Surveillance in Counter-Terrorism, Counter-Insurgency and Warfare

Jayadeva Ranade

Surveillance is a vital component of intelligence operations geared to securing sensitive facilities or combating terrorism or insurgency. Since the time man conceived of borders and frontiers, whether to stake out his property or secure the boundaries of his people, surveillance has been used in one form or another. It is primarily intended to protect and secure the individual, his property or commercial entity and the nation-state. Surveillance can be defined as intended "to detect, identify, track and intercept hostile action." In the modern day, especially with the ever-present danger of use of nuclear weapons in the subcontinent, this definition requires to be reinforced with a strong predictive component and continuing real-time inputs of an ongoing action to allow for counter-measures. This is in addition to the forensic, or post-event, role that surveillance plays. In the context of surveillance and India's terrorist threat, the observation of former Israeli Prime Minister Shimon Peres, is pertinent. He said: "We can't change their will to attack, only their ability to attack."

The craft of intelligence has come a long way since the days of yore when surveillance comprised almost entirely sending out scouts to reconnoitre the way ahead or enemy positions or position sentries on mountain passes. New innovative methods have been progressively introduced. Predictive methodology – or preemptive intelligence – and technology began to be deployed for modern surveillance. The need to secure air and sea frontiers in

Mr **Jayadeva Ranade** is former Additional Secretary, Cabinet Secretariat, Government of India and at present Distinguished Fellow, Centre for Air Power Studies, New Delhi.

addition to land borders and sensitive facilities has enhanced the importance of surveillance. Yet, in India, this aspect of the intelligence craft unfortunately continues to be neglected, possibly because by its very nature it is low profile, secretive and subterranean.

Rapid advances in science today ensure that technology contributes considerably to more effective surveillance and additionally plays a predictive role. It can relay advance intelligence on hostile activity as soon as it commences or begins to approach the target. While human intelligence (or HUMINT) is crucial and irreplaceable, technological enhancements are today an important part of surveillance. Monitoring of internet, landline and mobile communications of terrorist suspects gives vital advance information on plans and movements. This monitoring is part of the surveillance too. Today, when scarce vital resources worth billions of dollars lie in offshore locations or difficult inaccessible terrains, surveillance technology can play a meaningful role. In some cases, in fact, it will be the sole source of surveillance. India, with its 7,500 km of coastline, 230,5143 sq km of resource-rich exclusive economic zone and miles of air space, needs effective surveillance to prevent unauthorised activity which could result in huge financial loss or loss of sovereign territory. Technology is an imperative value-addition for this as continual surveillance only by humans, ships or aircraft is just not possible over such large areas.

Today, when rapid advances in communications and transport systems necessitate quick responses, technology plays an even more vital role in surveillance. The emergence of trans-national terrorism has accentuated the need for 'passive', 'archival' and real-time active surveillance. In 'passive' surveillance is included all forms of surveillance intended to routinely monitor normal human activity in sensitive or protected areas. 'Archival' surveillance comprises in-built recognition features in surveillance technology that identify particular individuals as well as their being in a specific place at a specific time and stores this data. 'Real-time' or 'active' surveillance is the monitoring of an event or activity as it occurs or unfolds. The latter information especially needs to be instantly available to the authorities for appropriate action. In all these areas, the role of technology is growing. For India, which is being subjected to a steadily expanding arc of terrorist actions, technologically enhanced surveillance is an inescapable necessity.

The effectiveness of comprehensive surveillance aided by technology was vividly demonstrated in two recent terrorist-related incidents at two separate, distant locations. These incidents occurred in Dubai and the USA. In the first,

effective surveillance provided fairly conclusive clues as to the movements, actions and identities of the team that had arrived in Dubai to carry out an assassination. The second instance showed the effectiveness of technology-backed surveillance in the timely apprehension of a suspected terrorist leading to the identification of three more individuals.

The 'action' in Dubai, which involved the assassination in January 2010 of a Hamas leader and 'hitman' in Dubai by an 'action' team of the Israeli intelligence agency, Mossad, is a good example of effective 'passive' as well as 'archival' surveillance. The assassination of senior Hamas militant leader, Mahmoud al-Mabhouh on January 19, 2010, continues to generate a tremendous amount of discussion and speculation among intelligence and counter-terrorism experts many months after the fact. For weeks after the 'hit', Dubai's police force kept steadily releasing new information almost on a daily basis, which drove the news cycle and kept the story in the media spotlight. Among the most astounding releases has been the nearly 30 minutes of surveillance camera footage that depicts portions of a period spanning the arrival of the assassination team in Dubai, surveillance of al-Mabhouh, static surveillance of the hotels where he could have stayed, the hotel and corridor of the room where he actually stayed, his killing, and the exfiltration of the team some twenty-two hours later.

By last count, Dubai police claimed to have identified some 30 people suspected of involvement in the assassination and approximately 17 have been convincingly tied to the operation through video footage either as surveillants, managers or assassins, with the rest having only tenuous connections based on information released by the Dubai police. The surveillance camera tapes confirmed that the operation was certainly elaborate and required the resources and planning of a highly organised agency, one most likely working for a nation-state. Briefly, the security video coverage captured the arrival of the Hamas leader, his 'pick up' by the Israeli surveillance team at the airport, the tracking and 'housing' in the hotel of the Hamas leader, his assassination, and the escape of the suspected Israeli team from Dubai. It facilitated identification of some of the passports held by the Israeli team. Despite strenuous Israeli denials, as a consequence of information gathered through technical surveillance by the Dubai authorities, at least two Israeli diplomats were expelled by foreign governments for obtaining forged passports and the Mossad chief had to resign.

The second equally revealing instance of the effectiveness of surveillance was that of Faisal Shahzad in New York in May 2010. In this case, the terrorist,

a US citizen of Pakistani origin, attempted to detonate a car bomb at Times Square, which providentially failed to explode. Due to 'passive surveillance' technology being in place, the US authorities had already 'picked up' Faisal Shahzad after he returned in February from a 5-month-long sojourn in Pakistan. An alert passerby spotted the smoke emanating from the car Faisal Shahzad had parked at Times Square and alerted the police. Once alerted, the authorities defused the defective bomb and scanned the surveillance cameras deployed around Times Square. They identified the vehicle and its registration number, identified Faisal Shahzad from the stored surveillance tapes, matched that with his identity in the documents used for hiring the car and electronically flashed his photograph to all border control and police units. Meanwhile, Faisal Shahzad had checked into the airport and boarded an aircraft bound for Pakistan. He slipped through security at the check-in, but a guard at the boarding gate identified him from the photograph on the alert that had just been issued and informed the authorities. The aircraft was called back and Faisal Shahzad arrested. Had surveillance not been given adequate importance, the opportunity to identify and arrest Faisal Shahzad and interrogate him would have been missed. The authorities are now on the hunt for three accomplices of Faisal Shahzad.

With the advent of instant communication and the potency of private television channels, the political and executive authorities need to be more sensitive towards thwarting terrorist actions in the future.

Cities like Delhi, Mumbai, Hyderabad and Bengaluru, for instance, lack even basic surveillance coverage. These cities are all prime terrorist targets and should have been blanketed by surveillance cameras equipped with facial recognition features. London, Washington, New York, Montreal, Tokyo and Beijing, for example, are among the most surveilled cities in the world and none of them has been subject to as many terrorist attacks as Indian cities have been. Demonstrating the usefulness of this technology in counter-insurgency operations also, China recently disclosed that in its troubled Xinjiang Uighur Autonomous Region, it has installed one million surveillance cameras. Obviously, the authorities have incorporated facial recognition and remote communications features in these surveillance cameras. In India, on the other hand, in the few cases where surveillance cameras are mounted, they are either

non-functional, improperly installed, or cover a very limited area. In any event, they are inadequate in number and not equipped to remotely convey instant information to the police, or anti-terrorist, control room and mobile police units.

With the advent of instant communication and the potency of private television channels, the political and executive authorities need to be more sensitive to thwarting terrorist actions in the future. At the very least, they would need to appear to be effectively dealing with the threat. The 26/11 terrorist attacks in Mumbai demonstrated the effectiveness of private television channels in bringing the unfolding events into people's homes. The inability of any of the concerned security agencies to tackle the threat was visible. The people's ire was unprecedented and indicative of what can be expected in the future.

The security and police forces need to gear themselves to react instantly to tackle ongoing situations and this requires the visual capturing of ongoing events and their instant uninterrupted communication to headquarters, field formations and mobile units/forces. In cities, there is an urgent need for positioning thousands of remotely controlled surveillance cameras equipped with facial recognition and communications technology that can instantly convey visuals to the control rooms and mobile security units and identify the individuals captured by it. Had these been in place in Mumbai, the police force would have had information as to the number of terrorists, their whereabouts, and the action that was taking place in Mumbai, etc. They would have promptly identified it as a terrorist action and not a gangland war. Action to neutralise, or apprehend, and contain the terrorists could have been taken within an hour.

In the context of the ever-present threat of terrorism, cities, ports, airports, railway stations and market places need to be brought under the umbrella of surveillance cover. For those entrusted with the task of keeping a tight grip on the country's purse strings, they can be assured that saving human lives compensates for expenditure on these systems. Moreover, once deployed sensibly, the surveillance camera systems will simultaneously reduce the incidence of crime, facilitate identification and apprehension of the perpetrators, make the cities safer and improve traffic discipline. The imposition and recovery of fines from traffic violations alone will help recover the expenditure on the surveillance system—possibly within a couple of months!

There is emphasis today, in view of the terrorist threat, for 'preemptive' intelligence through surveillance of the land, air and sea borders. To obtain this intelligence, the US, European Union (EU), etc are using a variety of equipment and refining surveillance technology. For example, global positioning systems (GPS) are increasingly being used on land, the sea and in the air. Similarly, air, sea and land-borne cargo is scanned at the point of loading, thus, bringing it into the ambit of preemptive surveillance intelligence. For border surveillance, in addition to basics like solar lighting, ground-based radars, patrol craft and sonars, countries are increasingly expanding the area surveilled by deploying drones, unmanned aerial vehicles (UAVs), and underwater unmanned vessels (UUVs). China, for example, has quietly made rapid strides in UAV and UUV manufacture and technology. Satellite platforms are routinely used. The US and EU have introduced a series of measures to screen populations and travellers. The US has introduced similar systems, including biometrics, ID cards, visitor identification systems and a passenger database. The US is attempting now to introduce the electronic system of travel authorisation, or prior authorisation to travel. Together, these surveillance technology platforms provide an ever expanding database facilitating instant facial and biometric recognition of visitors and suspects. Over time, these simplify security and immigration clearance procedures for travellers at the point of entry while appreciably enhancing security.

Satellites appear to currently provide the best solution for monitoring of activity in areas around the borders, including deep inside the neighbouring countries.

Counter-insurgency operations are an area where the use of surveillance technology will minimise casualties and enhance the rates of success. Presently when the Central Reserve Police Force (CRPF) patrols move out of their camps, they have virtually no means of instant communication with their base and neither is the base able to identify the precise location of the patrol. The camps themselves have no equipment to detect hostile activity around their perimeter. Today, when technology is available to meet these requirements, the CRPF camps and patrols operating in forested 'Maoist country' should be liberally equipped with GPS, remote wireless SATCOM equipment and surveillance cameras, and trained in their use. Bases of a permanent or semi-permanent nature could be equipped with wide-scan cameras mounted on specially

The Kargil War brought into sharp focus the need for technologically-assisted surveillance as a non-subjective additional precaution and a safety layer.

rigged masts. These could be configured for both night and day-time operations. Additionally, the camps should have off-air mobile phone monitoring capability which will facilitate interception of the communications of hostile elements and location of their positions. These need to be augmented with the deployment of lightweight, limited range UAVs. The latter can monitor the terrain and surrounding environs for the patrols during their mission, keep the base simultaneously informed and also provide a more effective security cover for the base camp by monitoring a wider area around the camp for hostile activity. Protective cover for CRPF patrols, personnel movement and replenishments needs to be provided by helicopters, which can combine this with reconnaissance functions. The present practice of personnel proceeding on leave or transfer going to the nearest road-head to catch a bus is fraught with risk. It opens the possibility of the personnel being killed by the 'Maoists' or being 'won over'. If they are equipped with biometric, GPS-embedded cards, their locations would always be known, thereby minimising the risk.

Surveillance, particularly backed by technology, is equally effective in monitoring the country's land, sea and air borders. While in the subcontinent there continues to be emphasis on human resources, these are increasingly proving inadequate. Satellites appear to currently provide the best solution for monitoring of activity in areas around the borders, including deep inside the neighbouring countries. Google Earth is a good example. The land borders remain porous despite the deployment of forces. In some cases, like with Nepal, it requires innovative techniques, the cost of which requires to be matched with the threat perception. With Pakistan, the threat perceived overrides the cost considerations and has seen the erection of a border fence. This needs to be augmented with sensors and remote wireless visual communication between the border command posts and UAVs. Satellite coverage needs to be virtually continuous, particularly of missile sites and airfields where aircraft capable of carrying nuclear weapons are deployed, especially in view of Pakistan being a de facto nuclear power. To monitor the coast off Pakistan, the UUVs would be useful. The border with Bangladesh is similarly porous and greater weightage needs to be given here to augmenting patrolling with new technology. Innovative

new techniques are called for. Often, these would require to be backed by technology.

India's requirements are peculiar. It is situated in a 'rough' neighbourhood and has inaccessible mountainous stretches for long distances along the border with Pakistan in the northwest and in the north and northeast with China. Both countries are nuclear states and have ballistic or battlefield tactical missiles targeted at India. This imposes a burden on the intelligence agencies to provide accurate intelligence regarding the intentions, plans and actions of these countries in the quickest possible time. Reaction time is limited to a few minutes. Use of modern monitoring and interception technology and equipment, capable of 'strategic reach' is vital. Simultaneously, the armed forces require having the capability to move rapidly to man the forward defences. The task is complicated by the borders being inaccessible for much of the year and the terrain on India's side being tougher. The Kargil War brought into sharp focus the need for technologically-assisted surveillance as a non-subjective additional precaution and a safety layer. The intelligence output generated by technologically-assisted surveillance, like satellites and UAVs, would obviate recurrence of the possibility of information being suppressed from the higher national leadership. Effective surveillance and patrolling of these particular sectors is possible only with technology. Most stretches of the border with China, for example, are in tough, remote mountain terrain. It takes days before a border patrol can reach the frontiers. Technology-assisted border surveillance is of the utmost importance in such sectors to avoid being caught by surprise and suddenly find the adversary encamped within our territory. In addition to satellites, here a variety of radars would be required to ensure effective surveillance and these need to be backed by sensors and the extensive use of UAVs.

To effectively monitor its coastline, important naval and civil harbours and vital sea-lanes, India needs to deploy UUVs in addition to other maritime and satellite coverage.

The type of terrain and evolving nature of future wars in this region make it essential also for India's highest echelons of military and political leadership to reappraise their war plans, including for limited confrontation or conflict. In such a scenario air power would not imply escalation of the force level, but as a necessary component to playing a larger and more significant role in surveillance and action. It would simultaneously be a deterrent. In addition to retaining

the capability to lift large numbers of armed and equipped troops to remote posts, the air force should have the capacity to keep them aerially resupplied. It would need to be deployed as a first line of defence to delay the advancing hostile forces, frustrate opposing air forces and later to acquire and maintain air dominance. China's navy is also making rapid progress towards acquiring 'blue water' capability and it has already acquired a deterrence capability because of its large submarine force. To effectively monitor its coastline, important naval and civil harbours and vital sea-lanes, India needs to deploy UUVs in addition to other maritime and satellite coverage.

With the increase in the dimension of the threats, technology has anticipatedly found a larger role for itself. Technology in surveillance minimises the 'human' role thereby effecting manpower-saving, optimises the effective time-on-target, eliminates human factors like subjectivity, fatigue, etc, ensures almost instant accurate communication of developments via visuals or data, provides an additional source of real-time intelligence to the security forces, and captures incontrovertible data and images for evaluation.

India needs to accept the fact that terrorism targeted at it is unlikely to go away any time soon. Neither is the rough neighbourhood likely to change for the better in the foreseeable future. It is imperative, therefore, to evolve and implement modern surveillance methods suited to India's specific requirements. These surveillance methodologies include campaigns to raise public awareness, satellites, monitoring capabilities, instant wireless communications, face and voice databases and instant recognition capability, GPS, UAVs, UUVs, etc. In view of its large expanse of territory – both land and sea – India needs to use the entire range of modern surveillance platforms.

At the same time, in democracies such as India's, it is necessary to safeguard individual freedoms and privacy. It is imperative, therefore, to ensure that surveillance devices are not misused and that personnel using them are adequately sensitised. If necessary, appropriate legal safeguards and legislation need to be introduced.