

# BEYOND GUNS, GUARDS AND 'BANDOBAST'

*The terror attack in Mumbai points to the need for an integrated automated system to raise the homeland security bar high enough to deter any threat*

AJAI CHOWDHRY

*Terrorists certainly rely on technology. The terrorists who struck Mumbai stunned authorities not only with their use of sophisticated weaponry but also with their comfort with modern technology.*

— William LaRaia and Michael C. Walker in *A New Understanding of Terrorism* on the siege in Mumbai on November 26, 2008

What American security experts LaRaia and Walker highlight is a heightened realisation of India's security imperatives, post 26/11. The terrorists not only held the nation's financial capital to ransom for more than two days, but also had hi-tech equipment and communication support of VoIP-enabled SAT phones, GPS navigators, a publicly available virtual global mapping system and emails to execute their sinister plot.

The terror unleashed spells out the need for an integrated automated system to raise the homeland security bar high enough to deter any threat to the country.

While our armed forces and intelligence services are well-equipped and have the capability to deploy anti-terror technology, homeland security needs to go beyond guns, guards and *bandobast*. There is a need to not feel complacent with mere deployment of boom barriers, CCTVs and a heavy posse of personnel to counter terrorism. Coordination between control centres, security agencies and on-ground policing holds the key and this can be only achieved with an integrated system.

High-end IP surveillance cameras used with video analytics is more effective than manpower-intensive surveillance systems sans analytics.

Similarly, integrated security structures—including the Command, Control, Intelligence or C2I system—integrate various sensors, like access-control, under-vehicle surveillance, screening and many other sensors. This, in fact, is 'actionable' intelligence, as it allows authorities to act in a focused manner.

'Actionable' intelligence also integrates databases incidental to security, including aviation, passports and immigration, policing and other internal security apparatus, disaster management and relief response, communication departments, and, registration of births and deaths—the scope is vast.

Immediately after taking over as the Home Minister after 26/11, P. Chi-



The 26/11 terror strike was of a type that had never before been seen in India

dambaram set in motion a speedy overhaul of homeland security, including beefing up maritime protection, borders, airports, mass-transport networks and critical infrastructure security. The Multi-Agency Centre (MAC) was the first to be operationalised. MAC enables analysis of intelligence inputs on a real-time basis and sharing of information among intelligence agencies and police forces.

India's commitment to homeland security got a 35 per cent boost to over \$29.52 billion (Rs 135,792 crore) this fiscal, \$10 billion (Rs 46,000 crore) of which is for upgrading and revamping equipment and technologies, including ground, sea and air surveillance systems and communications. There is no official data available on the size of the market, but Frost & Sullivan's Indian Homeland Security Market 2008 projection puts India's overall spending at around \$1,000 million (Rs 4,600 crore) in 2010.

Security is an intrinsic part of growth. The economy's average growth rate of 7 per cent since 2006-07 has factored in the government's decision to increase investments in all key domains, including defence and homeland security. Further, increased private participation in the defence industry since 2001 has seen greater investment opportunities.

However, given the enormity of the situation—the US State Department has proclaimed India worst hit by terror in its 2008-09 global terrorism report—the homeland security market needs to open further.

Frost & Sullivan estimates that cumulative spending on India's civil se-

curity, growing at 20 per cent a year, will go up to \$9.7 billion (Rs 44,620 crore) by 2016. This is less than the \$10 billion (Rs 46,000 crore) US aid Pakistan received in 2001 in the wake of 9/11; less than 2 per cent of the Planning Commission's estimate of \$500 billion (Rs 23 lakh crore) for infrastructure during the 11th Plan period (2007-12).

Another case in point: the 2010 Budget request of the US Department of Homeland Security (DHS) is \$55.1 billion (Rs 253,460 crore)—450 times more than India's projected homeland security spending in 2016!

An integrated security system is relatively new even for the West. After 9/11, a shaken America set up the DHS. The Secure Communities programme of the DHS depends on state-of-the-art technology to identify criminals through modernised information sharing; prioritise enforcement actions to ensure apprehensions and removal of dangerous criminal aliens; and transform criminal alien enforcement processes and systems to achieve lasting goals.

However, the UK was a frontrunner in establishing a technology-driven barrier—the Ring of Steel—following the IRA bombings in the 1990s. Roads entering London were made narrow, with small chicanes slowing down vehicles to be recorded by CCTV cameras. Following al Qaeda threats, the Ring of Steel was widened in 2003.

Last year, China spent \$5.5 billion on integrated security for the Beijing Olympics. Eighteen Games sites were secured with a network hinging upon

strategic placements of quick response teams, linked CCTV solutions, surveillance resources, non-intrusive round-the-clock vigil, and monitoring facilities.

Recently, the counter-terrorism programme of the New York Police Department mooted the Lower Manhattan Security Initiative, which envisages 3,000 security cameras and licence plate-reading devices at an estimated cost of above \$90 million to secure Lower Manhattan.

In India too, there is a need for such security measures to nip the terror mechanism in the bud. First of all, the attitude towards high security has to change and the advantages of integrated technology in pre-empting terror strikes must be realised. The law and order machinery must comprehend the need for a technology-led network to neutralise threats.

As 26/11 and earlier terror attacks reveal, terrorists don't target government installations alone. Privately owned spaces, including hotels, restaurants and religious houses, are also on their hit-list. It's imperative that the private sector invests in security as adequately as it does in infrastructure, energy efficiency, and sustenance programmes. Incentives to companies deploying, advocating and adhering to security measures can further the cause.

Although there are insurance covers available against terrorism, it is also vital to link insurance with security. Terror attacks have economic ramifications. What 26/11 did to India's image was reflected in tourism, travel and the hospitality sectors. As domestic travellers hesitated following the attacks, travel advisories by countries against visits to India made matters worse.

The threats have cast a shadow on sports tourism too. Security concerns saw the multimillion-dollar IPL—II being moved to South Africa following a clash of dates of the cricket event with the general elections. This resulted in huge financial loss for advertisers, franchise owners, support businesses and the exchequer.

We are mere months away from Commonwealth Games 2010. The government has approved Rs 370 crore for an integrated security system at the Games—the first of its kind for an event of such a large scale.

Such measures must not remain confined to the Games. As a start, we need to make each of our seven megacities—Delhi, Mumbai, Kolkata, Chennai, Bangalore, Hyderabad and Ahmedabad—secure through such integrated technologies.

The author is Chairman & CEO, HCL Infosystems