Mumbai investigators found key clues in cyberspace

Praveen Swami

Police unravelled electronic threads linking perpetrators to Pakistan

Hacked Internet servers were used to set up fake e-mail addresses

Money was electronically transferred and GPS guided perpetrators to their targets

NEW DELHI: The November 2008 massacre in Mumbai was carried out using old fashioned instruments of terror: the gun and the bomb.

But the death they delivered was facilitated by state-of-the-art digital technologies — on ones and zeros flying, as it were, through cyberspace.

Mobile phones and voice-over-Internet protocol links connected the Lashkar fidayeen to satellite phones used by their controllers in Pakistan; hacked Internet servers were used to set up fake e-mail addresses; money was electronically transferred halfway across the world; and global positioning systems guided the perpetrators to their targets.

Documents filed by Maharashtra prosecutors in a Mumbai court earlier this week show, though, that each of these technologies left behind a trail of digital clues that investigators were able to pin down the perpetrators — and, in the process, blow apart Islamabad’s claims that Pakistan-based groups had nothing to do with the massacre.

Cellphone trail

Mumbai police experts, working with help from America’s Federal Bureau of Investigation and India’s own covert services, first focussed on three Indian cellphone numbers used by the Lashkar fidayeen to communicate with their handlers in Pakistan: +91 9819464530, +91 9820704561 and +91 9910719424.

Each cellphone, logs showed, had received calls from a United States number, +1(201)2531824 and made outgoing calls to three Austrian numbers, +43(720)880764, +43(720)880767, and +43(720)880768
All the overseas numbers, it turned out, had been generated through Callphonex, a VOIP service provider based in New Jersey, U.S. Callphonex told investigators that an individual who identified himself as Kharak Singh and claimed to be a VOIP retailer based in India had opened the account from which the numbers were generated on October 20 and October 21, 2008.

Paracha International Exchange, a Lahore-based agent for the international money-transfer service MoneyGram, wired $250.00 into Kharak Singh’s account with Callphonex six days later. MoneyGram records show the payment was made by Muhammad Ishfaq, who recorded that he was a resident of Peshawar, but did not provide government identification.

Callphonex executives told investigators they did ask why payment for an Indian businessman’s account was being made from Pakistan, but do not appear to have taken any further action.

Later, on November 25, 2008, a second payment of $229.00 was wired to Callphonex, this time through a Western Union agent in Brescia, Italy. Western Union, unlike MoneyGram, demanded proper identification from Javed Iqbal, who initiated the transfer. He provided them with a Pakistani passport, which bore the number KC092481 — which was to lead to his eventual arrest by authorities in that country, although it is unclear if he will face trial.

Nokia’s Dong Guan plant in China, which had manufactured the five Nokia 1200 sets recovered from the terrorists, had records showing they had been shipped to two distributors in Pakistan — United Mobile, and 12 Pakistan.

E-mail leads

Now, investigators set their minds to the e-mail address the man calling himself Kharak Singh used to communicate with Callphonex.

Mumbai police cyber detectives found that the e-mail address, kharak_telco@yahoo.com, had been accessed from several Internet-protocol addresses. Five of these IP addresses were in Pakistan — one, interestingly, registered to Colonel R. Saadat Ullah of the Pakistan Government’s Special Communications Organisation in Rawalpindi, where that country’s military is headquartered.

The perpetrators had also hacked servers outside of Pakistan to access the e-mail account. Two of these, registered to Vladimir Zernov of the Moscow-based company GASCOM, proved to be of enormous value.

Police found that a claim of responsibility issued minutes after the attack by an organisation calling itself the Deccan Mujahideen had been generated from the IP address 82.114.141.99, which was registered to GASCOM. However, it had, also been used to send e-mail from kharak_telco@yahoo.com to Callphonex.

In other words, the two individuals were most likely the same individual — and, given the link between the Callphonex accounts and Pakistan, was almost certainly based there.

GPS logs
FBI experts provided more hard evidence linking the Mumbai perpetrators to Pakistan after analysing the five Global Positioning System sets they had used.

One set, a Garmin Rhino 120 with the serial number 415148192, which was found in the Taj Hotel, had a list stored in a memory with the longitudes and latitudes of 50 locations in Karachi — presumably generated when the set’s users were familiarising themselves with its working.

Moreover, a Garmin 12 Map found on the fishing ship Kuber, which the terrorists had hijacked to land in Mumbai, bore latitude and longitude data recording the terrorists’ journey from Karachi to Mumbai. Waypoints — pre-fed latitude-longitude entries to guide long-distance journeys — between Karachi and Mumbai were marked as Ocean 1, Ocean 2, Ocean 3, Ocean A, Jala-1, Jala-2, Jala-3 and Jala-4.

© Copyright 2000 - 2008 The Hindu