The Significance of Counter-intelligence in Counterterrorism

Shri Prem Mahadevan*

Introduction

This essay argues that counterterrorism is not an intelligence function, but a counter-intelligence one. The distinction is not merely semantic: it lies at the core of tragedies such as the Mumbai 2008 attacks. Since the tensions between these two kinds of activity – intelligence and counter-intelligence – remain unresolved, counterterrorism efforts get bogged down.

Defeating the current terrorist threat requires replacing intelligence methods with counter-intelligence ones. It involves moving away from a defensive mindset that constantly seeks to predict the enemy's next move and thus implicitly concedes the initiative to him. Instead, the government should seek to surprise the enemy, which requires first blinding him through counter-intelligence operations.

The essay explains the differences between intelligence and counter-intelligence. It goes on to argue that counter-intelligence constitutes the main strength of terrorist movements. Lastly, the essay argues that this strength needs to be overwhelmed through a proactive counterterrorist posture. To prevent more terrorist attacks, the Indian government must leverage territorial dominance to attain informational dominance.

Three Differences between Intelligence and Counter-intelligence

The terms 'intelligence' and 'counter-intelligence' carry different implications for counterterrorist practitioners. These differences need to be explicated. Intelligence is about predicting an enemy's behaviour, with the enemy typically being a foreign state.1 Counter-intelligence is about neutralising foreign threats that are attempting to infiltrate one's own state and damage it from within. Differences between the two activities can be conceptualised as: differences of purpose, process and priorities.

A Difference of Purpose. Counter-intelligence is inherently aggressive, since it aims to disrupt threats rather than just monitor them (which is the objective of intelligence work). Intelligence officers usually draw a 'red line' between reporting facts and advocating policy.2 Their job, as they see it, is merely to keep policymakers updated about threats; how to react is the policymakers' prerogative.

Such clear-cut divisions of responsibility do not exist in counter-intelligence. Instead, there is an imperative need for taking follow-up action independently of political considerations. This is because each counter-intelligence target, be it a foreign spy ring or a terrorist cell, represents a threat-in-being. Its neutralisation is mandatory. The first point of tension between intelligence and counter-intelligence is thus: intelligence is about observation, counter-intelligence is about action.

A Difference of Process. There is a procedural difference between the production of intelligence assessments and those of counter-intelligence. With the former, the over-arching objective is to speak 'truth unto power', irrespective of how well-received such truth is likely to be.3 Analytical objectivity is to be maintained at all costs. To ensure that decision-makers do not receive reports that blindly pander to their policy preferences, intelligence assessment is staggered among a range of agencies.4

In counter-intelligence, the aim is not to divine 'truth' by subjecting the same set of facts to a variety of agency interpretations. Rather, the aim is to bring together data from a variety of agencies onto a common analytical platform so as to detect the existence of hidden threats within one's political system. Centralised assessment and institutionalised data-sharing is what is needed, not competition.5

A Difference of Priorities. The third difference between intelligence and counter-intelligence is one of collection priorities. Intelligence focuses on discerning an enemy's intentions, since these can change quicker than his capabilities.6 Moreover, the usually static nature of the international system means that collection operations are conducted within a high-impact/low-probability paradigm. Though the consequences of being attacked by an enemy state are huge, the likelihood of such an attack actually occurring is quite low.

With counter-intelligence, this paradigm is reversed. The intention of foreign powers to conduct intelligence operations can be taken for granted. Rather, it is their capabilities for doing so which need to be monitored, since these can vary over time. Furthermore, even an extremely damaging intelligence penetration cannot do damage of the magnitude that a military assault can achieve. Unlike intelligence, therefore, counter-intelligence activity is conducted within a high-probability/low-impact paradigm.

This paradigm also applies to counterterrorism. Terrorists' intentions to kill indiscriminately are well-known. What is needed is knowledge of their attack capabilities.7 These capabilities are quite small, and are thus inherently difficult to track, compared to troop movements in enemy states. Further complications are caused by the strength of terrorist counter-intelligence.

Counter-intelligence: The Asymmetric Advantage of Terrorism

For terrorists to succeed, they must keep attacking the state, while escaping its retribution. Anonymity is thus crucial to the continuance of their activities. In pursuit of anonymity, terrorists rely on two advantages that are peculiar to them: tight operational security, and ruthless elimination of informers. Together, these factors give terrorist organisations a massive advantage in counter-intelligence, which the state's security apparatus finds difficult to overcome.

Good Operational Security. Unlike conventional militaries, terrorists emphasise security over co-ordination. Their logic is that while an attack can always be postponed if preparations are incomplete, detection by the authorities would permanently wreck its prospects.8 To increase the resistance of their organisation to intelligence penetration, terrorists compartmentalise their activities. Finances, intelligence-gathering and logistics are handled by different cells from those that actually carry out attacks.9 The 'need-to-know' principle is rigorously enforced.

Once recruited to a terrorist organisation, new members are expected to show blind obedience to its leaders. Such obedience is particularly forthcoming from individuals eager to climb the organisational hierarchy. Thus, as former Central Intelligence Agency (CIA) analyst Michael Scheuer has noted, the higher a terrorist rises in the decision-making structure of his group, the less susceptible he becomes to inducements for betrayal. This means that those individuals who are most likely to have the information sought by intelligence agencies, are also least likely to sell that information.10

Punishment of Betrayers. Further difficulties in intelligence collection are caused by the ferocity with which terrorists punish informers. By a process of systematic intimidation, terrorists create what one writer has termed as a 'counter-intelligence state'. This is a state where social control is exercised through a system of organised terror and pervasive surveillance. Any well-organised terrorist group, such as Lashkar-e-Toiba (LeT), is therefore 'pathological about enemies and makes the search for them and their discovery and elimination an overriding state objective'.

Given the degree to which terrorists remain vigilant against betrayal, professional intelligence agencies have little scope to operate. Any leakage of attack plans leads to an immediate investigation aimed at unmasking government spies. In this situation, no informer can risk making regular contact with his/her handler. It was for this reason that the Intelligence Bureau's network in Jammu & Kashmir collapsed during 1990, following the assassination of five key operatives.

Counter-intelligence forms the primary strength of terrorist movements. Overcoming this strength is the equivalent of defeating the terrorist threat, while avoiding engagement with it sustains the threat. Harvard scholar Ivan Arreguin-Toft therefore suggests that a government can only win against terrorists by fighting on their terms.12 Since terrorism is all about avoiding direct contact with the state's coercive apparatus, terrorist organisations will never provide clear-cut targets for attack. Further, their advantage in counter-intelligence means that efforts by intelligence agencies to locate such targets shall be frustrated. To win against terrorism, governments must first win the counter-intelligence battle.

Fighting Counter-intelligence with Counter-intelligence

The key to defeating terrorist counter-intelligence does not lie in a defensive counterterrorist posture that focuses on predicting terrorist attacks. Rather, it lies in mounting an even more formidable counter-intelligence effort that makes up in scale what it lacks in ferocity. Here, governments possess a key advantage over terrorists. With their large and well-indexed archives, official bureaucracies provide a wealth of background data for use in mapping out terrorist support infrastructure.13 This institutional memory in turn functions as a guide for countering action, focusing it unto critical nodes in the terrorists' logistical and intelligence network.

Counter-intelligence is relevant to this process because unlike intelligence activity, it is accustomed to functioning within legal constraints. Indeed, counterterrorism is itself an amalgam of three counter-intelligence functions, each with its own unique dynamics. These are: counter-sabotage, counter-espionage and counter-subversion. The relevance of each of these three functions to counterterrorism is be discussed below.

Counter-sabotage is the process of hardening security around likely targets to cope with surprise attacks. It is an essential component of counterterrorism because much of a terrorist organisation's morale hinges on the ability of its cadres to conduct daring, deep-penetration strikes.14 Depriving terrorists of the ability to attack prestigious or infrastructure targets thus amounts to a psychological victory. For this, counter-sabotage experts need to take stock of terrorist attack capabilities, and develop response protocols for all scenarios where these can be used, not just the most likely ones. Failure to adopt this methodology resulted in a large number of deaths during the Mumbai 2008 attacks.

Indian intelligence agencies knew that an attack was coming and that it would be directed at hotels, but were unsure what form it would take. Upon their advice, precautions were taken against bomb attacks. This was a reasonable move from the perspective of trend analysis – a technique commonly used in forecasting. The so-called 'Indian Mujahiddin' bombing campaign of 2007-08 had indicated that explosives were the preferred method of killing for terrorist groups.

Unfortunately, what was overlooked was evidence that LeT continued to train fidayeen (suicidal) squads for attacks using hand-held weapons. Such attacks were much rarer than bombings, but still possible. Whereas an intelligence assessment would have considered them unlikely, a counter-sabotage assessment would have examined the practicality of defending against them. In the process, it would have identified the glaring deficiencies in police training, communications and weaponry which became obvious on 26/11.

Counter-espionage is crucial to degrading the capacity of terrorist organisations to adapt to their external environment. Such adaptability is a sign of the organisations' operational sophistication and responsiveness to feedback from their supporters.15 It is a red flag that governments must take notice of. Since the aim of counterterrorism is to split terrorists from their support base, their sources of information need to be closed down. Particularly important to this process is electronic surveillance – the monitoring of e-mails, faxes, telephone and cellular calls.

Indian intelligence agencies did an excellent job of listening in, minute by minute, on the Mumbai attackers' conversations with their handlers in Pakistan. However, they were unable to use this technical sophistry prior to the attacks to identify those providing informational support to LeT. That there was some measure of local support seems obvious. The precision with which the terrorists chose their landing site, the identification of Nariman House (a completely non-descript building) as a target, and the detailed knowledge that they had of the hotels' topography, all indicate pre-operational reconnaissance.

From prior incidents of Pan-Islamist terrorism, it seems likely that Pakistani Inter Services Intelligence (ISI) agents reconnoitered for the LeT fidayeen. These individuals, and not the actual gunmen, ensured that the devastation caused on 26 November 2008 was so considerable. Identifying them would have required allowing the IB to focus on its primary task of uncovering foreign spy networks. Instead, the Bureau had been forced to assume an intelligence role, since the defensive nature of Indian counterterrorist policy made predicting the terrorists' next attack essential.

Counter-subversion aims to identify and neutralise elements within one's own society who propagate seditious ideology. These elements thrive by abusing democratic rights such as freedom of speech and freedom of assembly, turning them into vehicles for radicalisation.16 Combating such activity requires intelligence agencies to infiltrate terrorist front organisations not with a view to monitoring their activities, but to gather evidence that will support criminal prosecutions. The existence of strong anti-terrorism legislation and full co-operation of the judicial system is integral to this endeavour.

India however, has a poor record of using legal processes to combat subversion. This is because its political class has itself subverted the rule of law to serve narrow partisan interests. During 2001-2004, the Prevention of Terrorism Act (POTA) was misused by certain state governments to harass political dissidents. Thereafter, the Act was repealed on a purely reflexive basis, to score points with minorities. In the process, the Country was left without a legal framework to allow for police action against subversive individuals.

This proved costly in the period 2004-2008, when Pakistan-based terrorists intensified their offensive against the Indian heartland. Many of their Indian accomplices were known to local police forces, but they could not be touched because of a lack of legal provisions. Meanwhile, the intelligence agencies monitored major centres of Pan-Islamist subversion, but did not have the wherewithal to track terrorist activity based out of small towns. Aware that the IB has a poor coverage of rural areas, the ISI-LeT combine created support networks in these areas. Consequently, the rate at which terrorist recruiters won converts to their cause was greater than the rate at which they could be neutralised.

Recommendations

This essay argues that counter-intelligence activity is far more relevant to counterterrorism than is intelligence. Demanding forewarning of terrorists' intentions to kill civilians is as ludicrous as demanding forewarning of foreign governments' desire to steal national secrets. Instead of merely predicting threats, intelligence agencies need to make a paradigm shift and start countering them. Obstacles to such a paradigm shift derive mainly from fundamental differences of purpose, process and priorities that exist between intelligence and counter-intelligence.

Four measures need to be taken to re-orient Indian counterterrorism from an intelligence-driven approach to a counter-intelligence-driven one. First, the IB's Multi Agency Centre, set up in 2001 to consolidate all terrorism-related information into a common database, must be strengthened. Centralised analysis is essential if alarming trends in terrorist activity are to be detected in time for police forces to mount surgical interventions. Second, the IB's technical collection assets must be enhanced, since they are vital to detecting the flow of intelligence to terrorist planners in Pakistan. Only by degrading the ISI's espionage capability in India will the security establishment succeed in depriving terrorists of the information needed for planning an attack. Third, the IB must be given funds to expand its coverage of rural areas by raising large numbers of human assets. The poor quality of telecommunications in these areas will require IB agents to physically infiltrate terrorist front organisations and gather evidence of seditious activity. Lastly, the state police forces, together with the newly-raised National Investigation Agency, must be provided with the political backing needed to arrest and prosecute individuals suspected of supporting terrorism. Failure to take these steps will reflect a continued reliance on predictive reporting to warn of terrorist attacks, and an inability to think offensively.

***Shri Prem Mahadevan** is currently researching on 'The Dynamics of Counterterrorist Intelligence' as a doctoral candidate at Kings College, London.

Journal of the United Service Institution of India, Vol. CXXXIX, No. 576, April-June 2009.