Technology, Terror & a Thoughtless State

K.P.S. Gill
Faultlines: Volume- 3 October-1999

Policing in general, and counter-terrorism operations in particular have, in India, remained trapped in a low technology *cul de sac* for decades. Indeed, it would be safe to say that, on the threshold of the twenty-first century, a bulk of the police forces in the country are operating at technological levels that date back to the early twentieth century – or, at best, to the post-World War II colonial era. The primitive *lathi* (bamboo stick) and the bolt-action .303 are often the only instruments of authority that the police wields in an increasingly volatile context that comprehends constantly widening areas of escalating civil strife.

The situation has been compounded infinitely by terrorism and low intensity warfare that have become a permanent feature of India's internal security scenario over the past two decades. In this time, the technologies available to terrorists have improved continuously, albeit along a linear, accretionist scale, dramatically increasing their firepower, mobility, communications and surveillance capabilities. The response pattern of the security forces to these incremental gains has lagged significantly and consistently behind. Virtually no shift in the technologies available to the terrorists in any theatre has been presaged and countered in advance of its introduction into the theatre of conflict – even where the direction of change is clearly predictable and inevitable.

The introduction of cellular phones and later, of Iridium technology, are cases in point. India woke up to the cellular phone technology well after it was already entrenched, not only in the advanced nations of the West, but in most of the market economies of South Asia. The potential for misuse and abuse of cellular communications by criminals and terrorists was not only evident, but substantially documented in many of these countries well before the cell phone found entry into India. And yet, when these instruments were introduced into the terrorist inventory, or to run criminal networks (in some cases even from within the state's prisons), enforcement agencies responded with inept amazement, and it was some time before they began to turn the technology to their own advantage, setting up the requisite facilities to monitor calls on these networks and to identify and locate terrorists and criminals by tagging suspect connections. The legislative response has been even tardier. Far from establishing an adequate regulatory mechanism to prevent abuse of this technology, laws do not even provide for any failsafe methods to ensure that connections on cellular networks are not acquired under false identities, or anonymously.

The matter does not end here. The slow creep of Iridium technology, heralded by a long drawn international media blitz, caught intelligence agencies as completely unprepared and ill-equipped as its precursor, the cell phone. Another potential opportunity had been squandered, with the advantage, once again, surrendered to the forces of disorder and violence.

Similar patterns are visible in weapons technologies available to terrorists. Kalashnikov Assault Rifles, RDX and sophisticated timing devices, shoulder fired rockets and missiles, Unmanned Arial Vehicles (UAVs) for surveillance and attack – the introduction of each of these in the Indian theatre of low intensity warfare was easily predictable and inevitable, given regional geopolitics and the prevailing supply situation. Yet, on each occasion, the security

forces and with them, every other institution of governance, has been caught entirely unprepared.

The responsibility for this failure cannot squarely or correctly be laid on the security forces, the legislature, or any specific institutions or arm of governance. It is, in substantial measure, structural. The flow of information between the vast governmental apparatus of research and various field and operational agencies, as also state and central legislatures, is mediated – or perhaps more accurately, obstructed – by a bureaucratic maze that destroys all possibilities of proactive, or even efficiently reactive, response. The reverse flow of information from the field – regarding specific problems and challenges emerging from technological shifts in terrorist capabilities – is similarly inhibited.

More than a century ago, George Bernard Shaw had wryly remarked, "The British soldier can stand up to anything except the British War Office."[1] The statement describes perfectly the relationship between the Indian *jawan* and the formless, faceless bureaucracy that defines the conditions and circumstances under which he must serve. Bureaucrats by and large, prefer to deal with problems they understand and feel they can succeed with. In general, they do not understand low intensity warfare and terrorism, are largely ignorant of the ground situations in which forces are required to operate, and of the character and role of modern technologies in contemporary conflict. To the extent that this is the case, they tend to undervalue, neglect and ignore threats emanating from this direction, preferring conventional responses, such as the shuffling around of forces in a reassuring demonstration of their own power. That this demonstration feeds nothing more than their own flagging confidence is increasingly evident in the rising casualties terrorists are inflicting, both on civilians and on the SFs themselves, and in the widening gaps that exist between technologies and materials accessed by terrorists and those that have been made available to the SFs. Denial, I have had occasion to note in another context, marks the bureaucratic response to the emerging challenges of a world in transition. Bureaucrats lack, and have stubbornly refused to acquire, the specialised skills that contemporary technological changes have made imperative, turning themselves, at a stroke, into ill-adapted anachronisms fated to extinction.[2] The problem is not, as most bureaucrats would immediately argue, one of the allocation of scarce resources. It is primarily a problem of perceptions, and of the growing inadequacy of a predominantly ‘generalist’ bureaucracy in an increasingly specialised world. Most of our administrators and policymakers lack the requisite technical knowledge, or even the general awareness of technological shifts occurring in the field of conflict and, much more, on the outer periphery of technological innovation and research.

At least part of the problem is also the contempt in which the lives of personnel in the uniformed services are generally held. The predominant attitude appears to be that, since these men have volunteered for service in the police, para-military forces, or the army, they should accept even the most extraordinary – and often avoidable – risks and hardships without complaint, and must expect to be killed. This characterisation may sound uncharitable to all but those who have actually been involved in the thankless task of negotiating with the bureaucracy on behalf of the fighting men of this country.[3]

I have, in the past, cited the example of the impact of the introduction, in May 1987, of the Kalashnikov (AK-47) in the Punjab terrorists’ arsenal, and my requests for an upgradation of the SF’s firepower.[4] The police and SFs were, at that time, armed with the obsolete .303 Lee

Enfield rifles, or the equally obsolete bolt-action 7.62s. The CRPF were slightly better equipped, with 175 Self Loading Rifles (SLRs) per battalion – although the SLR was no match for the AK-47. When no new supplies seemed forthcoming, I requested that the large number of Light Machine Guns (LMGs) then lying unused in police armouries all over the state be deployed against the terrorists. Completely ludicrous arguments were advanced to obstruct this move – among them the assertion that such weapons may be used by the police against unarmed crowds and would contribute to the possibilities of 'human rights violations'. This reflected such ignorance of police procedures that, had it not been articulated at the highest levels of governance, it would not even deserve explanation. The fact is, every police station is armed with a mix of weapons, and each of these is issued for specific use. Teargas would be issued for mob control; rifles, only when these were required. I cannot imagine a police officer in India who would authorise the issue of machine guns for any kind of crowd control or management of unarmed demonstrations. Suffice it to say that, eventually, after the LMGs were deployed, far from these being used against civilian crowds, the SFs in Punjab never found it necessary to use any kind of firearms for crowd control. This was the case even through the turbulent 1990-91 period when tens of thousands of agitated Sikhs gathered in quasi-religious demonstrations to protest the "martyrdom" of various prominent terrorists.[5] The fact is, better arms and equipment with the SFs do not lead to human rights violations or police excesses. If anything, the reverse may be true, as inadequately equipped forces confront a better equipped enemy, and succumb to the inevitable frustrations of a war of attrition which they see themselves fighting with their hands tied down.

Take another example. For the past decade, on an average, nearly a thousand security men have been killed each year – most of them in terrorist conflicts, or while confronting well-equipped criminals from organised networks. India's vast technological resources, research establishments and immense manufacturing capacities are capable, we are constantly reminded, of putting satellites into space, of building nuclear bombs and missiles for their delivery across continents, and of creating supercomputers. Yet they cannot, or have not been tasked to, produce a lightweight, safe and economical bulletproof jacket that could protect its men in action. Instead, police administrators in the past have been forced to depend on their own inventiveness and the resources of the market to fabricate a crude jacket of steel plates. This may weigh as much as 9.5 kilos (the maximum permitted by MHA specifications), inhibits movement, and offers limited protection against the high density fire of the Kalashnikov assault rifle. The DRDO has developed a BP Jacket that weighs 7.8 kg, and this is now issued to many of the SFs. Is this the best we can do against the imported jackets that come up to a few hundred grammes, and are safer?

This is critical. The fighting capabilities of a soldier are not measured in terms of firepower, mobility and communications alone – though these may be the most important parameters. Indeed, bureaucratic indifference and neglect is reflected most dramatically and persistently in the personal effects and protection that are standard issue to each *jawan*. Dramatic changes in design have resulted in the development of rucksacks that can redistribute weight from the shoulders to the waist, and could significantly diminishing both the burden and discomfort of carrying the 5 to 20 kilo standard issue that each *jawan* must bear in various situations, and at little incremental cost. But the forces in this country have failed to move beyond the crude World War I backpack – the *pitthoo* – that cuts deeply and painfully into the shoulders if carried for any length of time. Nor has there been any change in the heavy, clumsy and comfortless

boots that *jawans* wear. Only a fraction of the personnel serving in high altitude areas are issued imported alpine jackets; most must make do with the cold comfort of the bulky and relatively ineffective Indian issue. The recent Kargil conflict exposed the somewhat bizarre predicament of the army of a 'Nuclear nation' temporarily paralysed by the lack of suitable mountain footwear for its soldiers.[6] Hasty imports were needed to resolve that problem. And yet, India has been fighting the highest altitude war in the world on the Siachin Glacier since 1984; paramilitary forces have also been fighting terrorists at high altitudes in J&K for nearly a decade. Can we not even produce a suitable pair of shoes for our fighting men?

The question is not of technological competence, but of attitudes. The fact is that, even today, the *jawan* is thought of as a sort of combination of *coolie* and cannon fodder, not only by policy makers and bureaucrats, but by many of his own officers as well, and by much of the public at large (except in brief periods of national crisis where excessive sentimentality dominates the public response). These attitudes have been able to survive at the threshold of the 21st century largely because a burgeoning population of the rural poor keeps our armed forces supplied with poorly qualified manpower, and because we have, till now, been able to measure our strengths purely in terms of crude numbers.

This, however, will not do in the new century. We are now on the verge, not only of an unprecedented acceleration, but of a radical discontinuity in the linear trajectory that terrorist technologies have followed over the past decades. Indeed, we must now prepare for a paradigm shift in the very nature of low intensity warfare and terrorism. The stubborn courage, the dedication, the unquestioning obedience and spirit of sacrifice of our Forces may have sufficed in the past, but these will need to be backed with far greater technological competence, equipment and infrastructure – and more importantly, far greater prescience and planning – if we are to succeed against the emerging "capacity for hyperviolence"[7] that is passing progressively into the hands of the terrorists.

The character and potential scale of this "capacity for hyperviolence" has not yet been adequately understood by our bureaucrats and policymakers. The sheer enormity and swiftness of the changes that threaten us in this sphere make not just the decisions of the past, but the decision-making process itself, entirely obsolete. Alvin Toffler notes in connection with the 'non-state actors' in the emerging international political scenario that:

Governments find it increasingly difficult to deal with these new actors on the world stage. Governments are too bureaucratic. Their response times are too slow. They are linked into so many foreign relationships that require consultation and agreement with allies, and must cater to so many domestic political interest groups, that it takes them too long to react to initiatives by drug lords or religious fanatics and terrorists.[8]

The terrorists themselves, however, are entirely free of constraints or compunctions.

By contrast, many of the Global Gladiators, guerillas and drug cartels in particular, are non- or even pre-bureaucratic. A single charismatic leader calls the shots quickly, and with chilling – or killing – effect.[9]

The Global Gladiator's capacity for hyperviolence is, today, finding increasing potential for expression in two distinct trends: i. the rapid, though linear, improvement of technologies available to terrorists and the widening gap between these and the technologies available to counterterrorist forces; and ii. the radical leap in technologies for low intensity warfare –

including weapons of mass destruction (WMD) – that is now imminent. Both these will demand unique patterns of response, and neither can be neglected, if we are to survive as a nation. Our success will depend entirely on our ability to understand and predict the character and dimensions of these changes, and to initiate responses well in advance of their realisation.

Linear Developments

The primary sources of arms and communication technologies for terrorists in various parts of the country, till the mid-eighties, were weapon snatching, theft or robbery, raids on police armouries, ambushes on SF patrols and convoys and a trickle of arms and equipment acquired in the black market abroad and smuggled into the theatre of conflict. There was, consequently, a certain symmetry in technologies available to terrorists and those used by the SFs, with an advantage of numbers and assured supplies accruing to the latter.

Pakistan's direct intervention in terrorism on Indian soil – specifically in Punjab – in the mid-eighties brought about an irreversible change in this situation. For the first time, agencies of a nation-state, with their enormous resources and legitimate access to high military technologies, guaranteed supplies to non-state terrorist groupings. For some time, these supplies had to be paid for by the militants, usually in funds mobilised through extortion or the drug trade; after 1989, however, they not only came free of cost, but in a far greater number than ever before. Initially, the sheer enormity of this change was not realised in India beyond the limited circle within the police and military leadership who had to confront and counter the escalated threat. Indeed, even today, when Pakistan's covert agencies are offering weapons to any and every militant group – irrespective of ideology and wherever they may be active, in J&K, the North East, even Bihar and Orissa – there are many in the civil administration who persist in the belief that the problem can be confronted locally, and through conventional law enforcement measures based on assumptions of the minimum use of force.

A decade-and-a-half ago, terrorists in India had access to an arsenal that comprehended single shot rifles, pistols, a few SLRs, carbines and sten guns, hand grenades and crude bombs. Today, they have graduated to sophisticated assault rifles, high velocity telescopic sniper rifles, Light and Medium Machine Guns, armour piercing incendiary ammunition, RDX and PETN based explosives with complex triggering devices including trip-switches, remote control mechanisms, light differential relay switches, high frequency based triggering devices, time pencils and electronic timers. They have access to virtually unlimited supplies of ordinary and anti-personnel grenades, anti-tank and anti-personnel mines, grenade- and rocket-launchers, mortars, anti-aircraft guns and Stinger surface to air missiles. Sophisticated communications and surveillance equipment, including unmanned aerial vehicles (UAVs) are also in use. They are now reports that some form of chemical weapons may also have been introduced into their armoury, though these have not yet been used.[10]

The *rate* of improvement in the terrorist armoury, moreover, has undergone continuous acceleration, keeping pace with the most recent developments in the technologies available on the international market – both legal and underground. In contrast, the state's response remains inexcusably sluggish and often erratic, if not entirely whimsical.

In the post-Kargil era, this judgement may seem somewhat harsh, especially in view of the quick decision to upgrade equipment for counterinsurgency operations and the defence of the LoC at a proposed cost of almost Rs. 40 billion. If anything, however, this decision merely

confirms the *ad hoc*, knee jerk character of our responses, and provides a suitable example for analysis of the standard governmental response in the aftermath of a crisis.[11] The projected 'upgradation,' reportedly to be realized over the next seven years (a fairly long period in terms of present rates of technological change), represents little more than a lavish buying spree that will bring in automatic grenade launchers, sniper rifles and flame throwers from Russia, multi-grenade launchers and mine-protected vehicles from South Africa, under-barrel grenade launchers from Bulgaria, C-90 disposable rocket launchers from Spain, and bullet proof vests from UK and Germany.[12]

This is, presumably, a partial and unconfirmed list of the actual acquisitions to be made. Consequently, it would be infructuous and inappropriate to go into the merits of any of the items on the proposed procurement list. There are, however, several *prima facie* problems with the 'upgradation' plan.

This is a recurrent theme in technological acquisitions for the army and SFs. Part of the problem, of course, is the pervasive blight of corruption, as a result of which the acquired systems are not subjected to a transparent and objective process of evaluation. The greater problem, however, is a failure on the part of bureaucrats and technical advisors who act at a sanitized distance from the actual theatre of conflict, and are, consequently, in no position to make a correct evaluation of the utility of specific systems.

Weapons and technologies have to be situation and threat specific, and should facilitate a resolution of an existing or emerging problem in the quickest possible time, with minimum damage. During the Punjab campaign, an elite commando group was deployed for night ambushes in Tarn Taran in 1989. They were expected to have an overwhelming advantage, since they were equipped with night-vision devices. Unfortunately, the experiment was a failure, with the number of casualties canceling out on each side. This was because no one had anticipated the impact of artificial light on night-vision devices, and most of the villages in the Punjab are electrified. The commandos went in blind into an engagement where they thought they would have the devastating advantage of sight over their adversaries.

The problem was, and frequently remains, that the selection of weapons and technologies is based on theories and books, not on direct discussions with field commanders or on operational requirements and experience.

1. It is evidently based on perceptions of what is required to counter the current patterns of attack to which the SFs are being subjected and the levels of technology presently available to the terrorist. To the extent that these acquisitions are to reach the field in phases over the next seven years, many of them will be outdated and ineffectual by the time this happens. Any long-term acquisition would have to be based on projections – however tentative these may be – of emerging technologies, and must attempt to outstrip the terrorists' rate of acquisition of technologies if they are to be effective. I cannot think of a single example where this has been the case in the sphere of counter-insurgency technologies in India.
2. To the extent that this is a 'wish list' largely dreamt up by military and civilian bureaucrats at Delhi, many of the acquisitions may prove ineffective or inappropriate in the field. There are already reports in the Press, for instance, that suggest that the

anti-mine vehicles purchased from South Africa, some of which have already been deployed in the field, are unsuitable for J&K – their principal destination – since they are "built for the plains and the cabin is so high up that it is almost impossible for the driver to see a road in mountainous terrain. It requires an escort party to show the way."[13]

3. Many, if not most, of the technologies that we are shopping for all over the world are available, or can be developed, within the country at costs that would prove to be a fraction of the price of imports. To the extent that they are made to specifications defined in the field, and can be continuously modified to confront emerging shifts in the pattern of terrorist movements and attacks, they would meet the short-term requirements of the forces far better than unitary systems imported from foreign manufacturers.

It is important to remind ourselves once again, in this context, that not all the proposed imports are high-ended weapons or communication systems, and that many of the very expensive (and reportedly overpriced) items – including the anti-mine vehicles – have already been developed and used within India in other theatres. The problem, however, cannot be resolved within the present institutional system. The flow of technologies from scientific and research establishments has been fitful and capricious, often as divorced from the ground situation as the 'wish lists' of the Central bureaucracy. The Defence Research & Development Organisations (DRDO) alone, I believe, would be sitting on an entire treasure house of technologies that could be translated into force multipliers on the ground. But what actually reaches the Forces is defined through the same convoluted, irrational bureaucratic process that robs it of all possible efficacy, and condemns immense resources and research efforts to absolute futility.[14]

The problem, moreover, is not just of bridging the immense gap between India's premier defence laboratories and the SFs in the field. Indeed, there is much that could be done at levels of innovation of which students in our technological institutes and colleges are perfectly capable. It is my firm conviction that many of the required technical inputs could be sourced locally, if a mechanism could be devised where students and faculty of these institutions are specifically tasked to solve problems locally confronted by SF commanders. There is a story doing the rounds – apocryphal, no doubt – of a police officer in J&K who used the skills of a local television repair mechanic to fabricate a crude though effective – and very cheap – Direction Finding Device to identify and locate militant wireless facilities.

Unfortunately, none of the SFs or enforcement agencies in India has the wherewithal, the orientation, or, ordinarily, even the authority, to make their own technological choices. More than six years after terrorism was defeated in Punjab, the lessons of that campaign remain poorly understood and largely ignored. Nevertheless, the salutary consequences of programmes that place actual, even though limited, technological initiatives in the hands of the SFs, were more than adequately demonstrated there.

With mounting casualties under a sustained, increasingly sophisticated and devastating terrorist offensive, a small "special cell" was set up in February 1990 under the charge of K. K. Attri, DIG, and in coordination with Dr. Gopalji Misra, Director, Forensic Sciences Laboratories (FSL), Punjab. The Cell was to undertake a continuous and systematic assessment of the operational skills of the terrorists and the technologies available to them. The Cell also

established a working alliance with universities, national laboratories such as the CSIO and TBRL as well as with research facilities of the DRDO all over the country. Liaison was also maintained with the National Security Guard (NSG) and the Special Protection Group (SPG).

Traditionally, the FSL had only been involved with casework and the related forensic examination of evidence. It now undertook the study of terrorist weaponry, explosives and initiators, and mobility aids, including optical devices, vehicles, etc. On this basis, a thorough threat assessment was made, and the deep involvement of Pakistan's covert agencies in arming the Punjab terrorists was also established. This evaluation was collated and disseminated through the operational, monitoring and planning levels in the Police and other wings of Government involved in the war against terrorism, and contributed significantly to logistics and operational planning of the SFs. This was, to my mind, a unique and unparalleled experiment in this country. It was, however, only a beginning.

The Special Cell also began a process of developing appropriate technologies to confront specific challenges posed by the various weapons, communications and other systems available to the terrorists, as well as solutions to specific problems that arose out of their *modus operandi*. The FSL's work included R&D on bullet-proofing materials, including steel, glass, Kevlar and polycarbonates, as well as projects to develop optical, electrical and electronic devices. Some of the innovations proved exceptionally helpful in the fight against terror, either resulting in specific breakthroughs, or minimally ensuring dramatic cost reductions and improved operational effectiveness. They included the following:

The impact of such innovations was dramatically illustrated by the development of the BP Tractor. The sugarcane fields in Punjab gave the terrorists excellent cover for ambush and escape, and had proven to be a major headache for the police. So great was their advantage that the militants forced farmers on pain of death to sow sugarcane all along the roads and their clandestine routes. After an attack, the terrorists would simply run into the fields, and if the police tried to follow, they would simply be picked off one by one. When the first BP Tractors were pressed into operations, this advantage simply vanished, and the sanctuary of the sugarcane field was lost, forcing irreversible tactical changes on the terrorists. Later, the terrorists got hold of armour piercing bullets and inflicted a few casualties on policemen in the armoured tractors, thus neutralising the advantage. By then, however, the time for 'sugarcane terrorism' was over.

1. The Infrared Filter Glass Torch: Toughened glass was coated with a combination of dyes to check the visible light and allow the filtration of infrared radiation. This coated glass was used on dragon lights and allowed for visibility of about 250 metres with the help of night vision goggles during dark nights. A heavier coating on such glass used over aeroplane landing lights increased visibility upto 700 metres. Each such light, fitted into portable wooden boxes, and connected to two 12 volt truck batteries, was found extremely useful for watching terrorist movements at night without giving any indication of the police position.

2. Infra-red filter head- and parking-lights: The headlights and parking lights of police vehicles were similarly treated to permit the vehicles to be driven at night without disclosing their position from a distance.

3. Parabolic sound enlarger: this device allowed tracking of the movement of terrorists during the night in forested areas or across water bodies through the directional focusing of a parabola that amplified sound that could be monitored on headphones.

4. Mechanical clock detector: to detect mechanical timing devices for bombs concealed in closed packages, boxes or luggage. The device was developed at a cost barely 7 per cent of similar devices available on the market.

5. Electronic timer detector: While the mechanical clock is relatively easy to detect, the silent electronic timer is a greater challenge. The detector could locate a timer concealed in any kind of packing, behind walls, and from a distance of upto 15 inches. In 1992, when this device was developed by the FSL, no similar mechanism was available in the international market. The first such device to be made available commercially came in 1994, with a price tag of Rs. 290,000. The Punjab Police detector cost Rs. 10,000.

6. Poison detection kit: A simple kit that could be easily operated by a police constable, and which gave its results within five minutes, was developed to identify potassium cyanide or arsenic in water or food.

7. Country-made bullet proof jackets: Various steels were tested and tempered to develop plates that could protect against the AK-47. Crude jackets, with these steel plates stitched into in strong cloth provided a degree of protection to a large number of SF and police personnel and, despite their weight, contributed enormously to their operational efficiency and confidence. These jackets cost a fraction of factory made BP jackets, and the design is still in use in other theatres of LIC.

8. Bullet Proof Mobile *Morchas*: Three plates of 6mm tempered steel were shaped into a simple structure that could be carried and installed anywhere through a hooking system. Each plate was provided with a firing port. These mobile *morchas* or posts proved very useful during encounters/ambushes, and were strong enough to stop AK 47 bullets. A pair of such plates (size: 46"x27") was also sufficient to protect an LCV passenger vehicle or Gypsy.

9. Bullet proofing of vehicles: Steel easily available on the market was tempered to produce economical bullet proof Gypsies, Jeeps, Ambassador cars, LCVs and police trucks. At the peak of terrorism, Punjab had more than 650 BP vehicles. Bomb protected flooring also saved lives against the increasing use of IEDs and landmines during the later phases of terrorism in the State.

10. R&D on BP materials: R&D on materials, including various steels and alloys, glasses, composite materials and polycarbonates, led to the replacement of Kevlar pads on the floor and in the ceiling of Ambassador cars, resulting in a saving of as much as Rs. 100,000 per protected vehicle. Tempered steel, similarly, reduced the cost of bullet proofing of LCVs and police trucks, as compared to the cost of Jackal steel previously in use. The design of innovative door-catches for protected vehicles added to their security under attack. The replacement of the Ambassador engines by an Isuzu 1800 petrol engines acquired in the second hand market also proved to be a highly cost-effective way of improving efficiency.

11. R&D on Ammunition: At each stage, exhaustive studies were carried out on various types of ammunition used by terrorists in order to develop appropriate protection against them, and save valuable lives.

12. Simple and panel periscopes: Simple periscopes with three backup mirrors were developed for observation from secure positions without exposing the observer. The system survived even if the mirrors were hit twice, as the third angled mirror remained intact.

13. Protective viewing window: A protected, BP viewing window, with a visibility angle of 140^{o}, was fitted into BP patrol vehicles and BP mobile *morchas*. This constituted a quantum leap over the periscopes that had been devised earlier.

14. Riot Control Shields: made out of polycarbonate shields ranging between 4mm and 12 mm. The material did not break even if beaten with iron rods and could not be penetrated with a knife. Polycarbonate sheets of 6 to 8mm thickness could stop 12 bore shots and lead projectiles from small fire arms, including revolvers and pistols.

Some of these innovations would, to those who are focused on the hi-technology end of defence research, appear to be crude, even primitive – though others involved fairly sophisticated R&D with special materials and alloys. It is, however, impossible for such distanced observers to estimate the sheer and overwhelming impact that each of these developments had in the fight against the terrorists in Punjab.

It would be equally difficult for such observers to imagine the sheer enormity of the constraints under which these developments took place. There was unrelenting resistance from the bureaucracy and audit institutions to every unorthodox initiative, often forcing absolutely ludicrous decisions. A small group had been constituted to work on steel wool, which would have been lighter and stronger than the material then being used for bullet proofing. The project had to be given up, largely due to an ingrained fear of innovation. The in-house cost of effective bullet proofing of a vehicle was under Rs. 400,000. Yet, a costlier alternative, involving the established system of open tenders and outside manufacture, had to be adopted, since audit objections would subsequently be raised against a manufacturing activity that did not fall within the department's mandate. Indeed, such strong inhibitors to unorthodox development exist within the prevailing administrative system that it was well nigh impossible to secure funds for such projects.[15]

This system will have to be dismantled if the hyperviolence of future terrorism is to be effectively neutralised. A continuous system of unmediated coordination between field commanders and R&D personnel at various levels will have to be created so that the time lag between emerging trends in terrorism and counterterrorist initiatives is diminished. This will demand extraordinary efforts, since the technological advantages of state players are being progressively eroded by the terrorists' free access to advanced technologies.

There is, consequently, a need for a dual response that requires both local level facilities and efforts that do not go beyond tinkering with existing technologies, on the one hand, as well as highly sophisticated research at the very limits of contemporary scientific knowledge, on the other.

This, however, will not be enough. It is no longer sufficient to constantly run close on the heels of the terrorist. He must be overtaken and outmanoeuvred if his increasing and potentially devastating power is to be neutralised.

In general, CT (Counterterrorism) planners have been successful when they were able to match or exceed the technological skills of their terrorist adversaries… (T)he forces of order no longer enjoy an inherent advantage in the competition with those who would prevent the orderly functioning of society. Therefore, their success will not be a function of privilege or position but rather the reward for their greater ingenuity and resourcefulness.[16]

This requires even deeper levels and more complex structures of coordination and research, and a technological perspective that must define – as minutely and accurately as is humanly possible – the direction and character of future weapon systems and enabling technologies that will be deployed in low intensity wars. Once such a perspective has been constructed – and even as it is constantly reviewed and revised – research, developmental and manufacturing initiatives must create the technologies to counter these systems well before they are accessed by the terrorist. In war, surprise is a critical ingredient for victory – and it is imperative that the Indian security establishment is not taken by surprise.

As stated earlier, the mere development or theoretical availability of a technology has no impact on the ground. Systems for its timely production and deployment are just as important. In this, the private sector can and should be co-opted, though some precautions may be necessary to ensure that sensitive technologies are not exploited for purely commercial ends. Nevertheless, it is important to remind ourselves that those who draw their salaries from the state do not have a necessary monopoly on patriotism, nor, for that matter, an exclusive duty to fight the nation's wars.

Our approach, however, must comprehend much more than weapon systems and technologies. While it is well beyond the scope of this paper to discuss the issue in any detail, it is essential to recognise that the manpower resources and training requirements that will create the low intensity warfighter of the 21st century, will be radically different from the ill-equipped and poorly trained *jawan* of the 20th. It must, equally, be recognised that changes in manpower and training policies today will significantly impact on the constitution and character of the security forces several years hence. There is, consequently, no more time to waste in this regard.

Leaping the Abyss

Procrastination is a luxury that we can afford even less in view of the "great leap forward" that weapons of mass destruction now offer the terrorist. The slow-bleeding warfare that has been inflicted upon us, particularly over the past two decades, has cost the nation thousands of lives, billions of rupees. Yet, even at our present levels of engagement, it is entirely possible to contain its impact within levels that are considered – by an increasingly brutalised and unresponsive public and political leadership – "acceptable", and without a compelling proximate threat of national disintegration. All this changes with the paradigm shift that must be anticipated in the technologies of terror in the new millenium.

The Pokhran II tests of May 1998, and the retaliatory demonstration in Chagai, heralded a new phase in the precarious strategic equilibrium that prevails in the Indian subcontinent. A great deal has already been written about this momentous development and the advent of the perilous 'nuclear age' of Asia. The debate, however, remains trapped within the paradigms of deterrence

defined by the West over decades of the Cold War, and fails to distinguish, or even acknowledge, the unique circumstances that prevail in South Asia.

Critically, current Indian strategic perspectives on the issue end with capabilities to ensure a retaliatory strike that would inflict destruction that the "aggressor will find unacceptable" if nuclear weapons are used against us. This is nothing but the regurgitation of classical deterrence postures and the infamous Mutually Assured Destruction (MAD) doctrine – a doctrine that, no doubt, kept the superpowers out of nuclear conflict for nearly five decades of an intense Cold War that often expressed itself through proxy wars and direct confrontations in other countries. Nevertheless, it is important to understand the circumstances that made MAD so effective in assuring nuclear peace. The first of these was the fact that all nuclear powers of the Cold War period had long standing and entirely stable institutions of governance with clear chains of command and elaborate systems of checks and balances that forced a rational decision on all the players in this confrontation. Secondly, the projected nuclear strikes in case of a conflagration were of such an intensity and number that there were no possibilities whatsoever of either nation surviving; indeed, there was little chance of life – certainly human life – surviving on this planet. In effect, the calculations played out in the war games of both the superpowers engaged in the Cold War ensured an absolute No Win situation. There was no calculus or alternate rational scheme that could tempt either to risk actual use of their arsenal, whatever the aggravation.

The situation is made infinitely more complex by the advent of a range of other weapons of mass destruction (WMD) – including chemical and biological weapons – where the barrier to acquisition is much lower than the one that inhibits access to nuclear technologies. The destructive potential of these weapons is well known in a restricted circle of scientists and strategic scholars in India, but the larger community of administrators and policy makers remain oblivious of their dangers. A small package of chemical agents, for instance, is estimated to be 40 times more effective as a weapon than a comparable package of conventional explosives.[17] But this is just an insignificant fraction of what biological weapons can do.

To gain an understanding of the lethality of these toxins, the brevity of their production time-frames, and their ease of concealment, consider that with merely a flask of culture medium and a few anthrax spores, a terrorist with college-level laboratory skill can produce one kilogram of anthrax bacteria in just eight days. One half a gram – about 0.02 ounces – comprises enough doses to kill five million people. Butulinum toxins are equally fatal.[18]

Indeed, "college level laboratory skills" may also be fairly redundant, as "rogue states… wield nuclear, biological, or chemical weapons through the vehicle of terror surrogates as a practically untraceable tool for covert proxy war."[19] A chilling reminder that this is no Cassandra's call is the fact that the list of nations known to currently possess biological weapons includes a number of unstable regimes and many that are present sponsors of terrorism. The list of biological weapons nations includes Russia, Iraq, Iran, China, North Korea, Egypt, Syria, Taiwan, Israel, and, critically, Pakistan, but "The threat lies not in the length of this list but in the fact that many of these nations reject the political and territorial status quo and are more likely to use such weapons to advance an aggressive agenda."[20]

The assumptions of classical deterrence theory, consequently and obviously, cannot apply to the Indian sub-continent. Classical deterrence may work most of the time against stable nation states, but it has no relevance to the non-state nuclear weapons player, or, for that matter, to a

rogue state acting through such a player. These are very real possibilities and may be realised in a number of alternative scenarios, all of which cannot be examined here. Nevertheless, there are two explicit dangers that need to be immediately recognised.

For those who believe that they are fighting on God's Command and for the establishment of His Empire on earth – and believe this with absolute and uncompromising ardour – the lives of their fellow men, and indeed their own lives, do not have the value that is placed on them by liberal-democratic rationality. Nor indeed does the *mujahiddeen* mindset yield to the imperatives of traditional nationalism. It is entirely possible that, were such individuals placed in positions of control over nuclear, chemical or biological weapons of mass destruction, they would accept the possibility of the annihilation of their own nation if they could believe that the 'Empire of God' (or, bluntly, the 'Islamic World') could be expanded.

Such a calculus would, moreover, be applied in a situation that differs radically from classical deterrence assumptions in that the scale of destruction projected is lower. The intended damage would substantially be confined to India and Pakistan, though it may flow across their borders in limited measure. Nevertheless, it would had the potential to "Free" the subcontinent of the power of the "Unbeliever" and open it up to a final "Islamic Conquest" from Central Asia.

It must be recognised that the influence of what is described as Islamic Fundamentalism is increasing enormously in Pakistan and, if present trends continue – especially with the consolidation of the *Taliban* regime in Afghanistan – it is inevitable that they will eventually seize power in that state, irrespective of the opinions and desires of the more moderate population who may incline towards peace with India.

While no quantitative probabilities can be assigned to the possibilities of the use of WMDs against India by such a future regime, it is essential for acknowledge this possibility, and to discover means to defeat the calculus of this millennial rationality.

1. The first of these arises out of the character and the increasing influence and stridency of what is described as 'Islamic Fundamentalism and Militancy' in the region. As with all millennial faiths, the calculus of those who subscribe to such an ideology differs strikingly from what we – and classical deterrence strategies – would regard as rational. Nevertheless, the 'millennial rationality' has its own internal coherence and must be understood and confronted as such.

2. A second threat, possibly more insidious than the one described above, arises out of the character and patterns of Pakistan's sustained strategies against India over the last decade and a half, and is exacerbated by the new paradigm of the combined use of regular forces and terrorists that has been exposed through their recent actions in Kargil. It is certain that – irrespective of the outcome in Kargil – Pakistan will continue in its efforts to expand the sphere of low intensity warfare within India. If any regime in Pakistan were to convince itself that regional, communal and political fragmentation in India had reached a stage where the destruction of a few critical centres of authority would effectively ensure the disintegration of the nation, it is possible that it would gamble on the use of small nuclear devices – the notorious "suitcase bomb" – or other WMDs smuggled in and deployed by terrorists.

Such a calculus is not based on – and does not need – millennial rationality, though such thinking would certainly heighten the dangers. The power elite and an influential segment of the Pakistani Establishment conceive of India's disintegration as an end in itself, even if no territorial advantages accrued to it. To the extent that such a strategy would also offer the possibility of at least partially escaping responsibility by crediting such actions to 'Freedom Fighters' within India, it becomes all the more attractive.

We cannot pretend that there are any easy solutions to these problems. Nevertheless, there are general directions that need to be explored if we are to obviate the threat they constitute.

The first of these refers to the boundaries of our strategic perspective. Clearly, it cannot end with an assured retaliatory strike, for the extremist calculus would not necessarily be deterred by such a possibility, nor, indeed, would it be clear as to who such a strike is to be directed against.

Only if those who contemplate nuclear or biological aggression against us are convinced that India would not only survive, but that their own sphere of influence would significantly shrink, would such extremist elements be deterred against an adventure using WMDs against us. Such a deterrent must be based on the creation of political, administrative and institutional structures, processes and procedures that would survive such a catastrophic strike. These must comprehend the identification of possible target cities, plans for evacuation, the containment of a panic that could reach unprecedented proportions, the restoration of order within the surviving populations of these target cities and provision of medical and other relief to them at a scale that has never been envisaged in the past, and the preservation of order in the most far flung areas of the country. Equally, they must include a clear chain of surviving command and a plan for retaliatory strikes based on prior identification of possible perpetrators, and mandatory punitive protocols. While such identification may not be perfectly adequate, knowledge that such intelligence exists would work as a deterrent on the entire and highly interdependent network of terrorist organisations and their sponsors.

This is, clearly, only a crude outline of what is needed, and an enormous exercise would be required to define and implement the necessary plans. Our strategic perspective must, however, at least identify the directions that such plans must follow and initiate the processes that would lead to their realisation. Such an exercise has already been initiated in nations where the terrorist threat is at much lower levels in comparison to the situation in India.[21]

There is, in the observations above, an overwhelming focus on the threat of unconventional aggression by Pakistan and by militants based in, or connected with, that state. This is a product, perhaps, of our present situation, as of a personal perception. This threat, however great it may presently be, does not exhaust the dimensions of the dangers of attack by WMDs that India faces. Indeed, our future strategic doctrine must identify potential adversaries and define their varying calculii – every adversary would not use the same calculus and our projected responses must accommodate these variations. Nor, indeed, is it sufficient to base our strategic perspectives on present perceptions of who our potential adversaries are. In a rapidly changing world, these relationships will shift, even as access to unconventional weapons and delivery systems widens. Each such possibility needs separate examination if it is to yield valid strategic options. And a continuous and intense exercise to identify and play out each potential scenario must be undertaken if we are to defend ourselves against every emerging eventuality.

Virtual Wars

There is one more danger that is currently exercising counterterrorism strategists across the world. It is variously referred to as Cyberwar, Netwar, or Information Warfare and Terrorism. Its potential for destruction in the coming century is immense. Scenarios have been drawn up that link narrowly targeted attacks with a cumulative potential to disrupt complex electronic command and control systems across continents.[22] The destructive potential of cyberwarfare is expected to increase exponentially with the progressive computerisation of all systems in business, social services, governance and defence. The degree of vulnerability can be estimated by the fact that, during recent tests, computer specialists demonstrated their ability to crash the computer systems of both the New York Stock Exchange and the social security system. One expert estimates that as many as 80% of the Fortune 500 companies have been electronically penetrated by hackers.[23] A 1997 survey by the Computer Security Institute and the FBI's International Computer Crime Squad found that 75% of the respondents reported financial losses due to various computer security breaches.[24]

Even the most secure defence establishments have been hacked, and this includes the US military nerve centre at The Pentagon where computer systems were reportedly under "an unprecedented and concerted series of external attacks" in March this year.[25] Several successful breaches are known to have occurred, including one by an "18-year old Israeli computer enthusiast with a lot of time on his hands, and two teenagers from California who were using readily available software tools downloaded from the Internet to discredit the Pentagon's computer security."[26] Representative Curt Weldon, who chaired the subcommittee of the US House Armed Services Committee that heard testimonies relating to the US Defence Department computers is reported to have stated, "This Y2K thing is a piece of cake compared to this."

Cyberwarfare, moreover, creates another critical shift in the character of terrorism. The idea of the 'one man army' is more completely realised in the identity of a well informed hacker than it ever has been through any other technology. A single individual, with the right knowledge and skills, and working on a simple computer hooked to the internet – a computer indistinguishable from ones commonly used by students, professionals or businessmen, and freely available at an extremely modest, and declining, price – could realise his own anarchical agenda without help from, or complicity of, any other agency or group. This would make detection difficult, if not impossible, and there would be no physical risks even at the moment of 'engagement'. And the damage could be done to massive national infrastructure, commercial, information and defence systems across continents. This single factor has the potential to force fundamental and comprehensive revisions in our concepts and strategies of the future of counterterrorist warfare.

In India, all this may still seem to be in the realm of science fiction. Computers have, of course, entered the office space in every sector of the economy, of governance and of defence. But they are, as yet, far from the integrated systems of command and control whose disruption could bring the life of a nation to a standstill. Indeed, at this point of time, even where computers are integral to critical operations, their disruption would, at worst, cause a temporary setback before operations were resumed under traditional technological and command structures. Cyberterrorism, consequently, remains a distant prospect, given low levels of computerisation in most core sectors. 'Information Warfare' is, as a result, widely interpreted

by Indian planners within the traditional categories of propaganda, with the difference that, now, a new electronic medium is available.

This situation cannot, of course, persist for long. If India is to follow a vigorous programme of economic development, it will have to adopt contemporary technologies – including computerisation and global networking of all critical operations. And as it does so, its vulnerabilities to the malevolent hacker will grow.

It would be foolhardy to believe that we will have time enough to respond when the danger manifests itself. Indeed, it is now that preventive action must be initiated, so that safety is built into the very architecture of the nation's expanding private and public networks – to the extent that this is possible. How this can be done is, of course, a matter for the experts. That it needs to be done, however, is something that bureaucrats and planners will have to realise and concede, before the experts can get down to their jobs.

The cumulative impact of technological change in terrorist warfare is truly terrifying and contains within it the seeds of the destruction of many a nation at the hands of even the most insignificant minorities.

In a world of satellites, lasers, computers, briefcase weapons, precision targeting, and a choice of viruses with which to attack people or computers, nations as we now know them may well find themselves up against potent adversaries, some no more than a millionth their size.[27]

The politics of rage and vengeance has closed avenues of rational negotiation with radical groups whose motivation no longer attaches value to traditional notions of national or self-interest. The sheer speed of transformations, and of potential attack, the multiplicity of potential sources of aggression, the anonymity and degree of dispersal with which a terrorist offensive can be planned and executed, all these will make the world a dangerous and unstable place in the new millennium.

The source of all these dangers is a growing pool of widely available knowledge – of weapon systems, of information that was traditionally monopolised by governments, and of skills to translate such information into subversive action. There is only one possible protection against these, and that, again, is to secure greater knowledge, continuously upgraded intelligence, skills and technologies that keep us far ahead of the forces of disorder.

At this point of time, however, we appear to be lagging well behind.

* Mr. K.P.S. Gill is the publisher and editor of Faultlines, the founding President of the Institute for Conflict Management, and a member of the National Security Advisory Board (NSAB). An officer of the Assam cadre of the Indian Police Service, he served in a number of theatres of civil strife and low intensity warfare. As Director General of the Punjab Police, he led the successful campaign against terrorism in that state. Among other activities after his retirement from the Police, he writes on internal security, political and developmental issues for a number of newspapers and magazines.

1. SHAW, G.B., "The Devil's Disciple", cited in Norman F. Dixon, On the Psychology of Military Incompetence", Jonathan Cape, London, with BI Publications, New Delhi, 1976, p. 110.

2. Cf. K.P.S. Gill, "Bureaucracy must emerge from its maze," Pioneer, 23.1.99.
3. See Manvendra Singh, "Years after request, Army still awaits counter-insurgency equipment", Indian Express, 12.12.97, which describes a five-year wait for ‘inexpensive’, ‘lifesaving’ and ‘operation enhancing’ equipment. Snowmobiles case
4. "Endgame in Punjab: 1988-93," Faultlines, Vol. 1.1, ICM-Bulwark Books, May 1999, pp. 13-14.
5. Ibid., pp. 41-44.
6. See; also see J G Nadkarni, "The Army needs modernisation: We love quantity", The Indian Express, 11.8.99; "How well equipped are the jawans", Times of India, 9.6.99, which speaks of the equipment available to soldiers of the Indian army, who are, by and large, much better off than the para-military and state armed police forces.
7. TOFFLER, Alvin, Powershift, Bantam Paperback Edition, 1991, p. 417.
8. Ibid., p. 453.
9. Ibid.
10. "Militants possess chemical weapons", Pioneer, September 27, 1999; "Pak Militants ‘May’ Use Poisonous Gases", The Tribune, September 27, 1999.
11. VAID, Mahendra, "Rs 4,000 cr worth of weapons, equipment for infantry," Times of India, October 22, 1999; GUPTA, Shishir, "Govt okays upgradation of weaponry," Hindustan Times, October 22, 1999.
12. VAID, Ibid.
13. JOHN, Wilson, "Army buys second-hand junk for a fortune," The Pioneer, October 22, 1999.
14. Cf. for instance, though in a different context, the report that the Indian Air Force ignored indigenous radar technologies for over a decade because an "influential lobby" favoured imports. THOMAS, Wg. Cdr. Joseph, "IAF Ignored Reconnaissance Radar", in Bharat Verma (Ed.) Indian Defence Review, Vol. 14 (3), July-September 1999, pp. 93-94.
15. Information available to me suggests that most of these projects were wound up after my departure from Punjab. The crisis had passed, and the Establishment lapsed into its habitual stupor.
16. BOWERS, Stephen R. & KEYS, R. Kimberly, "Technology and Terrorism: The New Threat for the Millennium," Conflict Studies 309, Institute for the Study of Conflict & Terrorism, 1999, p. 22.
17. BOWERS & KEYS, op. cit., p. 16.
18. FOXELL, Joseph W., Jr., "The Debate on the Potential for Mass-Casualty Terrorism: The Challenge to US Security", Terrorism and Political Violence, Vol. II. No. 1 (Spring 1999), p. 102.

19. Ibid., p. 99

20. BOWERS & KIMBERLY, op.cit., p. 13.

21. Cf., for instance, the US Department for Defence Plan for Integrating National Guard and Reserve Component Support for Response to Attacks Using Weapons of Mass Destruction, Prepared by the DoD Tiger Team, January, 1998.

22. DEVOST, Matthew G., HOUGHTON, Brian K. & POLLARD, Neal A., "Information Terrorism: Can You Trust Your Toaster?", Sun Tzu Art of War in Information Warfare, Institute for National Strategic Studies, http://www.ndu.edu

23. DeBORCHGRAVE, Arnaud, cited in Bowers & Kimberly, op.cit., p. 6.

24. Sword & Shield – Cyber Crime Rap Sheet, http://www.sscs.net/cybercrime.html.

25. MARTINEZ, Michael J., "Pentagon Attacks Overblown?", http://abcnews.go.com

26. Ibid. See also Barbara Starr, "Pentagon Cyber-War," and Laura Myers, "Pentagon Computers Vulnerable" http://abcnews.go.com.

27. TOFFLER, op.cit., p. 453.