incident management systems that give advice protocols, track vulnerable staff and communicate securely to neighbouring buildings, families and support networks.

City Security and Resilience Networks (CSARN) is a UK-based not-for-profit organisation dedicated to promoting business security and staff safety across the world's major commercial centres. Set up by a group of international experts who had worked to protect business against attacks during Irish political violence and latterly Jihadist terrorism, in the UK, our group will deliver presentations and master classes on business protection, communication and crisis response at the Security Watch India/CSARN 'Security and Infrastructure' conference in Delhi (December 9/10).

One lesson from the attacks in New York and London stand out – despite brave efforts, the government and public sector alone cannot stop terrorism. Responsibility falls on the doorstep of every citizen and business. CRJ

*More than a thousand Indians lost their lives to domestic terrorism during 2007*

## AUTHOR

**Richard Bingley** is the Chief Executive of City Security and Resilience Networks ([www.CSARN.org](http://www.CSARN.org)) and member of CRJ's Editorial Advisory Panel. He is grateful to Brigadier Pradeep Sharma and Stirling Assynt ([www.stirlingassynt.com](http://www.stirlingassynt.com)) for information supplied

