AIR POWER

Journal of Air Power and Space Studies

Vol. 5 No. 1, Spring 2010 (January-March)

AIR POWER

CENTRE FOR AIR POWER STUDIES

New Delhi

AIR POWER is published quarterly by the Centre for Air Power Studies, New Delhi, established under an independent trust titled Forum for National Security Studies registered in 2002 in New Delhi.

AIR POWER Journal welcomes research articles on defence, military affairs and strategy (especially air power and space issues) of contemporary and historical interest. Articles in the Journal reflect the views and conclusions of the authors and not necessarily the opinions or policy of the Centre or any other institution.

Editor-in-Chief	Air Commodore Jasjit Singh AVSM VrC VM (Retd)
Managing Editor	Shri T. K. Mukherjee
Distributor	KW Publishers Pvt. Ltd.

All correspondence may be addressed to

Managing Editor
AIR POWER
Arjan Path, Subroto Park, New Delhi 110 010
Telephone: (91.11) 25699131-32 Fax: (91.11) 25682533 e-mail: diroffice@aerospaceindia.org
website: www.aerospaceindia.org

ISBN: 81-87966-30-0

AIR POWER Journal is published four times a year and is distributed by
KW Publishers Pvt. Ltd.
4676/21, First Floor, Ansari Road, Daryaganj, New Delhi 110 002
Telefax: 23263498 e-mail: knowledgeworld@vsnl.net

Printed and Published by Air Cmde Jasjit Singh (Retd) on behalf of the Forum for National Security Studies (the Trust running the Centre for Air Power Studies, New Delhi) and Printed by Rajkamal Electric Press, Plot No. 2, Phase IV, HSIIDC, Kundli 131028, Sonepat, Haryana and Published at P-284, Arjan Path, Subroto Park, New Delhi 110 010. Editor: Air Commodore Jasjit Singh (Retd).

RNI REGN No. DELENG/2006/18450

CONTENTS

Vol. 5 No. 1, Spring 2010 (January-March)

Wars in recent years have been more in the nature of military forces against guerrilla/militant fighters and terrorists as compared to the traditional, classic military-to-military wars. Lt. Col. **Rajiv Ghose**, SM, examines the nature of such wars (clubbed under one generic classification of "sub-conventional wars") in our region and the peculiar challenges they pose to the employment of air power in such wars. Challenges to India go even further because the terrorists come from a sanctuary where the state, which possesses nuclear weapons, itself supports the war.

Cruise missiles have been employed in military forces since 1944. Their shorter version, designed specially for the anti-ship role, played a key role during the Falklands War in 1982. **Sitakanta Mishra** examines the technological improvements that indicate a trend not only toward highly accurate cruise missiles, but also the potential of 'intelligent' cruise missiles that can cover long ranges and are able to select their targets and home onto them for greater accuracy.

Cyber space is being increasingly exploited in military and civil arenas and the advantages of doing so are enhancing the capabilities in both areas. But, as Wing Commander **M.K. Sharma** points out, there are also enormous vulnerabilities that pose serious challenges to national security, proving the historical lesson that every new capability that provides competitive advantages in war and peace, very soon must also face the challenge of its intrinsic and functional vulnerabilities being exploited by the adversary.

Network-Centric War (NCW) promises to revolutionise war in the future, not so much because it is basically a new concept, but because technology has made it possible to transfer information very rapidly to a range of users and commanders, thus, reducing the time factor for decision-making. In short and simple terms, NCW would shorten the sensor-to-shooter time in what a scholar had identified more than a decade ago in terms of "time" itself becoming the fifth dimension of war. Wing Commander **Sanjay Poduval** points out the tremendous advantages of NCW and, at the same time, cautions about its vulnerabilities in war.

Combat support has been expanding in scope, role and effects, so much so that it has become an integral part of combat operations. Very often, the efficacy of combat support can prove to be the tipping point in combat. It is in this context that Wing Commander **A.B.S. Chaudhry** carries out a review of **Combat Support Operations in the Indian Air Force: A Historical Appraisal.** Basic understanding of their role and importance is vital for future operations since they act as force multipliers and, in many cases, as force itself and, consequently have enormous influence on the doctrine, tactics and strategy of air warfare.

Wing Commander **Manoj Kumar** has delved into the question he has raised in the title of his study and comes to the conclusion that climate change issues have a profound and long lasting impact on national security which, in some cases, may cause irreversible impact. Some of the effects of environmental changes can already be identified. With climate change, we may expect a significant phenomenon of global warming which, in turn, would melt the earth's ice caps and lead to a rise of the sea level. This, in turn, could submerge many islands and areas, part of the mainland, with enormous impact on demographics.

Soviet military intervention in Afghanistan at the end of 1979 was, from the very beginning, an act that inevitably created a strong adverse impact on India's security, far beyond imaginable limits. And the after-shocks have continued till today and threaten to go on for an undefined period into the future now that the sole superpower has been sucked into the war against terrorism. Dr. **K.N. Tennyson** looks back at the historical processes that produced the constraints and initiatives that India took to try and get the Soviet military to withdraw from Afghanistan, while being unable to take a public position against the Soviet Union.

EDITOR'S NOTE

Wars across the world during the past two decades have repeatedly brought forth some abiding conclusions which clearly deserve serious objective attention. First and foremost is the unequivocal repeated demonstration of the preeminence of air power in achieving success/victory with minimum casualties to own forces as well as to the enemy. Surface forces are at the mercy of air power unless they are also protected by similar air power. But, at the same time, it also must be noted that in all the recent wars, air power was available asymmetrically, with the result that the US-led coalition forces, which in any case possess high-technology weapons and systems, undertook operations with total air superiority which could be termed close to the concept of "Command of the Air" which has now been adopted by China in its official defence strategy to win wars. What happens when you have to contend with a hostile air force? The obvious answer is that a degree of air effort and priority (depending upon the enemy's capabilities) would have to be devoted to contesting control of the air above if the field is not to be left free for the enemy air force to impose its will and restrict our freedom of action on the ground and in the air.

The second recurring theme in all the wars has been that they have been mostly what have come to be called asymmetric wars and/or 4th Generation wars, but which in essence are best described by the term *sub-conventional* wars (though the war that Hezbollah conducted against Israel in 2006 comes close to be termed as semi-conventional war). Air power certainly has been found to be very effective and accurate in such wars, and one of the mistakes that Israel had made in respect of the 2006 War was to have started believing that air power by itself was the prime instrument against such threats. This, of course, was easier to believe in a country whose survival in the past has depended heavily on air power. But this mindset delayed a coherent joint action where the land forces were used too late and in too small numbers. The increasing use of UAVs (Unmanned Aerial Vehicles), especially the UCAVs (Unmanned Combat Air Vehicles) has provided even greater capability in targeting moving and fleeting time-critical targets, especially when the target consists of an individual vehicle or even a person; but this also runs the risk of over-estimating their role and effect.

The third element that we need to take into account is that air power is intrinsically technology intensive, and, consequently, practitioners of air power place a heavy reliance on technology. We have seen that many of our air force leaders honestly and earnestly believed that force multipliers (based on high-technology) would not only achieve greater effects, but flowing from that logic, we could do more with less. This is true only in absolute terms, and not when seen in relative terms with an adversary who also acquires similar technology and force multipliers. But the more important point is that empirical evidence tells us that while technology and force size are crucial in war, and an advantage in either or both could be crucial in deciding the outcome of the conflict, the real factor that leads to that decision is how force is employed. It is in this context that we need to understand the dynamics of air power and warfare, whether the classical force-on-force or sub-conventional war, whatever name we ascribe to it.

AIR POWER IN SUB-CONVENTIONAL WARFARE IN THE SOUTH ASIAN REGION: PAST LESSONS AND FUTURE TRENDS

R. GHOSE

While the armed forces of the important states, and increasingly those of the developing countries as well, raced each other to see which one could produce and field the most powerful modern weapons, war did not stand still. Albeit, wars have never been the sole form of armed conflict and earlier the most important wars had been fought by states with their regular armies. However, after the 1945 War, this kind began to turn into an endangered species. One of the first 20th century armies to feel the fury of sub-conventional war was the German *Wehrmacht*[1]. First in Yugoslavia, Russia, Greece, and Poland, then increasingly in other countries such as Italy, France, and even Holland, Belgium and Scandinavia, the Germans were faced with armed opposition which disrupted their rule, tied down their resources and inflicted casualties.[2] Although they were perhaps the most ruthless conquerors in history and killed millions, they failed to stamp out even one of the movements under reference. On the contrary, the more brutal the operations became, the stronger the resistance evolved. In fact, this almost set off a logic to resort to sub-conventional means to

* Lt Col **R. Ghose** SM, is a Research Fellow at the Centre for Air Power Studies, New Delhi.

[1] *Defence Power,* refers to the German armed forces in World War II.

[2] Charles Townshend, *The Oxford History of Modern War* (Oxford: Oxford University Press, 2000), p. 355.

The more powerful and more modern the technology, the less adaptable it became to stamp out this kind of warfare at the sub-conventional strata.

gain certain rights, make believe or otherwise. In fact, this logic led to a whole series of 'wars of liberation' in Palestine (1946-48); Indonesia (1947-49); Indo-China (1946-54), Malaysia (1948-60); Kenya (1953-58); Algeria (1954-62); Cyprus (1955-60); Aden (1967-69); and a host of less important cases.[3] How can one explain the victories won by those, initially at least, who did not possess much military experience or organisation, hardly any weapons in comparison, and had limited economic resources? While circumstances differed from one place to another, the bottom-line answer was always the same: the more powerful and more modern the technology, the less adaptable it became to stamp out this kind of warfare at the sub-conventional strata.

India faces a huge challenge of tackling the lower end of the spectrum of warfare which we refer to as sub-conventional war, associated with the ongoing conflict in Jammu and Kashmir (J&K), the Naxalite problem, the uprisings in the northeast and the linkages to terror attacks like in New Delhi,[4] Mumbai,[5] Bengaluru, Ahmedabad [6] and other towns and cities. These are all but grim reminders of this new reality where even the finest militaries in the world have been rudely jolted by the pervasive influence of this genre of warfare.

After World War II, progressive nations with large and powerful militaries began to develop military power as a means of coercion as a matter of state policy by engaging in coercive diplomacy. The linkage between the coercive capability of the larger powers and the emergence of sub-conventional warfare becomes important when we witness the means

[3] Ibid., p. 356.

[4] "The Indian Media has Called for Tougher Laws and Strategies to Combat Attacks by Militant Groups in the Country", published on September 15, 2008, at http://news.bbc.co.uk/2/hi/7615941.stm

[5] "Mumbai Terror Attacks Lead Papers", published on October 27, 2008, at http://news.bbc.co.uk/2/hi/uk_news/7751739.stm

[6] Wilson John, " Indian Security Agencies Struggle will Probe into Serial Bombings in Gujarat and Karnataka", published on August 6, 2008, at http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=5103

of combating terrorists, insurgents and 'freedom fighters', in remarkably new ways which test the capabilities of established military forces in what is referred to variously as asymmetric, irregular or even hybrid warfare. When we look across the spectrum of this kind of conflict, countries like the United States (US), Soviet Union, later Russia, United Kingdom (UK), India, Israel and Sri Lanka have all used divergent tactics with the essence of deterrence and coercion to achieve similar objectives. It can be conveniently deduced that sub-conventional warfare has emerged as an effective counter to a larger ability to coerce, and the tools used are in stark contrast to the tools of conventional coercion, be it diplomatic or military. What, then, is this sub-conventional war and the methods used in this kind of warfare? The inability of countries to counter coercion with open force, and fight conventional wars with entities such as non-state actors has led to the emergence of war-fighting concepts which logically precipitate from the failure of coercion, which invariably leads to gradually escalated use of force.

Air power formed the primary tool when engaged in such escalation, and also the much-needed catalyst for conflict resolution, too. Examples exist in the form of the Vietnam conflict, the British intervention in Ireland, the Soviets in Afghanistan and the Russians in Chechnya, the Indian Peace-Keeping Force (IPKF) operations in Sri Lanka, and the Lebanon War of 2006. In the modern era of warfare, the Israelis have been pioneers in the use of air and space assets to prosecute campaigns against non-state actors like Hamas and Hezbollah, even without committing ground forces. Similar have been cases of the recent exploits by the American and Coalition forces in Afghanistan. Though their strategy has met with success, it has also evoked widespread criticism. It has certainly opened new vistas for employment of air power, where deterrence and coercion seem to have worked side by side and complementary to one another; but there are some important questions that can be answered only after we see the outcome of the application of air power in combating sub-conventional warfare. This is especially so in South Asia, with a backdrop of the restraining factors and limitations of air power in such wars. It will also be pertinent to note what technology has to offer via perspectives and possibilities on the use of air power in sub-conventional conflicts. Finally, the trend that can been seen in the likely future is on air power application in such a manner that the perpetrators of sub-conventional warfare are confronted with an unacceptable exerting pressure that exhausts them. If yes, then, is air power still an instrument of coercion or rather compellence, though this time not against established nations directly but against non-state actors, terrorists and insurgents?

The flexibility and unpredictability, with which these wars are fought, reflect the degree of difficulty the armed forces face in formulating tactics and strategies.

Nations do get involved when state boundaries and regional power politics assist in the existence of sanctuaries from where non-state actors are able to operate with impunity, at times, and, to that extent, transnational sanctuaries have remained a persistent source of the problem throughout history. Having faced typical confrontational elements of sub-conventional conflict, it should now be time enough for India to focus on the Naxalite movement which also has a similar genre, given the alacrity with which they have struck and have been troubling India since the early Sixties. In conjunction with uprisings in the northeastern states, they now threaten the very fabric of governance and rule. Understanding the movement is not within the purview of this article, however, how to deal with the nature of the movement's threatening posture with an 'air-first' response or simply air power will be considered in some detail while discussing India's response to its internal sub-conventional tackle. After years of trying to fingerprint the uncertain genre of this kind of warfare, the terms flexibility and unpredictability, with which these wars are fought, reflect the degree of difficulty the armed forces face in formulating tactics and strategies to fight battles in such an atmosphere. Choosing the right weapons and training regular forces to think and train in a manner that contradicts the age-old tenets of war-fighting are other dilemmas that merit constant attention.

AN EXISTENTIAL PROBLEM: SANCTUARIES

Despite adherence to ideology, the perpetrators of sub-conventional conflict use the international system, and their version of hiding behind the veil of state boundaries has been a norm which makes state forces somewhat incapable without regional and inter-country cooperation, both diplomatic and military. Some states oppose, but are incapable of completely stopping this use of their territories. Others, for reasons ranging from regional power politics, to sympathy for the ideology, either provide direct support, or knowingly allow use of their lands. Therefore, international borders, and the transnational sanctuaries and supply lines that get inherently protected, are crucial issues in such warfare. Transnational sanctuaries play a role in such warfare from the onset. Active sanctuaries have been used throughout the world. In the Greek Civil War (1946-49), the Communist rebels enjoyed the use of sanctuaries in Albania, Yugoslavia, and Bulgaria.[7] The Communist insurgents fighting the British-supported government in Malaya[8] from 1948 to 1960, had sanctuaries in neighbouring Thailand. The anti-French rebels in Indochina (1945-54) could look to China for supply and refuge,[9] and the anti-French fighters in the Algerian War of Independence (1954-62) had sanctuaries in Morocco and Tunisia.[10] In all these cases, the anti-government forces were generally successful as long as they had access to, and made use of, their sanctuaries.

Shortly after the Americans and their allies took Kabul in the fall of 2001, the Taliban and Al Qaeda retreated to the mountainous Afghan frontier with Pakistan. In the Tora Bora region, south of Jalalabad, they made use of old supply stores to dig into the mountains and valleys, and continue the fight. In December 2001, Allied forces launched a series of assaults on the enemy positions, eventually killing and capturing many, though many others escaped across the border into Pakistan. In the March 2002 Operation Anaconda near the Pakistan border south of Kabul, events followed a similar course. Coalition troops encircled Al Qaeda positions in

[7] See Ulrich Sinn, " Greek Sanctuaries as Places of Refuge", in Nanno Marinatos and Robin Hagg, eds., *Greek Sanctuaries: New Approaches* (London: Routledge, 1993) for an understanding; and Michael Brecher and Jonathan Wilkenfeld, *A Study of Crisis* (Ann Arbor: University of Michigan Press, 1997).

[8] See John A. Nagl, *Counterinsurgency Lessons from Malaya and Vietnam* (Westport: Praeger Publishers, 2002).

[9] Jacques Dalloz, *The War in Indo-China1945-54* (Dublin: Gill & Macmillan, 1990), p. 153.

[10] Paul-Marie De la Gorce, *The French Army : A Military-Political History* (New York: George Breziller Inc, 1963), p. 455.

a mountain valley roughly 25 miles from the border. The fight continued till the enemy's collapsing and breaking up into smaller groups to flee to Pakistan.[11]

Pakistani officials have repeatedly asserted that their "forces are fully capable of securing and protecting Pakistan's borders."[12] Indeed, Pakistani forces must have worked to kill and arrest hundreds[13] with periodically launched raids or air strikes along the border in search of the leaders. One prominent effort came in January 2006, when a US air strike targeting Al Qaeda leaders in the border village of Damadola killed civilians in the village, resulting in civilian protests against Pakistan's government for cooperating with the United States. Later, Afghan President Hamid Karzai and Pakistani President Pervez Musharraf had a brief public dispute over Pakistani efforts to police the borders.[14] The tenuous situation along the frontier continues to this day.

Another example was the Syrian border which continued to be a problem even after the end of major conventional operations in Iraq by May 2003. L. Paul Bremer, the Administrator of the Coalition Provisional Authority in Iraq, wrote in his memoirs about a July 2003 discussion of the major problems where he stated that Iraq's long, porous border with Syria had offered the primary escape route for the fleeing extremist fighters. But Syria seemed immune to most diplomatic or economic underpinnings and seemed susceptible only to direct military intervention which was unlikely with the US forces engaged in Iraq and Afghanistan.[15] In order to effect better security along the frontier, the border was divided into sectors and schedules set up to observe various areas of infiltration. Air force and navy pilots flew observation missions, as did Unmanned Aerial Vehicles (UAVs). They also

[11] Richard W. Stewart, *The United States Army in Afghanistan: Operation Enduring Freedom* (Washington, DC: US Army Center of Military History, 2003), pp. 26-44.

[12] "Pakistan Rejects US 'Right' to Incursions," *Los Angeles Times*, January 5, 2003, available at http://www.latimes.com/news/custom/showcase/la-print-edition,htmlstory

[13] "Pakistan Says 50 Killed in Airstrike on Terror Camp," *Los Angeles Times*, September 10, 2004, available at http://www.latimes.com/news/custom/showcase/la-print-edition,htmlstory

[14] Zahid Hussain, "Political Fallout in Pakistan Strike Tests a US Ally," *Wall Street Journal*, January 16, 2006, available at http://online.wsj.com/public/page/news-global-world.html

[15] L. Paul Bremer, *My Year in Iraq: The Struggle to Build a Future of Hope* (New York: Simon and Schuster, 2006), pp. 104-105.

buried seismic sensors called steel rattlers to detect moving vehicles at the border. But the territory could never be completely shut down along with the border. Part of the problem was the ingenuity of the insurgents. The foreign fighters came in a lot of different ways. Water trucks had false tanks where human beings could be stowed away. Commercial traffic at border crossings offered numerous trucks loaded with fruit and merchandise, but they also catered to false hiding places where Rocket Propelled Grenades (RPGs) and weapons could be stacked up, and, of course, there was no time to unload a complete truck and then load it back up.[16] Air power had very little to leverage on such occasions.

There are lessons to be learned from Vietnam, including many relating to transnational sanctuary.

India also faces this problem with the porous borders in the northeastern states.[17] Also, in spite of the fencing along the border and Line of Control (LoC), there have been numerous instances where infiltration has been reported and acknowledged.[18]

APPLICATION OF AIR POWER IN COMBATING SUB-CONVENTIONAL WARFARE

Despite a mighty effort in Vietnam, a world's great superpower proved unable to prevail in the face of a relentless enemy. Vietnam is also remembered as a symbol of a military disaster, never to be repeated. The military had for too long ignored many of the most important lessons even during the war. In fact, Robert Cassidy explains a shortcoming: "The American military culture's efforts to expunge the spectre of Vietnam, embodied in the mantra 'No More Vietnams,' also prevents learning from those lessons." There are lessons to be learned from Vietnam, including many relating to transnational sanctuary. The full range of issues relating to the tricky diplomatic problems

[16] Thomas A Bruscino, Jr, *Out of Bounds: Transnational Sanctuary in Irregular Warfare* (Kansas: Combat Studies Institute Press, 2006), pp. 2-5.

[17] P. C. Shekhar Reddy, *Peace and Development in the Northeast: A Virtuous Spiral* (New Delhi: Mittal Publications, 2007), p. 73.

[18] Press Trust of India, *Data India Issues 27-53* (New Delhi: Press Institute of India, 2005), p. 290.

of international frontiers and sub-conventional warfare were on display. So, too, were the responses. A wealthy and technologically advanced modern state had within its ability to attempt a wide variety of schemes to deny the Communist enemies their transnational sanctuaries. The failures and successes among those efforts, coupled with a solid understanding of the reasons thereto in the overall effort provide a variety of insights on the issue of transnational sanctuary in sub-conventional engagement.

The same could be said of the Soviet War in Afghanistan (1979-89). The Soviets had amassed an enormous and technologically advanced military, like the Americans before Vietnam, but they had not invested much time or effort in developing any sub-conventional doctrine, so they had to play 'catch up' when intervening in Afghanistan. Like the Americans, they tried a wide variety of techniques to stop the insurgents from making use of their transnational sanctuary. But unlike the Americans, the Soviets had no compunctions whatsoever about using the most brutal techniques to put down insurgency.

In 1979, when the Soviet Union intervened in Afghanistan to support a pro-Soviet government, the world was initially impressed with the use of the Russian Spetnaz (Special Forces) and air power, but the war turned into a long, messy, and brutal struggle between the Soviet troops, their Afghan supporters and the opposing Mujahideen.[19] Air assets, both fixed-wing aircraft and helicopters, were used by the Soviet forces to lethal effect in Afghanistan, although rarely in a way to advance any political objectives. While aircraft were used extensively for resupply purposes in Afghanistan, and for bombardment to depopulate important rural areas, their main use was in support of ground operations. The main helicopters used were Mi-24 (Hinds), which carried four anti-tank missiles, had a maximum speed of 275 km per hour, and a 300 km range. With a crew of two, they could carry 8-10 troops. Fixed-wing aircraft came in different forms; while the Tu-16 and Su-24 bombers operated from bases in the USSR itself, the MiG-23/27 (Flogger) and Su-25 (Frogfoot) aircraft were deployed

[19] Thomas K. Adams, *The Army After Next* (Westport: Greenwood Publishing, 2006), p. 19.

in Afghanistan from 1980.[20] Attack aircraft were used most often for planned strikes against clearly identified targets, while helicopters performed the majority of 'on-call' strikes. Directed against civilians, these assets proved lethally effective but were certainly less effective against small resistance groups. The main problem was shortage of assets. The Soviet Army could never muster enough helicopters and air assault forces to perform all the necessary missions and the airborne and air assault forces were usually understrength. Furthermore, from late 1986, the supply of Stinger missiles to the Afghanistan resistance forced Soviet aircraft to take evasive actions which to a great degree compromised their initial military effectiveness.[21]

The Soviet Army could never muster enough helicopters and air assault forces to perform all the necessary missions.

The expanded use of the Spetsnaz forces in Afghanistan did mark an important turning point. With the increase use of Special Forces, the USSR moved towards overcoming one of the greatest weaknesses, namely the limited autonomy granted to relatively small groups of troops in a theatre of operations in which flexibility and local initiative were vital. They formed the core of a more specialised counter-insurgency force, which, comprising not only the Spetsnaz but also airborne, air assault, and designated reconnaissance troops, came to a total of 15 to 20 per cent of the force.[22] In spring 1985, the Spetsnaz forces were deployed along the Afghanistan-Pakistan border with a view to attempting to close it as more than 60 per cent of Afghanistan's border with Pakistan fell under their control. The Spetsnaz forces were better equipped and trained than their regular counterparts. However, they also suffered their losses and on three occasions, were completely wiped out by the resistance groups because of isolation from air cover.[23] On occasions, too, the benefits of surprise were lost with the Special Forces inserted only after a period of bombing and reconnaissance. This may have minimised the losses

[20] William Maley, *The Afghanistan Wars* (New York: Palgrave Macmillan, 2002), p. 48.
[21] Ibid., p. 49.
[22] Ibid.
[23] Ibid., p. 49.

on the Soviet side, but it also allowed the resistance groups to make good their escape to survival. When the Soviet forces opted to 'drive out the population', they set about doing it in some of the most barbarous ways one could imagine. Mud-brick buildings, of the kind which pre-dominated Afghan villages, were no match for aerial bombardment, rockets, and artillery.

Intelligence lies at the heart of effective military operations, although it cannot compensate for poor tactical execution.

Intelligence lies at the heart of effective military operations, although it cannot compensate for poor tactical execution. Information to facilitate military operations was gathered in a number of different ways. Helicopters were, of course, used for reconnaissance purposes. However, once it became necessary to collect more detailed Human Intelligence (HUMINT), the Soviet forces ran into difficulties, largely because of the instrumentalities, besides shortcomings prevalent in the existing system. The Soviet forces' dependence on their own system led to the troops having to do with limited ranges and their equipment coped poorly in the mountainous terrain even when it came to air-to-ground or just ground communications. Secondly, the resistance groups tended to rely on human messengers and made limited use of radios, thus, making interception difficult. Procedures used by the Soviet troops were cumbersome and inefficient. One really could not conclude whether it was the widespread deficiencies in communication between air and ground or any other reason that was reflective of endemic inflexibility, lack of imagination, compartmentalisation and reluctance to depart from rote and textbook procedures even when they did not work [24] and led to almost catastrophic results, till the Soviets finally decided to withdraw. However, it could be reasoned that lack of good communication was one of the marked reasons for operational failure in certain areas during combat.

The most effective weapon against the resistance was the Mi-24 helicopter gunship. By mid-1982, Soviet helicopter strength (the Mi-6 heavy transport

[24] Ibid., p. 52.

and assault, medium transport and assault and the heavily armoured Mi-24 Hind gunship) was estimated at roughly 600-700 machines, of which some 200 were thought to be Mi-24 Hinds.[25] Helicopters gave the Soviets mobility similar to that of the Americans during the Vietnam War with the US Huey Cobra attack helicopter. However, they had their share of operative shortcomings too.The gunships would inevitably continue on their flight-path unless they had come specifically to target a village. The guerrillas soon learned to leave their animals standing in small groups while they crouched motionless. In more exposed and open terrain, camps were pitched at night among nomad tents and herds so that a few extra strings of animals would not stand out in the event of a dawn air patrol.

While less protected Mi-8s were being brought down by guerrilla fire and even sprays of Kalashnikov bullets, the Hinds could fly with more impunity because of their armour protection though they still had their share of vulnerabilities. Only from the third year of occupation did one begin to see evidence of Mi-24s being knocked down.[26] Although considerable numbers of helicopters of all types as well as jetfighters had been shot down by the end of 1984, some of them by anti-air missiles, overall resistance weaponry had still not improved by this time to the point that the Soviets no longer dominated the skies. Nevertheless, all types of aircraft were now being forced to fly higher in the sky. The Soviets had also rediscovered what the British had learnt during their Afghan campaigns in the 19th and 20th centuries about the deployment of assault 'rangers' or commandos. Reliance was placed on Mi-8s as a primary form of transport while the Mi-24s provided close air cover which ultimately became the mainstay nature of operations for the Soviets. The air assault rangers proved particularly useful and effective in establishing forward positions during swift cordon and search, including search and destroy, missions.

[25] Edward Giradet, *Afghanistan: The Soviet War* (London: Taylor & Francis, 1985), p. 42. Travelling with the guerrillas in Nangarhar province, the author recalls the panic-stricken state of the rebellious group at the appearance of gunships, not realising that they were practically invisible from the air against a backdrop of rocks, tress and bushes.

[26] Ibid., p. 43.

Although to a lesser degree, the helicopters were used for escort convoys through vulnerable mountainous terrain. Flying in pairs, Mi-8s or Mi-24s would 'leap-frog' the length of the column, providing vehicles with a constant but not necessarily unassailable form of protection. Gunships also regularly crested the heights in the way of establishing pickets on mountain tops and ridges in order to control the lower slopes. While generally, troops have to climb themselves, the Soviets preceded ground offensives in the highland regions by dropping commando units on high points and then picking them up again when the operation was over.

As the resistance became increasingly adventurous, the airports and air bases became targets and the invincible Mi-24s were flying 'extremely' high to avoid the gauntlet of anti-aircraft and heavy machine-gun fire in areas where the guerrillas had established rudimentary but efficient aerial defence systems.[27] Once the guerrillas temporarily overran the city of Kandahar, forcing the government officials to run to the airport for shelter, and the Soviets had to retaliate mercilessly with their planes and artillery, inflicting such heavy losses that the local inhabitants asked the guerrillas to leave, which they did. However, such incidents did not carry the precedent and content of any operational logic.

The Soviets were into massive induction of troops since 1983. They gradually introduced up to five air assault brigades of specialised heliborne 'rangers' better suited for combat in the mountains, which were deployed in different locations around the country. This was in addition to seven motorised divisions[28] plus the 105th Airborne[29] – a total of some 8,5000 troops. An additional 30,000 men were also included, some of whom were used in cross-border operations. By early 1985, the figure had risen to the generally accepted one of 115,000, with 30,000-40,000 regularly deployed for special operations from bases inside Soviet Central Asia. In one of the cited operations in Kunar Valley which formed a 60-mile fertile farming district close to the Pakistan border, it was evident that the Soviets pounded the area for two days, then, while the troops were dropped from helicopters along the nearby

[27] Ibid., p. 44.

[28] Each division consisted of three infantry regiments, one tank and one tank regiment.

[29] 105th Airborne consisted of six paratroop regiments as well an artillery one.

ridges and on to rooftops, columns of tanks and BMP infantry combat vehicles swept rapidly, ploughing down whatever came in their way. [30]

The number of sorties steadily increased. Even by mid-1981, three sorties per day was the normal average.

The Soviets in Afghanistan were actually using weapons that were standard with their ground forces and these also included T-72 tanks and 152mm self-propelled howitzers but the weapons receiving the most attention were armed helicopters and, of course, chemical agents.[31] The helicopters were usually used in pairs. In carrying out air strikes, the Mi-24 gunships were often used in conjunction with Su-25 fighter bombers or MiG fighters. When a guerrilla band was located, gunships and fighter bombers would be summoned in to bomb and strafe the target until the suspected guerrilla group was believed to be eliminated. Consequently, the number of sorties steadily increased. Even by mid-1981, three sorties per day was the normal average.[32] As the sortie average increased, failure due to mechanical and pilot fatigue also rose and at times accounted for nearly 80 to 85 per cent of recorded incidents/accidents.[33] The Su-25 was a new aircraft that was being used outside the USSR only in Afghanistan. The Su-25 was a single-seat close support combat aircraft equipped with 500-kg bombs and rockets and a heavy calibre Gatling-type machine-gun. It could fly for long periods, dive steeply, and turn in mountainous valley areas. Having mentioned the use of chemical agents by the Soviets, the first public report came from the US government on March 22, 1982, where it was charged that reports had been received of 47 separate chemical attacks with a claimed death toll of more than 3,000 and the reports were indicative of both fixed-wing aircraft and helicopters being employed to disseminate chemical warfare agents by rockets, bombs and sprays.[34]

[30] Giradet, n. 25, pp. 32-33.

[31] J. Bruce Amstutz, *Afghanistan:The First Five Years of Soviet Occupation* (Washington D.C.: National Defense University, 1986), p. 170.

[32] Ibid., p. 171.

[33] Ibid., p. 172.

[34] Ibid., p. 173.

AIR POWER IN SRI LANKA

J. A. Khan states in his book *Air Power and Challenges to the IAF* that during the Indian Peace-Keeping Force (IPKF) operations in Sri Lanka, in many instances, the Army was not satisfied with the cooperation requested from the Indian Air Force (IAF).[35] He also states that there is an obvious anomaly at the decision-making level and it must be rectified in the interest of military operations required for national defence and security. Whether the decision-making is awry at the military or political level will stand immaterial when the country's defence and security is at stake, and, interestingly enough, we will observe some additional dilemmas when looking at the internal security status and its handling with air power when discussing later about tackling the Naxalism menace in India with an 'air' response. The difficult question arises when the use of air power is weighed against political implications. The temptation to use air bombardment to soften up the target before the ground attack is very great. Unless clearly mandated by a political statement, use of air power is a clear instance of the prevailing of the military over civilian judgements.[36] Till the recent onslaught on the Liberation Tigers of Tamil Eelam (LTTE) with an aim to annihilate and eradicate them, the use of air power even by the Sri Lankan Air Force was limited.[37] There was an instance where the President of Sri Lanka sent Foreign Minister Lakhsman Kadirgamar as a special envoy with a request to bomb Elephant Pass and other forward operational bases of the LTTE should Jaffna be on the verge of falling to the LTTE. [38] There was never a question then of Canberra bombers being alerted or Mirage fighters standing by at their base for such offensive operational missions which could have had huge collateral consequences. It was only

The difficult question arises when the use of air power is weighed against political implications. The temptation to use air bombardment to soften up the target before the ground attack is very great.

[35] J. A. Khan, *Air Power and Challenges to IAF* (New Delhi: APH Publishing, 2004), p. 195.

[36] Adrian Wijemanne, *War and Peace in Post-Colonial Ceylon 1948-1991* (New Delhi: Orient Longman, 1996), pp. 49-50.

[37] "International Dimension of the Sri Lankan Conflict: Threat and Response", Issue 27 of Marga monograph series on ethnic reconciliation (Ethul Kotte: Marga Institute, 2001), p. 15.

[38] Saroj Pathak, *War or Peace in Sri Lanka* (Mumbai: Popular Prakashan, 2004), pp. 195-196.

humanitarian assistance that could be rendered as it was once again felt that the application of destructive air power would make the difference but, at the same time, would create a situation that could be irremediable, as civilian casualties would surmount beyond reason and explanation.

Adverse public implications aside, the Sri Lankan armed forces were certainly gaining ground through effective use of air and firepower .

It is not that coercive air power was entirely out of fashion when it came to selective application. The Sri Lankan Air Force employed strike aircraft to target the LTTE and with a certain amount of precision which contributed to stalling the guerrillas to a considerable extent. After the Sri Lankan Army Chief Sarath Fonseca was targeted, the Sri Lankan Air Force conducted a series of air attacks on LTTE bases. This commenced with effect from April 24, 2006, and one such strike, on July 27, 2006, in the Verugall river region in Trincomalee and Keppapulavu in Mullaitivu district, in retaliation of the LTTE closing the sluice gates of Mavil Auru Dam which supplies water to land held by farmers, was particularly effective during a phase when the battle for control of waters had become crucial.[39] Though India did try to persuade Sri Lanka against unilateral application of air strikes, the Sri Lankan Air Force continued with air strikes till almost the last phase of their operation in wiping out the LTTE bastions. Adverse public implications aside, the Sri Lankan armed forces were certainly gaining ground through effective use of air and firepower along with the resolution of the armed forces that had become battle hardened over a period of time.[40] The concern on the Indian side was palpable from the very beginning of the IPKF operations. Then Prime Minister Rajiv Gandhi, in a statement in the Parliament on November 9, 1987, had said, "IPKF was given strict instructions not to use tactics or weapons which would result in casualties among the civilian population in Jaffna".[41] Coercive air power will, in most cases, have consequential damage

[39] Brig Rahul K. Bhonsle, *South Asia Security Trends* (New Delhi: Atlantic Publishers and Distributors, 2007), p. 111.

[40] Ibid., p. 100.

[41] P. A. Ghosh, *Ethnic Conflict in Sri Lanka and Role of Indian Peacekeeping Force* (New Delhi: APH Publications, 1999), p. 123.

which can be difficult to handle, and almost close to moralistic impossibility when the ethnicity and origin of groups being targeted is an issue.

All may not have been said about the aspects of application and understanding of air support when actual operations got going. On October 11, 1987, the IPKF began their advance towards Jaffna across landmines and booby traps. 91 Infantry Brigade, 72 Infantry Brigade and 18 Infantry Brigade made initial quick progress in their operations to seize Jaffna University campus and the LTTE tactical headquarters, but soon were slogging their way because any area that was vacated in the rear was by the LTTE cadres and soon the IPKF would have to clear the block. One of the main reasons cited for the tardy progress was the lack of offensive air support.[42] What the Air Force was asked to provide was air support with photo- reconnaissance which they did with their Jaguars and MiG-25s.[43] Debit this to faulty planning or improper understanding of the application of air support, but it certainly provided thought for not committing similar mistakes when the LTTE 'command centre' at the Jaffna University campus was being attempted. Insertion of a heliborne force was attempted which went awry from the beginning when the force was split because of navigation error, with the Mi-8s coming under heavy fire and damage, having no retaliatory power with them; also, no gunships were permitted as escorts.[44] The failure of such a combat air support operation was inevitable among other things which led to the cessation of such heliborne operations. Air power applications akin to surgery cannot be done piecemeal, with fragmented insertions.

Combined tactical operations at the company and battalion level involving the Army, Navy and Air Force were undertaken at an appreciable level. These operations were mainly conducted for searches, raids and domination of selected/designated areas, including induction and extraction of troops. Armed helicopters supported landing and disengagement of troops on several occasions. Even distant places could be dominated in this fashion. It was, however, difficult to achieve total surprise in spite of tactical and

[42] Ibid., p. 124.

[43] Ibid., p. 125.

[44] Maj Shankar Bhaduri, Maj Gen Afsir Karim, AVSM, Lt Gen Mathew Thomas, PVSM,AVSM, VSM, *The Sri Lankan Crisis* (New Delhi: Lancer, 1990), pp. 75-76.

circuitous routes followed by the aircraft despite being conducted in the hours of darkness. The entire coastline was covered with fishing colonies infested with LTTE informers. Thus, the LTTE were invariably successful in receiving timely warning and could hide themselves as well their weapons by merging with the fishermen and the boats. Nevertheless, it was noted that a successful and integrated unified command structure was evolved, at least at the ground level and, very often, helicopters were used for surveillance over vehicle convoys, train movements and to provide fire support when necessary. There was an existential problem of communication between helicopter crews and ground forces on several occasions but in spite of this persistent problem, it resulted in the LTTE having to vacate important areas in the hinterland, and moving deep into the jungles.[45]

Air support was visibly the most essential component in such war-fighting as the units and sub-units were required to cover large areas.

One area where the IPKF found itself tactically weak was the large number of small teams drawn out at company and battalion level[46] which could be integrated for fighting the guerrilla type of warfare. Air support was visibly the most essential component in such war-fighting as the units and sub-units were required to cover large areas in conformity with an overall design and plan which in itself required flexibility in grouping and regrouping and also involved setting up of additional bases or shifting bases in a very short time. For this, the air element was vital to keep the guerrillas on the run and isolate them.

During the last year of the operations against the LTTE, the Sri Lankan armed forces did not refrain from any kind of assault, including air attacks. For example, on April 30, 2008, the capture of an LTTE base called the ‘LTTE 18-Base’ in Northern Sri Lanka which also claimed an LTTE leader, was assisted by Sri Lankan Air Force fighter jets which were launched to assist the ground troops, while Mi-24 helicopter gunships raided LTTE locations

[45] Ghosh, n. 41, p. 115.

[46] Ibid., p. 116.

in the Mannar front.[47] Nitin Gokhale reveals in his book *Sri Lanka, From War to Peace* that the Mi-17s given by India to Sri Lanka made a huge difference in subsequent operations when it came to conducting some daring missions either for deep penetration of troops or extraction operations. The air effort provided the ground troops a greater degree of confidence while operating behind enemy lines and was the key factor in the Special Forces delivering spectacular results, as revealed by Sri Lankan Army officers.[48]

AIR POWER IN 'AF-PAK.'

The war in Afghanistan commenced in October 2001. After it was reported by the *National Commission on Terrorist Attacks upon the United States (The 9/11 Commission)* on July 22, 2004, that the attacks were conceived and implemented by members of Al Qaeda with their direct links with the Taliban, the US achieved a broader Coalition, including a first wave of air assets to which Australia contributed air-to-air refuelling tankers, Orion electronic gathering aircraft, F/A-18 fighter aircraft, New Zealand pitched in with two C-130 Hercules, Netherlands sent ground attack fighters and Apache gunships, Portugal provided 37 air traffic controllers, and Poland a transport C-130,[49] besides what the US had to induct as part of the effort. In fact, in the post-Cold War period, the US military which had designed itself to fight two wars simultaneously in either the Middle East or Europe, or Asia, had by the year 2000, determined by these objectives, acquired a more effective range of fighting capabilities which made them more mobile with the provisioning of more helicopters and heavy lift military air transports to shorten transportation time from bases to operative areas. Consequently, new air force technologies were also developed, including sophistication of the drones.[50]

[47] "Sri Lanka: 70 LTTE Rebels Killed in Army Offensive", posted on May 01, 2008 at http://ibnlive.in.com/news/sri-lanka-70-ltte-rebels-killed-in-army-offensive/64313-2.html

[48] "India Behind Lanka's Victory over LTTE: Book", posted on August 23, 2009, at http://timesofindia.indiatimes.com/india/India-behind-Lankas-victory-over-LTTE-Book/articleshow/4924585.cms. Incidentally, the Chinese gifted four F7 GS fighter planes with interception radars and heat-seeking missiles.

[49] Robert Catley, David Mosler, *The American Challenge: The World Resists US Liberalism* (Hampshire: Ashgate Publishing, 2007), pp. 111-112.

[50] Ibid., pp. 166-167.

Even before 9/11, the US had undertaken overt actions using air power. The first was in August 1998, and the second in September 2001. The first consisted of two cruise missile strikes – one against a pharmaceutical plant in Khartoum and the other against training camps in Afghanistan. This was in response to the bombing of US Embassies in Kenya and Tanzania.[51] The second attempt came after the 9\11 attacks when the US demand that Afghanistan hand over Osama bin Laden was backed by the movement of heavy bombers within striking distance of Afghanistan – but neither the coercive methods nor the intention of further application yielded any direct and concrete outcome.

Over the last three years, drone strikes have killed about 14 terrorist leaders but, according to Pakistani sources, have also killed some 700 civilians.

Air power application aims at ultimate victory. This would translate into a political-military victory which occupies an intermediate position between victory at a tactical level, which has a shorter term and more focussed effects in battle, and victory at the grand strategic level, which has wider and more significant implications for the state and the international system.[52] Therefore, a broader explanation would encompass the use of such overwhelming force which would signal the resolve of policy-makers to warn the adversary of the impending political purpose. But the value of this concept is its ability to emphasise that the relation between the scale of destruction and the implications of victory is clearly understood by the adversary; otherwise, the concept involves political risks, which the US faces in the dilemma of whether to continue, and for how long, in Afghanistan.

While violent extremist action as seen in sub-conventional means of conflict may be unpopular, for a frightened population, it may not seem more ominous than a faceless instrument that from afar often kills more innocents than militants. Press reports suggest that over the last three years, drone strikes have killed about 14 terrorist leaders but, according

[51] Robert J. Art and Patrick M. Conin, " Coercive Diplomacy" in Chester A. Crocker, Fen Osler Hampson, Pamela R. Aall, eds., *Leashing the Dogs of War: Conflict Management in a Divided World* (Washington D.C.: United States Institute of Peace, 2007), pp. 308-309.

[52] William C. Martel, *Victory in War: Foundation in Modern Military Policy* (New York: Cambridge University Press, 2007), p. 97.

to Pakistani sources, have also killed some 700 civilians.[53] (This translates into 50 innocents for every extremist eliminated and a strike rate of approximately 2 per cent – hardly a precision). After the assassination of Benazir Bhutto in December 2007, and an internal debate, President George W. Bush had authorised a broad expansion of drone strikes against a wide array of targets. The appeal of drone attacks is two-fold. One, they are measurable and, two, they minimise own casualties. But on balance, the benefits seem to be outweighed. Public outrage at the strikes is hardly limited to the region in which they take place. Covered extensively by the news media, they offend the people's deepest sensibilities, alienating them from the government and, therefore, contribute to instability. Dead non-combatants represent an alienated family which can be targeted to provide more recruits in the name of the movement—there has been evidence of the growing numbers of extremists in spite of regular elimination.

The use of drones displays every characteristic of a tactic or more accurately, a piece of technology, substituting for a strategy. These attacks have to be executed with a concerted information effort directed towards a real understanding of the dynamics which may make such attacks more effective. Such drone strikes, even while attempting to separate the extremists amidst the civilian population, in the attempt to break their power to intimidate, cannot achieve this objective. Imagine, for example, that burglars move into a neighbourhood. If the police were to start blowing up people's houses from the air, would this convince homeowners to rise up against the burglars? Isn't it more likely to turn the whole population against the police? And even if the pepole wanted to turn the burglars in, how exactly would they do that? Yet, this may be the same basic logic underlying the drone war. The drone strategy is similar to the French aerial bombardment in rural Algeria in the 1950s, and to the "air control" methods employed by the British in the tribal areas in the 1920s.[54] The historical

[53] David Kilcullen and Andrew Mcdonald, " Death from Above, Outrage Down Below", published on May 16, 2009, in *New York Times*, available at http://www.nytimes.com/2009/05/17/opinion/17exum.html

[54] David E. Omissi, *Air Power and Colonial Control: The Royal Air Force, 1919-1939* (New York: Manchester University Press, 1990), pp211-222. The idea being put forth is the intrusive nature of air power that is not accepted over a period of time.

resonance of the effort encourages people to see the drone attacks as a continuation of power and control policies.

This is not to suggest that the use of air power as part of a larger design is a strategic error but to emphasise the futility of the insistence to kill, without evaluating the wasted resources behind thousands of hours of intelligence, surveillance and reconnaissance devoted to the elimination of one man, when the same resources and air effort could have achieved apprehension of the guilty, or at least efforts on that count, protection of the people, and winning over of their hearts and minds. Surgery is one thing and complete recovery after the process without collapsing the patient during the operation and after is another.

Reliance on air power has been heavy and beginning August 2009, the Pakistan Air Force has been bombing targets in South Waziristan, while the Pakistan Army has said it has sealed off many Taliban supply and escape routes.

The reliance on air power has been heavy and beginning August 2009, the Pakistan Air Force has been bombing targets in South Waziristan, while the Pakistan Army has said it has sealed off many Taliban supply and escape routes.[55] According to local residents in the region, close to the battle zone, it appears that the army appeared to be mostly relying on air strikes and artillery against militants occupying the high ground. It has also been mentioned that the insurgents were firing heavy machine-guns at helicopter gunships, forcing the air force to use higher-flying jets,[56] meeting almost the same consequences and dilemmas that the Soviets faced in the 1980s. The outcome that will finally emerge from the offensive use of air power against the militants is still awaited, but the recent onslaught is reported to have resulted in the displacement of as many as 150,000 civilians, possibly more, with as many as 350,000 whose future is unknown. The United Nations has been stockpiling relief supplies in a town near the region while hoping that a

[55] Mir Ali, "Pakistan: 60 Militants Killed in Operation Against Taliban", posted on October 18, 2009, at http://www.foxnews.com/story/0,2933,568380,00.html

[56] The Pakistan Army is up against about 10,000 local militants and about 1,500 foreign fighters, most of them from Central Asia. They control roughly 1,275 square miles of territory, or about half of South Waziristan, in areas loyal to former militant chief Baitullah Mehsud, who was killed in a US missile strike in August 2009.

major refugee crisis like the one that occurred during the offensive in the Swat Valley, does not occur.

The coercive use of air power to counter sub-conventional combat and its repercussions do not foretell a reduced use of this medium in such applications.

FUTURE TRENDS

The coercive use of air power to counter sub-conventional combat and its repercussions do not foretell a reduced use of this medium in such applications. The air force will continue to operate under limitations but with the induction of more advanced technology, the problems of collateral damage and repercussions in the form of outcry from the general public and human rights organisations can be alleviated to a large extent. To this end, the following has been witnessed:

- Induction of high resolution infrared sensors.
- Identification of high value targets by army ground observers and also air force spotters.
- High grade imagery with sophisticated surveillance devices which are ground as well as air-based. Assistance is also being provided through satellite-based tracking.

The above has provided a rare window into this other air war though it is not that only passive measures had been the trend in recent times. Since May 2009, F-16 multi-role fighter jets of the Pakistan Air Force have flown more than 300 combat missions against militants in the Swat Valley and more than 100 missions in South Waziristan, attacking the mountain hideouts, training centres and ammunition dumps of the militants.[57] The changes being made are with the sole aim of reducing civilian casualties in terms of life and property but they are also dictated by the necessity of military operations in areas where there is a reluctance to commit ground troops, particularly in rugged terrain. It is also analysed that air strikes alone cannot ultimately substitute for ground forces or for better application in sub-conventional means of fighting, though they comprise a valuable tool

[57] Eric Schmitt, "Pakistan Injects Precision into Air War on Taliban", posted on July 29, 2009, at http://www.nytimes.com/2009/07/30/world/asia/30pstan.html

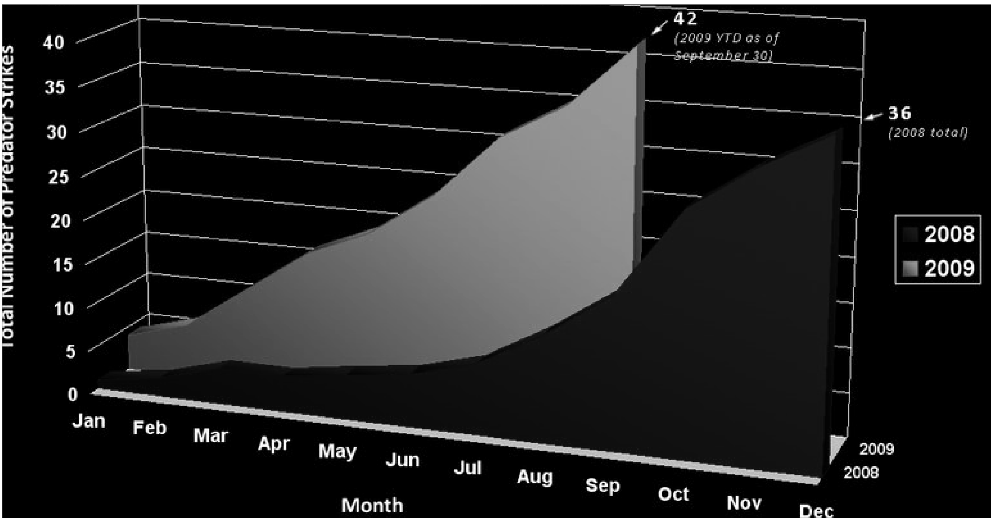
for fighting in inaccessible terrain. The scepticism that remains is that no damage assessment or information on the air strikes is available which can provide a qualitative comparison of what was intended and what has been achieved, or the actual effect.

Air strikes are only one component of solving the problem at hand. To develop truly sustainable continuity and depth in operations for extended periods, the key would rest in application of concepts and technology tailored to the specific environment.

Another aspect to be considered is that air strikes are only one component of solving the problem at hand. To develop truly sustainable continuity and depth in operations for extended periods, the key would rest in application of concepts and technology tailored to the specific environment. For example, in the arena of UAVs, rather than monitoring the cutting edge of advanced UAV systems and trying to manage cost economics concepts and technology, it might be better to seek simple, low-cost, and easily maintained systems that could fit easily into less advanced command-and-control processes. Opportunities might be found in rotary- and fixed-wing lift platforms; sensor payloads; strike platforms; command, control, and communications systems.

Operational air advisory teams of the armed forces can roll out military capabilities in support of the overall political strategy. Effective institutional infrastructure required for sustaining effective air power, ranging from recruiting and retention, through education and training, through logistics and resource management, to acquisition and procurement of material can be provided for initial advisory missions for the state paramilitary forces. A wing level structure could provide an umbrella for an embedded advisory capability. This is with emphasis on the fact that air activity to counter such kind of sub-conventional war has shown evidence of increase, contrary to a wane, though not particularly in India due to reasons not being discussed here. Fig 1 below indicates the number of predator strikes in the Afghanistan-Pakistan border region in 2008-09 (September).

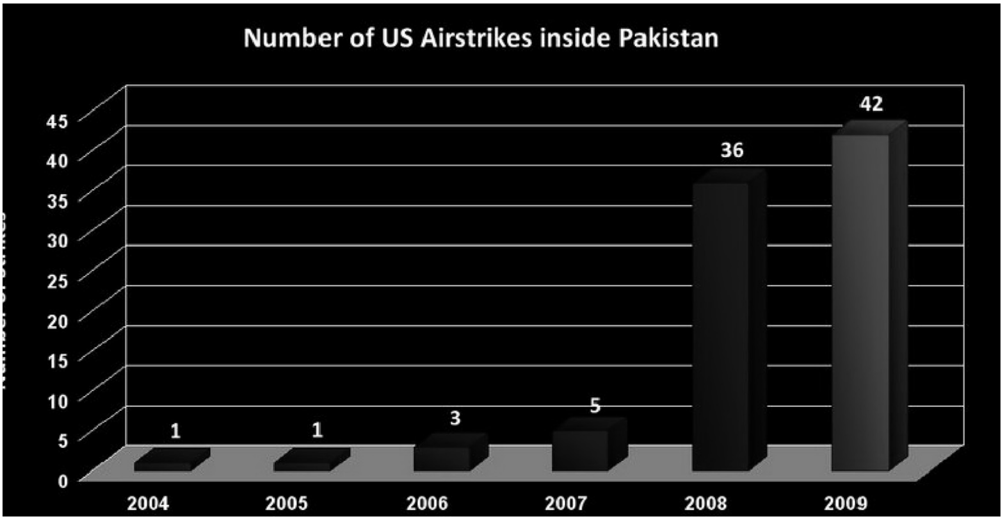
Fig 1



Source: http://www.longwarjournal.org/multimedia/US-strikes-Pakistan-Sept2009

Fig 2 also indicates the number of air strikes, that have shown an increase in the present onslaught in the Afghanistan-Pakistan border.

Fig 2



Source: http://www.longwarjournal.org/multimedia/US-strikes-Pakistan-Sept2009

The above gives evidence of the trend of increasing use of air power over the years to strike militants with either manned or unmanned aircraft. However, the lost lessons of air power have also echoed with the 'big-war' paradigm of the air doctrine, the foundation of which was laid during the formation of air power theory. The development of air power theory did change the strategic landscape of the 21st century but the limited practicality of full scale application in sub-conventional war is still evolving. The passive measures and defensive strands have been evident to various proponents of air power intervention. The realisation seems to be dawning that sub-conventional conflict, still seemingly insignificant to some, has different dimensions that can be applied selectively to avoid militants getting undue advantage through the media and public opinion.

INDIAN PERSPECTIVE

India has been battling with the sub-conventional form of warfare for decades and more intensely since the eruption of the uprisings in the northeastern states as well as J&K from the latter half of the 1980s. This kind of warfare has been extended into the hinterland, permeating into the country through its coastline as well as porous borders. How is air power useful or effective in such scenarios when the evident results are commonly evaluated on the kinetic and visible effects of such application? The Indian government had contemplated the use of air power against the Maoists but the rules of engagement in such situations had to be stringent by all measures.[58] It was clearly marked out that there would be no excessive force, no collateral damage, and only on positive identification and assurance of the above could any retaliatory but defensive action be taken. There have been some interesting responses, with a marked public one that stated that a decision to strike with air power against Naxals, who are armed, and have been killing paramilitary personnel and civilians alike for the past so many

[58] "Chidambaram Favours IAF Firing on Naxals", posted on October 07, 2009, at http://www.indianexpress.com/news/chidambaram-favours-iaf-firing-on-naxals/526200/. This was after the Maoists had stepped up intense activities and also covered the background of an Indian Air Force helicopter being fired upon and, hence, the requirement of defensive action, including survivability of own forces.

To some, the justification of using armed UAVs in the future as part of precision in warfare and effects-based operations has appealed considerably.

years, can be called for. Does one not approve of Pakistan's action in using air power to eliminate the Taliban? It may be debatable, but the fact is that in our country, while it is our very own people, they also have been killing their very own people.

The connotations are different even with the background that coercive force, in this case air power, can be used to defend against any threat which aims at disintegrating India from within or outside. First, any threat is to be exterminated from the roots and mere surgical extraction in bits will not solve that part of the menace which is firmly embedded. The airwaves have been humming with commentators who believe that Naxalism is an expression of the deep resentment of the marginalised tribals and the poor, and that development, not force, is the solution, which has also been adequately substantiated,[59] and this major deep-rooted part cannot be eliminated by air power.

To some, the justification of using armed UAVs in the future as part of precision in warfare and effects-based operations has appealed considerably. What counters this in good measure is the non-compliance of international humanitarian law which prohibits arbitrary execution, and this increasingly is being perceived as carrying out indiscriminate killings.[60] The onus here comes on the government to reveal and explain about the ways in which arbitrary and extra-judicial executions are carried out without the legal basis of selecting targeted individuals. With this, two other distinctive shortcomings area drawn up: first, it further desensitises the soldier and he becomes immune to the humanitarian aspect of dealing with humans even though they may be termed as enemies; and, second, the calibrated use of force may not be possible as it simply destroys or shoots to kill, as compared to injuring and taking into custody.

[59] "We are looking into the causes of the alienation and development deficiencies…." of the Naxal groups "How they Fight" *India Today*, October 26, 2009, p. 25.

[60] "United Nations Investigator Questions the Legality of US Use of Drone Strikes", *International Herald Tribune*, October 29, 2009, p. 4.

This is not to say that air power has no role to perform. A substantial portion of air power rests in its non-kinetic effects and application. Most states in India have not been able to impart any in-service training to their personnel in 20-25 years, [61] and so lies the fact behind their level of competency. It is also important to note that the third dimension is required to gain over outnumbering influence and leverage a multi-pronged strategy to tackle the guerrillas. Therefore, along with equipment, training becomes the essential factor before any strategy can be relied upon to deliver the ushered outcome. The air power component of the Indian armed forces is the only constituent organisation that can be relied upon to provide the necessary training to the state and central police personnel. To this effect, the entry of the state's Special Forces to fight the Naxals has marked the Cabinet Committee on Security's decision not to use helicopters in combat operations but only for relief and rescue.[62]

An offensive strategy against Naxal hideouts by making use of satellite data can always be made available by the Indian Space Research Organisation (ISRO). This, if given a practical shape, will involve the use of our weather microwave imaging satellite RISAT-II to pinpoint the support bases and movement of Naxal groups in the depths of the forests. This satellite is equipped with an X-band Synthetic Aperture Radar (SAR) and was launched in April 2009. It is capable of providing high quality images even under the cover of darkness, cloud and haze. ISRO describes RISAT as a satellite meant for monitoring floods, landslides, cyclones and agriculture-related activities. However, military analysts point out that this satellite, realised by ISRO in association with Israel Aerospace Industries (IAI), can help heighten our vigil against terrorist activities and troop movements. Designed for a lifespan of two years, RISAT-II is in a position to revisit an area in about 4-5 days. This revisiting capability is critical to intelligence gathering and surveillance and, therefore, may have to assisted by UAVs. Moreover, the highly agile RISAT-II can be manoeuvred to change its viewing angles as

[61] Mahendra Lal Kumawat, "Winning the Silent War", *India Today*, October 26, 2009, p. 26.

[62] Vishal Thapar, "IAF Not to Take Part in Anti-Naxal Combat Operation" published on October 08, 2009, at http://ibnlive.in.com/news/iaf-not-to-take-part-in-antinaxal-combat-operation/102920-3.html

For air power, combating the enduring insurgent characteristics calls for a fundamental review of the traditional balance of emphasis given to kinetic and non-kinetic air activities.

per the requirements of the users. From a strategic perspective, it implies that the satellite is ideal for monitoring human movement with a high degree of precision. RISAT-II, therefore, could prove really beneficial in zeroing in on Naxalite hideouts in the depths of the forests, and carrying out operations with minimum collateral damage. Incidentally, the Special Task Force (STF) set up to capture the notorious forest brigand Veerappan, from his forest hideout, had made use of the data from the Indian Remote Sensing (IRS) earth observation satellite of ISRO.[63] It is argued that satellites cannot always track down individuals;[64] however, jungle bases, tracks and other tell-tale signs can be deciphered and confirmed from other intelligence sources. Total dependence on one platform may not be the solution but having seen the geographical extent of our geographical vulnerable borders and permeable coastline, it may be justifiable; besides, force augmentation would require the deployment of UAVs.[65]

For air power, combating the enduring insurgent characteristics calls for a fundamental review of the traditional balance of emphasis given to kinetic and non-kinetic air activities (i.e. the mindset of striking targets outweighs information gathering). Although it is a simplistic error to typify conventional warfare means as being the primary domain for kinetic capabilities, the situation in our country is sufficiently distinct and demands a transfer of emphasis from the primacy given to kinetic capabilities. In particular, in the imperative to win and maintain the consent of both the indigenous population and the international audience, the additional use of force without sufficient constraints has

[63] Radhakrishna Rao,"Aerial Support for Countering Naxals," Paper No. 2981 at http://www.ipcs.org/article.database.phparticle

[64] "Satellites Can't Track Down…" published at http://timesofindia.indiatimes.com/news/city/bangalore/Satellites-cant-track-down-Veerappan/articleshow/20697516.cms

[65] The Coast Guard at present has 44 Air Units, including 24 coastal surveillance aircraft, 16 Chetak helicopters and four Advanced Light Helicopters (ALH). Rajat Pandit, "Year After 26/11, Coasts Still not Secure", *The Times of India*, October 29, 2009, New Delhi, p. 10.

reached high levels of scrutiny. However, this does not remove the need for lethal force in situations ,and is replete with incidents like air strikes to extricate the almost battalion strength of surrounded soldiers from Naga insurgents way back in the 1960s. The battle-winning impact of Close Air Support (CAS) to isolated or outnumbered ground forces cannot be denied in the face of humiliation and failure to defend the survivability of own forces. However, the increased priority that non-kinetic capabilities should attract is disguised by the factor of the insurgents' imprudent attempt in 'force-on-force' engagements where restraint becomes the key for state forces, as such operations by the insurgents are designed to provoke in most of the cases. It is also pertinent to note that India's problem of tackling sub-conventional tactics will keep enlarging in proportions which may not be matched with mere state force level increase in personnel. Presently, approximately 70,000[66] paramilitary personnel have already been deployed to begin operations in Naxalite affected states and, simultaneously, two influential separatists groups in Assam have also decided to step up their activities to stage terror attacks, taking the cue from the Taliban sponsored suicide attacks.[67] The country may not be able to cope with the nature of the problem and geographical expanse through only an increase in personnel without the induction of air and space technology across the front. It is not a question of tackling 10,000-15,000 militants; it involves countering their activity across 20 states and over 223 districts, and it is noted that the casualties now exceed those in J&K.[68]

India's problem of tackling sub-conventional tactics will keep enlarging in proportions which may not be matched with mere state force level increase in personnel.

The changing nature of conflict highlights the establishment of 'find, fix and strike'. While air and space power makes the amorphous environment quite transparent, it also assists in finding as well as fixing the insurgents;

[66] "Carrot and Stick", *The Times of India*, October 29, 2009, New Delhi, p. 18.

[67] "Ulfa, Bodos to Carry out Suicide Attacks", *Asian Age*, October 29, 2009, p. 1.

[68] Amarnath K. Menon, "Tackling the Red Terror", *India Today*, October 26, 2009, pp. 19-20.

the striking part can be handled in the appropriate measure by the state forces. The traditional military imperative to know what is happening or likely to happen behind a 'hill' will persist, grow, and manifest every change or step in a sub-conventional war tackling strategy. There may be certain reposturing of air power capabilities and application but unprecedented results can be forthcoming wherever air power is applied as it holds relevant solutions to addressing rising operational challenges in the sub-conventional kind of warfare.

CONCLUSION

To ensure a grounded and balanced understanding of tackling sub-conventional means of warfare with air power, there will be a need to take steps to expand opportunities for formal understanding and education on the social, psychological, cultural, political, security, and economic aspects. It is particularly important to study the impact of any air action and be able to distinguish characteristics that are idiosyncratic to a particular kind of conflict which happens to be sub-conventional in the present consideration. The Air Force does not have the force structure and personnel to support a strategy as outlined in the problem-solving matrix of the country. The cadre of specialists available with the armed forces of the country is the fulcrum on which the Services' broader capabilities are pivoted to support the police and paramilitary forces. In absolute terms and when compared with the present challenge facing the nation, air power can and should move quickly to remedy this situation. In particular, expansion of aviation advisory capacity and aspects of non-kinetic application for conflict mitigation should have the capacity and ability to shape the understanding of exploiting opportunities provided by applying air power in a way irrelevant or invisible to mainstream thinking.

TOWARDS 'INTELLIGENT' CRUISE MISSILES: CONTOURS OF INNOVATION

SITAKANTA MISHRA

As early as 1915, the *New York Tribune* described the progenitor of the cruise missile as "a device likely to revolutionize modern warfare".[1] True to this assertion, almost within a century, cruise missiles have begun to live up to the expectation. There has been significant advancement in the technologies used to construct the airframe, propulsion, penetration aids and guidance system, largely resolving the shortcomings in them. Today, the Global Positioning System (GPS) permits cruise missiles to be guided toward their targets with a level of precision that is measured in feet. Advances in propulsion technology have enabled cruise missiles now to operate at ranges that are transforming them into significant weapons. Also, innovations in stealth shaping and materials have increased their inherent survivability. With an operational pedigree covering seven decades, cruise missiles can now be regarded as "mature and well established technology".[2] The Gulf War and the Kosovo crisis of 1999 amply demonstrated how this piece of technology can revolutionise modern warfare.

* **Sitakanta Mishra** is an Associate Fellow at the Centre for Air Power Studies, New Delhi.

[1] *New York Tribune*, October 21, 1915, cited in David J. Nicholls, "Cruise Missiles and Modern War: Strategic and Technological Implications", *Occasional Paper No. 13*, Center for Strategy and Technology, Air War College, Air University, Maxwell Air Force Base, May 2000, p. 1.

[2] Carlo Kopp, "Cruise Missile Guidance Techniques", *Defence Today*, http://www.ausairpower.net/DT-CM-Guidance-June-2009.pdf, p. 55.

Certainly, significant technological advances accrued over the past forty years have transformed the cruise missiles into reliable weapons with considerable range, extraordinary accuracy, and a significant degree of survivability.[3] But due to the sheer variety available now (around 130 types) and their elastic and non-sequential evolution, tracing the magnitude of all the innovations accurately is a stupendous task. This article scrutinises only those landmark innovations in cruise missile technology which have transformed them into a state's major component of the combating inventory. Highlighting the modern attributes of cruise missiles, it identifies the current technological innovations that have actually endowed these attributes which distinguished them from their earlier versions.

CONTOURS OF INNOVATION

The attributes of modern cruise missiles are actually the offshoots of the successive value additions in different components of the missile. The journey of this missile, starting from the German V-1 to the hi-tech versions of today, in fact, is the journey of the technological "Innovation Stream"[4] conditioned by the imperatives of modern warfare, the contemporary security environment, and the technological changes occurring. Technological changes broadly constitute: (1) the incremental improvements in performance; (2) architectural advances that result from substitutions of sub-systems that are central to the device's functionality; and (3) the discontinuous or fundamental shift in the underlying technology that represents a leap in overall functionality.[5] Sometimes, the specific requirements of countries demand a specific innovation and the market is always sensitive to this. Therefore, the requirements of the current and emerging customers contribute to the flow of the innovation stream. Countries explore and exploit situations to carry forward their technological inquisitiveness. Of course, this innovation stream poses both organisational and resources related challenges.

[3] Nicholls, n. 1, p. 3.

[4] "Managing Multiple Streams of Innovation", Change Logic LLC, http://www.change-logic.com/pdf/Managing%20innovation%20streams.pdf

[5] Ibid.

As far as missile technology is concerned, the conceptual design of the innovation is most often conducted during the "exploratory development" phase. The *primary objective of exploratory development is to investigate and evaluate technology alternatives* to overcome existing shortcomings[6] (emphasis added). It is not that the existing technical shortcomings require replacement by completely new sets of technologies all the time. In fact, an "enabling technology" alone or in combination can provide the means to generate giant leaps in the performance and capabilities of the existing technology.[7] For example, the coming together of the satellite, telecommunication technologies, computer, Internet, and groupware has revolutionised the capabilities of all other existing systems. The same is the case with the evolution of cruise missile technology. The mid-Seventies saw the rebirth of the cruise missile, as inertial guidance, computer and propulsion technologies reached a level of development which allowed a new generation of these weapons. Subsequent sophistication in the enabling technologies transformed cruise missiles into the most modern and efficient weapon system.

The mid-Seventies saw the rebirth of the cruise missile, as inertial guidance, computer and propulsion technologies reached a level of development which allowed a new generation of these weapons.

Most of the advancements that have taken place in the 'enabling technologies' for the operational effectiveness of cruise missiles are related to their navigation and guidance, propulsion or engine technology, warhead and the design or the airframe. The earlier technology and design of cruise missiles mainly comprised a simple mid-course guidance (programmed autopilot or remote/command guidance), a conventional airframe (metal skin structure with conventional aerodynamic flight controls), conventional propulsion (jet propulsion or use of liquid rocket motors), and terminal

[6] Eugene L. Fleeman, "Technologies for Future Precision Strike Missile Systems – Missile Design Technology", paper presented at the RTO SCI Lecture Series on "Technologies for Future Precision Strike Missile Systems", held in Tbilisi, Georgia, June 18-19, 2001, http://ftp.rta.nato.int/public//PubFullText/RTO/EN/RTO-EN-018///EN-018-05.pdf

[7] "Enabling Technology", http://www.businessdictionary.com/definition/enabling-technology.html

Reverse engineering of German V-1 and V-2 missiles by the US and USSR in the post-War period further evolved the guidance technology.

guidance (either passive radio-frequency homing, radar, or passive infrared for terminal homing).[8] Such designs possessed severe limitations. Mid-course guidance had limited autonomy and accuracy, while propulsion systems produced limited ranges due to poor fuel efficiency (typically 300 km or less). Terminal guidance systems required a “cooperative target”, in that the ability to acquire targets at operating ranges beyond 150 km was severely limited by uncertainties in mid-course guidance.[9] Innovations in all these fields have improved the efficiency of cruise missiles gradually. The subsequent sections discuss how different enabling technologies, especially the guidance, propulsion and advanced materials used in the design of the airframe, added value to the earlier versions, thereby enhancing their overall performance.

INNOVATIONS IN NAVIGATION AND GUIDANCE

The basic objective of using a standoff weapon is to launch it from outside the enemy’s air defence system to avoid exposing the launch platform to the adversary’s retaliation.[10] But to make the missile reliably navigate thousands of miles to the target poses considerable design challenges. The German V-1, the first operational cruise missile, was guided by a gyroscope-based autopilot and an anemometer-driven distance measuring device.[11] This was especially intended for area bombardment of large urban targets like London. Before launch, the missile needed to align to the intended heading and distance, and once the odometer setting on the distance measuring device informed about the weapon arriving over the target, the autopilot would drive it into a steep nosedive. But this technique was inaccurate, with miles of error.

[8] Dennis M. Gormley and K. Scott McMahon, “Proliferation of Land-Attack Cruise Missiles:Prospects and Policy Implications”, http://ftp.fas.org/irp/threat/fp/b19ch6.htm

[9] Ibid.

[10] Kopp, n. 2.

[11] “Lawrence Sperry: Autopilot Inventor and Aviation Innovator”, http://www.historynet.com/lawrence-sperry-autopilot-inventor-and-aviation-innovator.htm#high_3

Reverse engineering of German V-1 and V-2 missiles by the US and USSR in the post-War period further evolved the guidance technology. The US Navy's Regulus series, the US Air Force's Mace/Matador series and the Soviets' KS-1 Kometa and Kh-20 Kangaroo series employed gyro-based autopilots in which radio command links permitted adjustment of the weapon's flight path. During the 1950s, all anti-ship cruise missile guidance was gyro-based, sometimes supplemented by mid-course radio link updates.[12] Terminal accuracy was provided by a compact short-range radar seeker, semi-active in the earliest designs but soon supplemented by active radar designs.[13] The next important innovation in the guidance system came with the Northrop SM-62 Snark intercontinental cruise missile. The Snark introduced a better inertial navigation system, which used a gyro stabilised platform. It also used precision accelerators to measure the vehicle's motion and an analogue computer system to accumulate measurements and locate the vehicle's position.[14]

But the drift in the inertial guidance was very high which resulted in cumulative positioning errors. Every hour of flight accumulated many miles of positioning error. To rectify this problem, another enabling technology, the stellar navigation system or the 'star tracker', was used. This is an automated optical device to measure angular measurements of the device against known star positions and used to calculate the vehicle's position in space.[15] Though it proved a success, its maintenance difficulties and the cost factor prevented this technology progressing further. However, the success of the stellar technique was path-breaking for the satellite navigation technique which was probably the progenitor of the currently used GPS and Glonass system. Satellite navigation experiments initiated during the 1960s were based on a concept similar to

[12] "Cruise Missiles of the 1950s & 1960s", http://www.vectorsite.net/twcruz_3.html

[13] Robert P. Papadakis, "Joint Vision 2010 and the Operational Commander: Is GPS A Double-Edged Sword?", http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA349297&Location=U2&doc=GetTRDoc.pdf

[14] "Northrop SSM-A-3/B-62/SM-62 Snark", http://www.designation-systems.net/dusrm/app1/sm-62.html

[15] Carlo Kopp, "Stellar Navigation to Satellite Navigation", http://www.ausairpower.net/DT-MS-0407.pdf

the stellar system, but used polar orbit satellites instead of the stars, supported by natural, light, man-made microwave signals and pseudo-range rather than angle measurements.[16]

In spite of the progressive improvements in the inertial system during the 1960s, the exorbitant cost of the system raised the debate of accuracy versus cost.

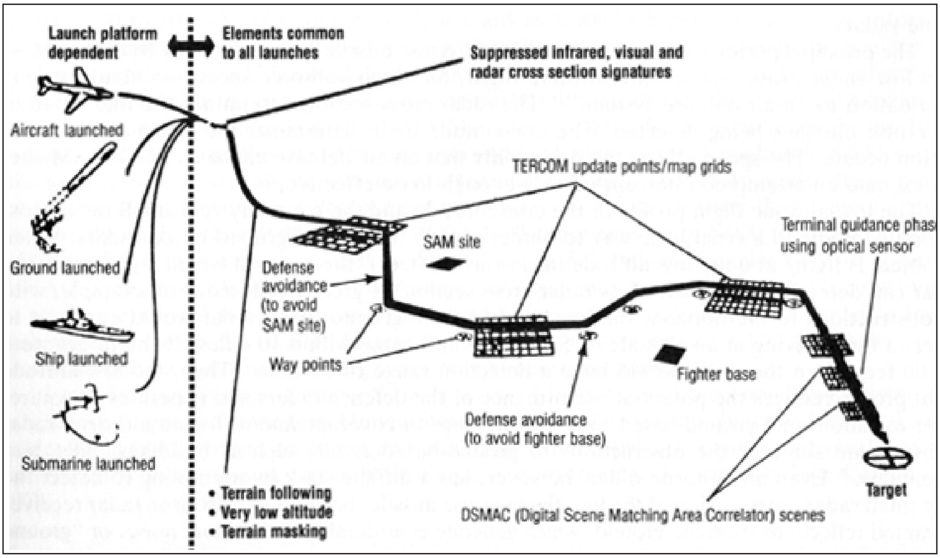
In spite of the progressive improvements in the inertial system during the 1960s, the exorbitant cost of the system raised the debate of accuracy versus cost. During the 1970s, this concern led to the next major advance in cruise missile guidance technique – the Terrain Contour Mapping (TERCOM). The technique of TERCOM was incorporated in the US and Soviet cruise missiles during the 1970s and 1980s respectively, to correct cumulative inertial system errors.[17] This technique was a significant improvement against stellar systems since it was compatible with the low altitude flight by a cruise missile. It was relatively cheap to manufacture and highly accurate, down to tens of metres. During its flight, the missile equipped with TERCOM continuously gauges the terrain elevation under its flight path by using a radar altimeter and compares the measured results with a barometric altimeter elevation.[18] The TERCOM navigator mounted on the missile carries a stored digital elevation map of the terrain it is intended to fly over. The elevation curve of the terrain flown over is then compared with the stored digital elevation map by an onboard computer, to find the best possible match. Once the profile is matched to the mapping data, the position can be found within the digital map with good accuracy to correct the inertial system error. Fig 1 shows how the TERCOM system works to guide the missile towards the target.

[16] Kopp, n. 2.

[17] Michael Dutra, "Strategic Myopia: The United States, Cruise Missiles, and the Missile Technology Control Regime", http://www.law.fsu.edu/journals/transnational/vol14_1/dutra.pdf, p. 70.

[18] "The Weapons Tutorial", *Atomic of Bulletin Scientists*, February 1984, p. 38.

Fig 1


Launch platform dependent
Elements common to all launches
Suppressed infrared, visual and radar cross section signatures
Aircraft launched
TERCOM update points/map grids
Terminal guidance phas
using optical sensor
SAM site
Ground launched
Defense avoidance (to avoid SAM site)
Way points
Ship launched
Fighter base
Defense avoidance (to avoid fighter base)
Submarine launched
• Terrain following
• Very low altitude
• Terrain masking
Target
DSMAC (Digital Scene Matching Area Correlator) scenes

Source: Joint Cruise Missiles Project Office

But TERCOM was not without shortcomings. Generating and maintaining precise elevation mapping data of the terrain over which the missile has to fly was challenging. This technique was also ineffective over water, seasonally shifting terrain like sand dunes, and terrain with varying seasonal radar reflectivity like places where snowfall could alter elevation or conceal terrain features.[19] The system represents the most significant challenge for a long-range cruise missile programme. It requires an extensive database of accurate topographic information to use terrain comparison. Sometimes, the technique becomes ineffective as some significant point is unavailable for reference. For example, for Chinese missiles like the DH-10 or CH-10, the TERCOM becomes relatively ineffective in areas such as the South China Sea.[20] Another difficulty with this technique was the storing of enough data in the onboard computer owing to its limited memory. The TERCOM, while enough for the nuclear armed Tomahawk, was not precise to hit individual buildings or structures with a conventional

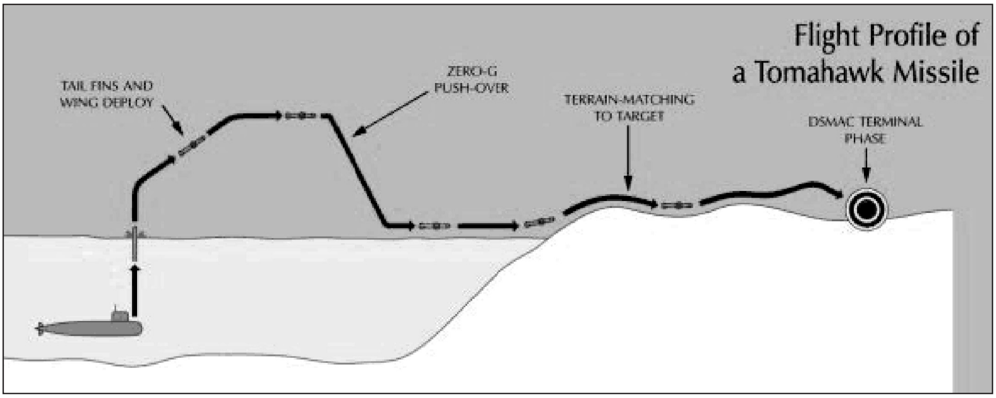
[19] Kopp, n. 2.

[20] "Land-Attack Cruise Missiles (LACM) DH-10 / CH-10, Hong Niao / Chang Feng, Dong Hai-10", http://www.globalsecurity.org/wmd/world/china/lacm.htm

warhead.[21] Therefore, the US Navy supplemented TERCOM in its RGM-109C/D Tomahawk Land Attack Cruise Missile (LACM) with an additional system termed as Digital Scene Matching Correlator (DSMAC) technology:[22] the scene matching correlator technology uses a camera to image the terrain beneath the weapon, and then digitally compares the image with a stored image produced by satellite or aerial reconnaissance. By measuring the rotation and translation required to exactly align the two images, the device can measure the position error of the vehicle very accurately, and use this to correct the inertial and TERCOM errors.[23] Fig 2 shows the flight of a Tomahawk guided by TERCOM.

By the 1980s, the GPS receivers were integrated to the cruise guidance system. This allowed the missile to continuously correct its inertial error, regardless of terrain and weather conditions.

Fig 2


Flight Profile of a Tomahawk Missile
TAIL FINS AND WING DEPLOY
ZERO-G PUSH-OVER
TERRAIN-MATCHING TO TARGET
DSMAC TERMINAL PHASE

Source: http://www.scribd.com/doc/14253521/Tomahawk-1

The DSMAC used in several blocks of the Tomahawk was indeed accurate, but produced operational side effects as it was sensitive to seasonal variations in terrain contrast.[24] This problem was sorted out by the

[21] Kopp, n. 2.
[22] "BGM-109 Tomahawk", http://www.fas.org/man/dod-101/sys/smart/bgm-109.htm
[23] Kopp, n. 2.
[24] Ibid.

use of GPS. By the 1980s, the GPS receivers were integrated to the cruise guidance system. This allowed the missile to continuously correct its inertial error, regardless of terrain and weather conditions, and worked well over both water and land. But GPS was vulnerable to jamming, as its signal is inherently faint. It was also susceptible to 'multipath' effects where GPS signals are reflected from terrain or buildings. Further, the accuracy of the flight depends on how many satellites are visible at any given time, and how they are spread across the sky. Therefore, during the late 1980s and 1990s, the guidance system became a synthesis of systems constituting the GPS, the inertial guidance package with mechanical inertial technology replaced by cheaper and more accurate ring laser gyro technology. The problems of accuracy of GPS have been progressively addressed by the introduction of the Wide Area Differential GPS technique to overcome the inherent range limits for local-area DGPS service by collecting local-area differential corrections.[25] Then, correction signals valid for a given geographical area are broadcast by radio link to the GPS receiver. For instance, the US cruise missiles used the WAGE (Wide Area GPS Enhancement) embedded in the GPS navigation message broadcast by satellites. This kind of technology could correct GPS errors down to several inches in three dimensions.

The introduction of smart antenna technology, based on 'digital beam-forming' in software, somehow addressed the problem of jamming and multipath. "With this arrangement, the GPS antenna sees the whole hemisphere above the missile, and collects signals from GPS satellites, as well as from the hostile jammers. *The Controlled Reception Pattern Antennae (CRPA) synthesises in software narrow beams which are pointed in space in the direction where the GPS almanac predicts a satellite will be, making the antenna effectively blind in all other directions. The system produces 'nulls' in the antenna pattern which are pointed at jammers to further suppress their effect."*[26] The latest generation cruise missiles are equipped with the GPS/inertial guidance supplemented by a nose mounted digital thermal imaging device to provide a DSMAC-like capability against fixed targets. Against mobile targets like

[25] Gormley and McMahon, n.8,

[26] Kopp, n. 2.

a radar or missile battery, they are empowered with suitable software and automatic recognition capability. Lastly, the data links, derived from the JTIDS/Link-16 technology,[27] are being introduced to provide capability to retarget the weapon if a mobile target is moved while the missile is en route; but to detect and retarget such movements requires reconnaissance and surveillance capability. Advancement in missile defence capabilities would pose further problems in targeting the enemy's assets through the available guidance technology but that, in turn, would induce further innovations in the system. However, analysing the trend of the evolution of cruise missile guidance, one can easily visualise that it will be ever "more intelligent, more autonomy, more diversity in sensors, better reliability and lower costs".[28]

INNOVATIONS IN PROPULSION TECHNIQUE

Starting from the V-1, which was powered by a 'pulsejet engine' that gave it its characteristic buzzing sound, to today's supersonic cruise missiles propelled by 'hybrid technology', the missile propulsion technique has undergone many evolutions. Propulsion has evolved from simple pulse jets, through turbojets and liquid propellant rockets or ramjets to the current mix of turbojets for subsonic tactical cruise missiles, turbofans for subsonic strategic cruise missiles and ramjets or mixed turbojet/rocket designs for supersonic tactical cruise missiles. The most widely known pulsejet was the German V-1 missile, or the "buzz bomb", used during World War II, which fired at a rate of about 50 cycles per second.[29] In a pulsejet, combustion is intermittent or pulsing, rather than continuous.[30] The engine admits air through the valves, and combustion is initiated to increase the pressure, closing the valves to prevent back-flow through the inlet. The hot gases are expelled through the rear nozzle, producing thrust and lowering the pressure

[27] JTIDS/Link 16 is a combination of systems that are on numerous US and Allied military platforms. It is a kind of network that allows forces to pass a variety of data back-and-forth. "Analysis of the Capabilities and Limitations of Link 16", http://books.nap.edu/openbook.php?record_id=10105&page=151

[28] Kopp, n. 2, p. 57.

[29] Kenneth P. Warrell, *The Evolution of Cruise Missiles* (Washington D.C.: Air University Press, 1985), p. 42.

[30] "The Working of a Pulsejet Engine", http://conceptengine.tripod.com/conceptengine/id17.html

to the point that the valves may open and admit fresh air. A pulsejet engine delivers thrust at zero speed, but the maximum possible flight speeds are below 960 km/h (600 mph). But poor efficiency, severe vibration, and high noise limited its use. Also, the pulsejet could not operate at speeds of less than 150 mph and required a booster and a long ramp for launch.[31]

The American programme that followed with the German V-1 led to very small fuel-efficient jet engines when the designers of the abortive US Navy Gorgon projects had planned to use a jet engine with an outside diameter of only 9 inches. The first American flying bomb experiment was the Northrop Corporation JB-1 series. The JB-1A version started with two General Electric B1 turbojets. A turbojet engine includes "a core engine, an afterburner, and a converging-diverging exhaust nozzle in serial flow communication".[32] The turbofan engines are highly fuel efficient and use a large fan, similar to a jet-engine fan, to move through the air. They offered long-range and subsonic speed with minimal infrared (IR) signature.[33] In the post-War period, Northrop proposed a subsonic turbojet-powered, 3,000-km range missile known as the Snark. The turbojet engine, as used in the Snark and in many later cruise missiles, was a small version of the type of engine used in conventional jet aircraft. It proved very efficient in matters of ranges needed by cruise missiles, particularly when they are accelerated to cruising speed. However, though the turbojet engine provided better speed, it consumed a huge amount of fuel and was capable of very limited range. Subsequently, the Snark missile programme was cancelled owing to the development of its air breathing companion, the Navaho.[34] An interim missile, the XSM-64, used ramjets, using the engine's forward motion to compress incoming air. But ramjets could not produce thrust at zero air speed[35] and, thus, could not move the device from a standstill.

Thereafter, very small fuel-efficient jet engines had started in the US and by 1962, the Williams Research Company had produced the WR-2, an

[31] Ibid.

[32] "Supersonic Missile Turbojet Engine", http://www.freepatentsonline.com/7424805.html

[33] "Military Jet Engines", http://engines.fighter-planes.com/jet_engine.htm

[34] "Navaho SSM-A-2", http://www.astronautix.com/lvs/navssma2.htm

[35] "Ramjet", http://wapedia.mobi/en/Ramjet

engine that delivered 70lb of thrust which was used to power small target drones such as the US MQM-74. By 1967, the WR-19 engine had demonstrated a thrust of 430lb for a weight of only 68lb and a fuel consumption of .7lb per hr per lb of thrust.[36] Also, further improvements in propulsion took place with the use of advanced fuels such as Shelldyne. Though it is much more expensive than conventional fuel, Shelldyne H has 33 per cent more energy per unit volume than JP-4 and could give improvements in range for the cruise missile of about 10-20 per cent.[37]

Both the turbofan and turbojet propulsion systems are most suited for subsonic cruise missiles, providing high efficiency to deliver a warhead at long range against non-time-critical targets.

Both the turbofan and turbojet propulsion systems are relatively mature technologies for precision strikes. They are most suited for subsonic cruise missiles, providing high efficiency to deliver a warhead at long range against non-time-critical targets. However, the use of the turbofan is advantageous in that it provides better fuel consumption than a turbojet, with a reduced infrared signature.[38] Most of the early variants of the cruise propulsion system were liquid fuelled. But this created many related problems that crippled the missiles' operational capability. First, the large volume fuel tank occupied a very large proportion of the mass of the vehicle, whereby the centre of mass shifts significantly rearward as the propellant is used; this results in loss of control of the vehicle when the centre mass gets too close to the centre of drag. Second, liquid propellants are subject to slosh, which has frequently led to loss of control of the vehicle. Third, liquid propellants can leak, possibly leading to the formation of an explosive mixture. Four, liquid propellants are subject to vortexing within the tank, particularly towards the end of

[36] Rajesh Kumar, "Tactical Reconnaissance: UAVs Versus Manned Aircraft", http://www.fas.org/irp/program/collect/docs/97-0349.pdf, March 1997.

[37] George N. Lewis; Theodore A. Postol, "Long-Range Nuclear Cruise Missiles and Stability", *Science & Global Security: The Technical Basis for Arms Control, Disarmament, and Nonproliferation Initiatives*, 1547-7800, vol 3, issue 1, 1992, pp. 49–99.

[38] Carlo Kopp, "The Strategic Cruise Missile", Part I, *Australian Aviation*, September-November 1985.

the burn, which can result in gas being sucked into the engine or the pump cryogenic propellant such as liquid oxygen freezes atmospheric water vapour into very hard crystals. This can damage or block seals and valves and can cause leaks and other failures.

It is pertinent to point out that ramjets differ in operation from both pulsejets, as used in the V-1, and from turbojets, such as employed in the Snark. The ramjet engine takes in air through a choke or diffuser in the inlet, which slows down the airflow and increases its pressure. The air is then mixed with fuel and continuously ignited by means of a spark-plug. The resulting combustion produces a jet of hot gases in the tail-pipe which react against the enclosed forward parts of the engine to generate a steady thrust. The 1950s saw different versions of the same missile using pulsejets, turbojets or ramjets. But subsequent experiments aiming at long-range started to enhance the engine capability, and thereby, the Modern Ramjet Engine (MRE) was developed. For example, in 1973, there was a perceived need to extend the range of the Phoenix missile because of enhanced threat capabilities. The MRE employed an IRR engine and, since it would require manoeuvring for the anti-air mission, it incorporated two cheek-mounted two-dimensional inlets and had bank-to-turn controls, the same as an airplane. The MRE concept used an integral rocket booster for vehicle acceleration to the ramjet takeover speed.[39]

In the USA, in the early 1970s, the Generic Ordnance Ramjet Engine system was developed through engine testing at NAWC/CL (Naval Air Warfare Centre/China Lake). The configuration chosen was a parallel rocket and annular ramjet. In the mid-1970s, a number of propulsion systems were being investigated for a long-range anti-air missile. Consequently, both solid-fuelled and liquid-fuelled ramjet engine development and demonstration programmes were initiated at NAWC/CL. The performance goals for both were to fly 150 nautical miles (nm) at a cruise speed of more than Mach 3. In the early 1980s,

[39] Paul J. Waltrup, et al., "History of Ramjet and Scramjet Propulsion Development for U.S. Navy Missiles", http://www.scribd.com/doc/6097480/History-of-Ramjet-and-Scramjet-Propulsion-Development-for-US-Navy-Missiles

Today, the propulsion unit of a cruise missile employs all the available and upgraded engines of the turbofan, pulsejet, turbojet, ramjet or solid fuelled rockets.

following successful semi-freejet engine tests of these missiles, a second-generation integral rocket, liquid-fuelled ramjet long-range air-to-air missile was developed for the Advanced Air-to-Air Missile (AAAM) system.[40]

In 1982, the US Air Force began studies for a new cruise missile with low-observable characteristics after it became clear that existing cruise missiles would have difficulty penetrating future air defence systems. The solution adopted was to incorporate various low-observable (stealth) technologies into a new Advanced Cruise Missile (ACM) system. The first test missile flew in July 1985 and the first production missiles were delivered to the US Air Force in 1987. The end of the Cold War led a major cutback in total ACM procurement. In all, 461 missiles were ultimately produced.[41] Another propulsion technique comprises the composite motor cases. Composites provide reduced weight compared to a steel motor case. It is viewed that the emphasis on reduced observable plumes will continue with high emphasis in the foreseeable future.[42]

Today, the propulsion unit of a cruise missile employs all the available and upgraded engines of the turbofan, pulsejet, turbojet, ramjet or solid fuelled rockets, each making a different category with different advantages and shortcomings. For example, the French Exocet missile, which is solid fuelled, designed to attack large ships, is very fast but of short range and with a significant IR signature.[43] The Chinese C-802 or the Yingji-82 missile powered by a turbojet engine is supersonic. Due to the missile's small radar reflectivity, low attack flight path (only five to seven metres above the sea surface) and the strong anti-jamming capability of its guidance equipment, target ships have

[40] Ibid.

[41] http://www.onwar.com/weapons/rocket/missiles/USA_AGM129.html

[42] Eugene L. Fleeman, "Technologies for Future Precision Strike Missile Systems – Introduction/ Overview", paper presented at the RTO SCI Lecture Series held in Atlanta, USA, 23-24 March 2000.

[43] "Exocet AM.39 / MM.40", http://www.fas.org/man/dod-101/sys/missile/row/exocet.htm

a very small chance of intercepting the missile.[44] However, the engine consumes a lot of fuel and has limited range. The turbofan US Tomahawk missile is highly fuel efficient and quiet. It offers long range and subsonic speed, with minimal IR signatures. The Block IV (TLAM-E) is the latest improvement to the Tomahawk missile family with advanced capability such as: (a) increased flexibility utilising two-way satellite communications to reprogramme the missile in flight to a new aimpoint or new pre-planned mission, send a new mission to the missile en route to a new target, and missile health and status messages during the flight; (b) increased responsiveness with faster launch timelines, mission planning capability aboard the launch platform, loiter capability in the area of emerging targets, ability to provide battle damage indication in the target area, and capability to provide a single-frame image of the target or other areas of interest along the missile flight path.[45] Lastly, the Russian SS-21 with the ramjet engine requires a booster to flow air at supersonic speed to take on further propulsion.

The Chinese C-802 or the Yingji-82 missile powered by a turbojet engine is supersonic.

The design of the cruise propulsion depends on the mission the system is assigned for. The first consideration of the system design for the liquid propulsion system is to decide which type of propellant to use for the specific type of mission. The most obvious advantage of the liquid propulsion system, as compared to its solid counterparts in general, is thrust management and control. Some missiles use both solid and liquid propellant for effective functioning. For example, the BrahMos has a two-stage propulsion system, with a solid-propellant rocket for initial acceleration and a liquid-fuelled ramjet responsible for sustained supersonic cruise, thereby competent for longer range.[46] An important aspect of the development of a cruise missile propulsion system is the use of a new generation of jet fuels – synthesised liquid

[44] "C-802", http://en.wikipedia.org/wiki/C-802

[45] "Tomahawk Cruise Missile", http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1300&ct=2

[46] http://www.brahmos.com/home.php

hydrocarbon fuels which increase the range of these missiles approximately 15 per cent over that attainable with conventional military and commercial aviation fuels.[47] Also, very small, efficient jet (turbine) engines which have very low-specific fuel consumption have been designed.

The cruise propulsion system has graduated manifold and will continue to evolve in the future.

The cruise propulsion system has graduated manifold and will continue to evolve in the future. For example, the Advanced Missile Propulsion Technology (AMPT) programme of the US Air Force aims to provide the products, services, and development required to support AMPT. The desired technologies span all areas of application for Solid Rocket Motors (SRMs), including ballistic and space boost, post-boost propulsion and tactical motors.[48]

INNOVATIONS IN THE AIRFRAME

The aerodynamic design or the airframe of the cruise missile which is responsible for the overall performance of the device has undergone many changes over the years. The airframe technology and designs have become progressively more compact to accommodate internal and external carriage by aircraft, launch tubes on warships or torpedo tubes in submarines. The composing materials, the composite structure, insulation materials, the shape of the device and stealth capability have constantly been improving to achieve the real purpose of the cruise missile.

In the domain of airframe materials technology, mainly five new enabling technologies have been innovated: (1) hypersonic structure materials; (2) composite structure materials; (3) hypersonic insulation materials; (4) multi-spectral domes; and (5) reduced parts count

[47] G.W. Burdette, H.R. Lander, J.R. McCoy, "High-Energy Fuels for Cruise Missiles", *Energy*, vol.2, no.5, September-October 1978.

[48] "Advanced Missile Propulsion Technology (AMPT)", https://www.fbo.gov/index?s=opportunity&mode=form&id=368ba3589e27404a0c700bdbce57461b&tab=core&_cview=1

structure.[49] Since the low cost cruise missile is designed to fly at subsonic speeds, the aerodynamic design of the airframe is made with fibreglass reinforced with phenolic resins containing hylon, silica, graphite or carbon and Kevlar composites, mainly to reduce radar profile.[50] Coatings containing finely ground ferrites also offer some degree of radar absorption. The heat signature of the engine could be significantly reduced by judicious entraining of slipstream air to dilute and cool the jet exhaust prior to ejection behind the craft.

To penetrate strategic air defence in depth, cruise missiles have to evade all defence mechanisms.

The composite materials are of new technology that finds increased use in new versions of cruise missiles and are good candidates for lighter weight insulation.[51] High temperature composites have particular benefits for hypersonic missiles, providing weight reduction. Titanium alloy technology also enables lighter weight missiles in a hypersonic, high temperature flight environment.

Six new enabling technologies in the field of missile aerodynamics are promising to extend cruse missiles capabilities. These are aerodynamic configuration shaping, lattice tail control, split canard control, forward swept surfaces, bank to turn manoeuvring, and flight trajectory shaping.[52] The tailored-lifting-body missile has higher aerodynamic efficiency (lift-to-drag ratio) with enhanced manoeuvrability that is appropriate for extended range cruise performance. Lattice fins are effective for lower hinge movement and higher control at the supersonic Mach number.

To penetrate strategic air defence in depth, cruise missiles have to evade all defence mechanisms. By reducing the infrared signature emitted by the engine, the missile can minimise the chances of its detection by enemy radar.

[49] Ion Dinescu and Mihaela Oprescu, "Technologies for Future Precision Strike Missile System", The Annals of "Dunarea De Jos", University of Galati, Fascicle IX Metallurgy and Materials Science, Air Force Academy, Henri Coanda, Brasov, 3003, p. 26

[50] Bruce Simpson, "The Low Cost Cruise Missile: A Looming Threat?", May 20, 2002, http://www.aardvark.co.nz/pjet/cruise.shtml

[51] Dinescu and Oprescu, n. 49.

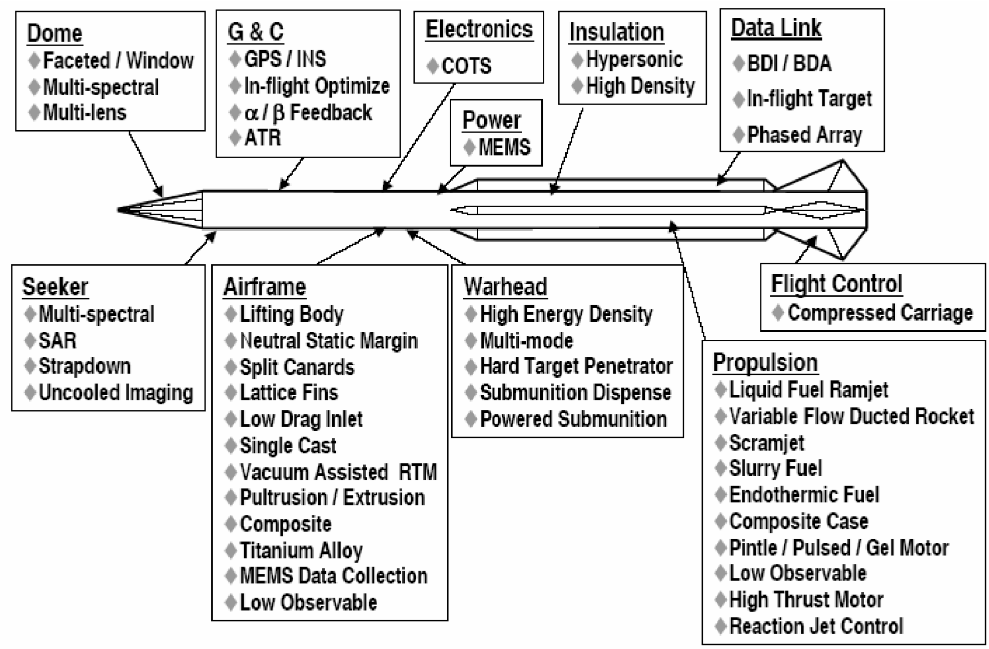
[52] Ibid., p. 24.

Present-day airframe design and the materials used have considerably enhanced its stealth capability. Penetration aids emerged during the 1960s as air defence systems evolved to greater potency, with low altitude terrain following or sea skimming flight profiles to hide missiles from radars and, increasingly, stealth shaping and materials to deny acquisition and tracking by air defence radars. Some Soviet cruise missiles were equipped with track-breaking defensive jammers to defeat interception by air defence missiles. For example, in 1982, the US Air Force began studies for a new cruise missile with stealth characteristics after it became clear that the AGM-86B Air-Launched Cruise Missile (ALCM) would soon be too easy to detect by future air defence systems.

The AGM-129 Advanced Cruise Missile (ACM) delivers the proven effectiveness of a cruise missile enhanced by stealth technology when the threat is deep and heavily defended.[53] Its external shape is optimised for low observable characteristics and includes forward swept wings and control surfaces, a flush air intake and a flat exhaust. These, combined with radar-absorbing material and several other features, result in a missile that is virtually impossible to detect on radar. Its stealth features are apparent: the nose is sharply pointed with sharp edges or chines, reminiscent of the chines used on the SR-71 Blackbird; the missile's wings are swept forward at 26 degrees, again to reduce reflections back to a radar transmitter/receiver forward of the missile; its turbofan engine exhaust consists of a 2D nozzle. It is in a 2D shape to allow the hot exhaust to rapidly mix with the cool surrounding air to reduce the overall IR signature. The inlet is mounted flush with the fuselage to reduce its Radar Cross-Section (RCS), and the missile is constructed with radar-absorbing materials and structures. Fig 3 lists all the new technologies for precision strike missiles.

[53] "AGM-129 Advanced Cruise Missile [ACM]", http://www.globalsecurity.org/wmd/systems/acm.htm

Fig 3



Source: http://ftp.rta.nato.int/public//PubFullText/RTO/EN/RTO-EN-018///EN-018-$I.pdf

TOWARDS 'INTELLIGENT' CRUISE MISSILES

Technological innovations are always purpose-driven though they create a demand for themselves, subsequently leading to demand-driven adaptations. As specific purposes or objectives change, demands for new technology propel further innovations. For example, Hitler's objective was to target the entire city of London, therefore, random firing of V-1 missiles served his purpose even though they were not accurate in targeting. Today's warfare warrants targeting of an individual or a particular building/ bunker. Also, sometimes a state has to wage a war within its own borders. Therefore, the shape of the battlefield has undergone surprising alterations and, thereby, the choices for weapons. One classic example is the use of the Israeli short-range AGM 142 "Hav Nap" cruise missiles by the American commanders which could fly directly into the mouths of the caves sheltering Osama bin Laden's forces in the Tora Bora mountains of eastern Afghanistan.[54] To fight such wars, more intelligent weapons are in demand. The cruise missile is perhaps the first kind of modern weapon which is constantly striving to reach the target by conveniently evading all surveillance.

Due to the cost, the imperative now is to improve the single shot kill probability of a missile to a certainty.

This stream of cruise missile evolution is ongoing and it will continue to move forward in the decades to come. Due to the cost, the imperative now is to improve the single shot kill probability of a missile to a certainty. With the innovations in the different fields of missile technology, the cruise missile as a "smart weapon" is fast becoming a "brilliant weapon" or an "intelligent weapon" that can manoeuvre, recognise and reach pin-point to the target. With advances in artificial intelligence, the deployment of "Intelligent Agents" (IA) has improved the performance of the missile and decreased the 'miss-distance' (the distance between the target and the closest point of approach of the missile) to a small value.[55] The IA is an autonomous entity which observes and acts upon an environment and directs its activity towards achieving goals. As a cooperative problem solver in a multi-agent environment, it negotiates by exchanging information with other agents to solve a problem.[56] In a conventional missile guidance system, from the launch to the time when terminal homing takes over, signals from ground-based radar are received and processed by the receiver unit onboard the missile. The signal environment can be hostile if jammers are present. Therefore, in modern missile systems, intelligent agents are interconnected to generate counter-moves in the hostile environment. For example, to overcome jamming, modern cruise missiles install the digital thermal imaging devices that interconnect the GPS/inertial guidance to provide DSMAC-like (Digital Scene Matching Area Correlator) capability. Many such intelligent agents are in use these days for appropriate counter-moves relevant to different phases of the missile's flight.

[54] Sean Rayment, "'Intelligent' Missile Used Against bin Laden Caves", December 16, 2001, http://www.telegraph.co.uk/news/worldnews/asia/afghanistan/1365479/Intelligent-missile-used-against-bin-Laden-caves.html

[55] V.Krishnabrahmam, N. Bhardwaj and K.N. Swamy, "Guided Missile with an Intelligent Agent", *Defence Science Journal*, vol 50, January 2000, p. 25.

[56] V.V.S. Sarma, "Intelligent Agents", *Journal of IETE*, vol. 42, no. 3, 1996, pp. 105-109.

The cruise missile evolution trend seems to be moving from aid to autonomy.

Generally, conventional cruise missiles are either track-in on some sort of signal or fly to a pre-determined point: there is no situational awareness of decision-making capability in the "end game" or no independent call as to whether or not to press "the kill". Subsequent innovations in the missile sub-systems have gradually infused some sort of decision-making power in the machine, whereby cruise missiles as "smart weapons" have fast become "intelligent weapons" that can manoeuvre, recognise and reach pin-point to the target. Therefore, the cruise missile evolution trend seems to be moving *from aid to autonomy*. Samuel Penn has categorised missiles into six categories according to their operational attributes (Table 1). But today's cruise missiles seem to imbibe all the novel features of previous versions and are constantly striving to become more *intelligent*. For example, the Thirsty Sabre missile can conduct a smart search of the area for targets, and once identified, kick out one of several munitions before moving on to the next target. The Tactical Tomahawk acts like a spy plane which can fly around the target area, give commanders a bird's eye view of the battlefield and then be re-programmed for new instructions. The German Taurus KEPD 350 smart penetrator system is capable of recognising already destroyed structures and counting floor levels of the buildings it attacks.

Table 1

Manual	**Homing Missile**	**Smart Missile**	**Brilliant Missile**	**Clever Missile**	**Genius Missile**	***Intelligent Missile***
Very basic missile.	Locks onto its target using very simple criteria, such as heat signature or nose.	Remote controlled.	Capable of homing in on a designated target.	Capable of making its own choices about targets.	Capable of selecting a target based on many criteria, using strategy to select not only the best target, but also the best route to the target.	Smart + Brilliant + Clever + Genius

Manually guided, being controlled remotely by an observer with a simple joystick. No guidance system of its own. Uses the heavy weapons skill of the controller.	Once fired, the target cannot be changed. They can be confused by sending out decoys.	The observer must maintain control until the last moment. No intelligence itself.	Designation is by a human operator, but after the missile is fired, no further designation is required (unlike for a smart missile). May use a number of techniques for recognising the target, but mostly based on visual or signature recognition.	Once a target is selected, it is capable of following that target itself without outside aid. It actively recognises its target, does not rely on a simple criteria such as heat for tracking.	Capable of working together in swarms, deciding between themselves how to divide up the targets, and changing targets as conditions change. Contra-grave genius missiles have the capability to lie in wait for targets, dodge counter-measures and generally behave like living attackers.	

Source: Samuel Penn, "Yags (Missiles 1.3), 2007", www.glendale.org.uk/yags/articles/missiles.pdf

The Taurus stealthy missile navigates through GPS guidance and an infrared seeker with visual displaying capabilities. The latter scans the overflown terrain at pre-defined checkpoints for possible variances from the pre-set course in order to correct its flight path. The system is designed as a standoff weapon against high value and heavily defended targets and can deliver its explosive power with an extremely high accuracy.[57] Depending on the type of target, several different detonation sequences and final target approach tactics can be applied. For underground bunkers, the Taurus can

[57] "German Stealth Cruise Missile Enters Service", http://www.strategypage.com/htmw/htairw/articles/20060402.aspx

attack in a nosedive to maximise the penetration depth. Less hardened targets will be engaged in an extreme low level flight to minimise the danger of detection. Therefore, this millennium seems to be the age of "intelligent missiles" and the current innovations have begun to suit the requirements of modern warfare: for instance, the US Intelligent Missile Project aims to develop techniques for embedding rule-based artificial intelligence system in the US Navy's missiles.

The key parameters in the fabrication of any cruise missile are its standoff range, its accuracy and its survivability against target defences.

The key parameters in the fabrication of any cruise missile are its standoff range, its accuracy and its survivability against target defences.[58] With advanced research and ongoing experiments, the cruise missile would be equipped with more advanced features. At the general level, further innovation in cruise missile technology is likely to drive down the total cost. The aim in the future would be to improve the reliability by accepting some increase in the unit costs, but, at the same time, reducing the number of devices required to complete a given mission. Second, improved miniaturised engines and new fuels can be expected to decrease the power plant/payload ratio. Third, advances in IR detector design seem likely to produce important operational improvements. In particular, the number of IR detector elements that can be fitted within an IR seeker head is being dramatically increased. Fourth, the continuing trend in micro-miniaturisation of electronics increases computational densities that have been produced over the recent years. For example, in the mid-1970s, it was possible to fit about 1,000 gate-arrays or the equivalent of seven transistors into a device measuring one quarter of an inch square. By the early 1980s, the capacity had been increased by a factor of four, and by 1985, a device only one-third larger could hold no fewer than 19,000 gate-arrays. In the last decade, computing power, using these and other devices, has increased by a factor of ten and the volume required has been reduced by a factor of six. This continuing

[58] Kopp, n.2, p. 55.

process of increasing computational density has very important implications for the operational functions of the future cruise missile and in particular for the physical size of the payload. Lastly, a significant field is stealth technology which is likely to play a major role in the future of air warfare in general and the cruise missile in particular. There is constant effort to innovate Radar Absorbent Materials (RAM) to reduce RCS. Together, the micro-miniaturisation, guidance and stealth techniques will to play a formative role in deciding the place of cruise missiles in the broader spectrum of air power.

This implies that no matter how sophisticated the technology, the issue of effective air defence would always remain.

With the advances in the defence mechanism and the technology used in specific missiles, chasing of an incoming missile has become possible. For example, the DSMAC used in several blocks of the Tomahawk, though it proved accurate, produced operational side effects during the 1991 Desert Storm campaign. During the operation, for the effective manoeuvre of the Tomahawks towards the selected targets, a number of Baghdad freeway intersections were used as referencing points, which actually allowed Saddam's air defence troops to set up gun batteries and shoot down a number of Tomahawks. This implies that no matter sophisticated how the technology, the issue of effective air defence would always remain. The very characteristics which made the V-1 a headache for British air defence planners in 1941, present the same broad issues for contemporary air defence system planners even though the technology of cruise missiles today is vastly superior to that of the early years. But what has changed between the earlier and current versions of the cruise missiles is the upgraded technology that has given the weapon radically increased capabilities.

CYBER SPACE VULNERABILITIES AND CHALLENGES: THREATS TO NATIONAL SECURITY DYNAMICS

M.K. SHARMA

Dominating the info spectrum is as critical to conflict as occupying the land or controlling the air has been in past.

— General John P. Jumper
USAF Chief of Staff

Cyber space is shaped by policies; it is not some natural feature or 'thing' that grows wild and free naturally.[1]Today, nations are incessantly trying to shape the realm of the Internet and enforce their authority in cyber space to the best of their ability. The asymmetric threat posed by the information revolution has got cyber security to the centre of national security policy concerns. The importance and relevance of the issue for the security community is based on the fact that the information infrastructure that serves as underlying infrastructure for government organisations, industries and the economy has become a key asset in today's security environment.[2]

All critical infrastructures are becoming increasingly dependent on the information infrastructure for information management, communication

[*] Wing Commander **M.K. Sharma** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

[1] John Perry Barlaw, "A Declaration of the Independence of Cyber Space" (1996) http://www.eff.org/homes/barlow.html.

[2] National Research Council, *Computer Science and Telecom Board Trust in Cyber Space* (Washington, D.C, 1999).

and control functions. Since the information infrastructure enables both economic vitality and military and civilian government functions, it has become a strong national security component. The dependence of defence and government information infrastructures on commercial (public or private) providers and cross-national inter-connection of infrastructures (post-liberalisation and globalisation) have heightened the security requirement of infrastructures in countries across the globe.

Cyber security means the measures for protecting computer systems, networks and information from disruption or unauthorised access, use, disclosure, modification or destruction.

The sophistication in the hacker tools has come of age from mere password guessing ability and self-replicating codes in the 80s, to password cracking, exploiting known vulnerabilities, back doors and disabling audits in the 90s and gaining all new heights of sophistication with techniques like sweepers, sniffers, hijacking sensors, stealth diagnostics and packet forging or spoofing today. This has resulted in availability of phenomenally powerful hacking tools, with a simultaneous sharp drop in the technical knowledge required to use them.

Cyber security means the measures for protecting computer systems, networks and information from disruption or unauthorised access, use, disclosure, modification or destruction.[3] Connectivity is increasing at a rate beyond the capacity to implement controls. Market pressures on hardware and software vendors reduce the introduction of security features and testing prior to product release. Retrofitting security into existing systems and applications is difficult, expensive, and, in some cases, impossible without serious operational impact. However, a more fundamental problem exists in the implementation of controls in that few organisations invest in proper risk assessment before implementing controls. Even fewer understand and qualify specific threats in order to evaluate risks accurately. The consequences can be profound because not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist

[3] As defined by the National Science and Technology Council (2006), p. ix.

or have minimal impact. Fundamentally, security is the identification and management of risk.

The aim of this paper is:

- To study the factors responsible for rising the vulnerabilities of cyber space.
- To study the nature and type of threats posed to cyber space.
- To review the cyber crime and security assurance level of Indian cyber space.

To find an answer to why cyber security has become an issue today, we must understand that the threats in cyber space remain, by and large, the same as in the physical world, for example, fraud, theft, terrorism, etc. There is an attacker and a victim, and the attacker requires the same three components to be successful: Motive, Opportunity and Means (MOM)**.** However, due to Information and Communication Technology (ICT) induced developments, things have changed today; automation has made attacks more profitable; action at a distance is now possible, with anonymity; and attack technique propagation is now more rapid and easier.

Today, MOM is more powerful than ever. Even a novice can download powerful intrusion tools and find free written guides to penetrate systems. The motive is there because there is no barrier to entry for an attacker: millions of pages of free instruction are available to anyone interested in reading it – massively accessible means**.** In a few minutes, you can hack a bank account and steal someone's life savings because there are still many financial institutions that do not protect their clients and their systems with any sophistication – for some, this presents an irresistible opportunity. So the stage is set today – powerful motive, perfect opportunity and the best means.

Intruders are building technical knowledge and skills, gaining leverage through automation, exploiting network interconnections and moving easily through the infrastructure, and they are becoming more skilled at masking their behaviour. In addition to this, there are three new trends that make all network dependent organisations transparent and vulnerable: Internet enabled connectivity; wireless networking; and mobile computing. Today, e-commerce, m-commerce supported by well-known brand names and critical sectors certainly make a good recipe for trouble for governments across the globe.

There is an evident reluctance on the part of public and private enterprises to implement cyber security measures, perhaps because the stakeholders, including the customers, have not yet started insisting on an assurance. Many organisations would not want to implement strong security measures thinking that they do not have anything that others would want – probably what they do not realise is that they could become launch pads for attacks on others through bots[4]. Quite possibly, there could be other pressing issues of survival that relegate security to an afterthought, especially in a period of economic recession like the current one. Besides this, there is a very difficult choice between convenience and security measures. The trouble is more serious if you are part of critical information infrastructure[5]—there could be someone who is determined to get you for obvious reasons. The need is to have not only preventive abilities, but also keep a track of the adversary's capabilities with the changing times.

VULNERABILITIES

The argument doing the rounds in various international fora that India is not vulnerable to cyber threats as the network penetration is very low and most government work is still done on paper files, does not stand ground because of the very fact that most of the things (economy, finance, banking, defence Services, academia, R&D centres and other NCII[6]) that matter to the very existence of the nation are networked. Possible vulnerabilities within

[4] A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie—in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator. Most computers compromised in this way are home-based. According to a report from the Russian-based Kaspersky Labs, botnets—not spam, viruses, or worms—currently pose the biggest threat to the Internet. http://en.wikipedia.org/wiki/Zombie_computer

[5] In India, the following sectors are considered critical: telecommunication, energy, defence, banking and finace, railways, space, civil aviation, insurance, ports, petroleum and natural gas, atomic energy and law enforcement agencies. Subimal Bhattacharjee, Argus Integrated Systems and Luthra & Luthra Law Offices, *The Country Survey of India 2006,* CIIP Handbook 2006 edition.

[6] National Critical Information Infrastructures.

various domains are required to be understood as many new sectors get networked each passing day.

Are the vulnerabilities to cyber attacks increasing with advancements in ICT? Apart from the increase in the number of techniques and sophistication in the methods of attack enjoying the anonymity of the source, there are increased vulnerabilities due to the sheer size and complexity of networks. Today, hundreds and thousands of small, Personal Computer (PC)-based client systems can be connected into a local area network; each of these systems is then interconnected to thousands to form local and wide area networks. The ability to understand the systems, network topologies, points of access and the myriad applications and users is beyond a single system administrator. This lack of control allows security weaknesses to develop or go unnoticed. As size and complexity grows, so does the speed and frequency of changes in terms of basic technology as well as applications and uses of computers and networks. Often, a system administrator finds it impossible to keep up with the functionality of new hardware and software. Within a large network, systems, applications and databases are added and removed daily. Remote connections are constantly changing. Again, in large networks, it is beyond a single system administrator to keep up with the continuous change. This allows vulnerable or unprotected entry points into the network.

Laptops and hand-held systems combined with wireless and cellular technologies add a new dimension to the complexity and control of access to systems and networks.

Mobility and portability is yet another factor adding fuel to the fire. Laptops and hand-held systems combined with wireless and cellular technologies add a new dimension to the complexity and control of access to systems and networks Again, authentication of legitimate users becomes difficult, if not impossible; also, tracing suspicious activity is much more difficult. These issues, combined with other techniques such as social engineering and taking advantage of security flaws within software, create environments where weaknesses in security can develop. Security is usually considered an afterthought in network design and implementation, and retrofitting security into an existing network can be costly and time consuming. To gain unauthorised access to systems and data, intruders can exploit all of these weaknesses.

BROAD CATEGORISATION OF INTRUDERS' OBJECTIVES

Any nation's resolve to invest in ICT security stems from the ongoing conflict between attackers and security agencies. This reflects the wide variety of motivations and goals of different players, as well as the technological tools and procedures available. Hackers are only one type of unauthorised users. There are many other types of attackers, including terrorists, criminals, unsatisfied employees, hostile and not so hostile nation-states. When it comes to national cyber security, the distinction between different types of enemies (attackers) on the basis of their source of motivation, and resources available to finance the attack is very important to build and choose the right strategy to handle any contingency.

When we look at the complete ICT infrastructure used by the private and public sectors and individuals worldwide, it mainly consists of three categories of resources: first, computing resources such as Central Processing Units (CPUs) and memory used to run applications; second, storage resources such as disc drives and Storage Area Networks (SANs) used to store data; and third, network resources, including routers, wireless access points and hubs, optical fibre cables and satellite links, which connect multiple storage and computing resources together. Therefore, it is evident that the network components are the most common targets because they provide access and allow the attacker to threaten applications, operating systems or storage or computing resources, once inside.

In the broad perspective of national security, any attack on the ICT infrastructure can be viewed as one or more of the specific goals of a state or non-state actor or individual or group to inflict economic damage on the target. This act has to be driven by some motive, with the specific goal being technical objectives. The motives are human objectives, which include financial gain, inflicting malicious harm or furthering national or ideological interests. To understand the vulnerabilities of our ICT infrastructure, an insight into the specific goals or technical objectives of the attacker serves as a better tool. Broadly, there could be three different objectives of the attacker or a combination of them:

1. **Damaging or Diminishing the Effectiveness of the Vital Cyber Security Infrastructure Components:** These attacks generally cause one or more vital portion of a network infrastructure to either become inoperable or to operate at a diminished capacity. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks or the attacks that could cause a vital server or router to go offline or reboot, fall in this category of attacks. These attacks could be directed at a specific organisation, government or individual, intended to disrupt services for a large number of hosts (i.e. end users) or a network.

   This happened in Estonia when its paperless government was attacked not through it geographical borders but through the Internet, affecting all major commercial banks, telecommunications, media outlets, and name servers. This was the first time and certainly not the last time that a botnet threatened the national security of an entire nation. Like nuclear radiation, cyber war doesn't make you bleed, but it can destroy everything. It's a classic example of a DDoS attack.

   The attacker could also disrupt services for a large number of hosts or networks through worms[7] or viruses[8] that can infect a host and propagate to other connected hosts. In the process, as a byproduct or direct consequence of virus activity, vital data on the infected host could be destroyed. French fighter planes were unable to take off after military computers were infected by a computer virus called "Conficker" transmitted through Windows, in October 2008, as the French military ignored the warnings and failed to install the necessary security measures. [9]

[7] A computer worm is a self-replicating computer programme. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing programme. Worms almost always cause at least some harm to the network, if only by consuming bandwidth http://en.wikipedia.org/wiki/Computer_worm

[8] A computer virus is a computer programme that can copy itself and infect a computer without the permission or knowledge of the owner. http://en.wikipedia.org/w/index.php?title=Special%3ASearch&search=&go=Go

[9] Kim Willsher, "French Fighter Planes Grounded by Computer Virus," *Ouest France,* Published: 11:43 am GMT, February 7, 2009.

Another very popular way this objective can be achieved is through Unsolicited Commercial E-mail (UCE) or spam, as it is commonly known. Analogous to barrage jamming[10] of a radar to saturate its receivers, a large number of spam messages originating from, or sent to, a single e-mail server, can crash it or degrade its performance, in the bargain causing delays in the delivery of important e-mail messages.

2. **Gaining Unauthorised Access to the Target's Sensitive Data and Information:** Most public organisations and particularly the private business organisations are vitally dependent on their proprietary information, including new product information, personnel data and / or from client records. An attacker may derive direct economic benefits from gaining access to and/or selling such information, or may inflict damage on an organisation's reputation. The attack may be preceded by worms and viruses that create back doors in the target's infrastructure (e.g. Blaster worm[11]) for an attacker to enter and collect information. Other ways of gaining confidential information could be: sniffing vital information from the network traffic originating from, or intended for, the target; guessing or cracking passwords on the systems of interest to gain access to the system; or causing a privilege escalation, in which an insider working in the organisation uses security holes to increase attacker's access level.

   Recently, the Chinese firm GE (Geely Excellence) launched a car at the Shanghai motor show with a price tag of £30,000, which is supposed to be the stolen copy of the original Rolls-Royce Phantom design with a £250,000 price-tag, the preserve of a privileged few.[12] Rolls-Royce is considering legal action against the Chinese copycat. This just shows how

[10] Barrage jamming: jamming by transmitting a band of frequencies that is large with respect to the bandwidth of the victim emitter, such that the victim emitter will not be able to avoid this noise signal by retuning. Wing Commander Sanjay Poduval, *Electronic Warfare: War In The Fourth Dimension* (New Delhi: KW Publishers, 2009), p. 31.

[11] The Blaster Worm (also known as Lovsan or Lovesan) is a computer worm that spread on computers running the Microsoft operating systems: Windows XP and Windows 2000, during August 2003. http://en.wikipedia.org/wiki/Blaster_(computer_worm) , http://www.cert.org/advisories/CA-2003-20.html.

[12] "Rolls-Royce-Considers-Legal-Action-Against-30000-Chinese-Copycat," http://www.telegraph.co.uk/motoring/5205369/Rolls-Royce-considers-legal-action-against-30000-Chinese-copycat.html : 9:31AM BST 23 Apr 2009

much of R&D effort can be stolen by unauthorised access to confidential and sensitive data.

A popular way of such attack is phishing[13] in which the attacker attempts to extract private and confidential information from the target by crafting forged e-mails or websites that pretend to originate from, or belong to, an entity the target may trust. Attackers who broke into TD Ameritrade's database (containing all 6.3 million customers' social security numbers, account numbers and e-mail addresses as well as their names, addresses, dates of birth, phone numbers and trading activity) also wanted the account usernames and passwords, so they launched a follow-up spear phishing attack.[14] Almost half of phishing thefts in 2006 were committed by groups operating through the Russian Business Network based in St. Petersburg.[15] Such e-mails generally attempt to solicit bank account numbers, credit card numbers or other private information from their targets for further resale or misuse. They can also modify or delete sensitive information, resulting in damaging consequences for their targets.

3. **Gaining Unauthorised Access to Cyber Resources for Illegal Use:** The technical objective is to attack and utilise the storage and network resources like disc space (for storing illegal images, video games, etc) of the victim's computers. The victim could be anyone from an individual with a computer and a broadband connection to an employee of a large organisation with multiple sites networked together who may possess resources that an attacker could utilise. A more popular form of this type of attack is manifested in breaking into systems to get free services, such as free access to the Internet using a personal or corporate wireless access point or in attacking the billing infrastructure of a cell phone

[13] Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT Administrators are commonly used to lure the unsuspecting public. http://en.wikipedia.org/wiki/Phishing

[14] "Torrent of Spam Likely to Hit 6.3 Million TD Ameritrade hack Victims," http://www.webcitation.org/5gY2R1j1g

[15] Brian Krebs, " Shadowy Russian Firm Seen as Conduit for Cybercrime," *Washington Post*, October 13, 2007.

service provider for getting free access to cell networks. In fact, cellular service providers are more vulnerable to these attacks than fixed line phone service providers. Convergence of digital and voice service on a single network allows attackers to introduce attack packets into the network more easily. Also, the fact that today's cellular networks have a direct connection to the Internet makes them more vulnerable to attacks from the Internet.

Like all other military targeting, most cyber attacks are preceded by the surveillance and reconnaissance phase in which the attacker gathers maximum possible information about the target.

Combination of Objectives: Generally, the attacker pursuing one of the goals goes through several steps, which may include one or more of other goals before the final goal is achieved. For example, an attacker may first scan a portion of the network to find any vulnerable hosts, then use an exploit to gain access to a number of personal computers connected to the Internet (objective 3) to perform a DoS attack on part of the target's infrastructure (objective 1), such that the attack disables the protective infrastructure of the target and the attacker may gain access to the target's confidential information (objective 2). The blaster worm that targeted hosts' running server applications took control of vulnerable hosts with the ultimate objective to launch a DoS attack on the Microsoft website that was scheduled to start on a specific day, when all infected hosts would begin generating bogus traffic intended to disrupt Microsoft's infrastructure.

Like all other military targeting, most cyber attacks are preceded by the surveillance and reconnaissance phase in which the attacker gathers maximum possible information about the target (individual, organisation, network component or nation's critical information infrastructure). This phase helps in identifying weaknesses in the target infrastructure that can later become a target of direct attack. The methods include: network scans to determine the topology of the target network, intercept and look at the content of packets travelling through the data lines using 'sniffer' applications; information about the target from open sources (Internet, print media, other types of media); social engineering, which involves meeting employees of the target organisation under an assumed identity (e.g. a sub-contractor or an employee from a remote unit). The latest tool for gathering information is called wardriving, where vulnerable wireless access points are identified and mapped using wireless laptops equipped with a Global Positioning System (GPS). Information gathering could also be directed to specific network components, hardware or software. An attacker may work to find a hole or bug in an operating system or application that is widely used by the target organisation/nation so that an attack can easily be launched on many individuals/organisations simultaneously (which make the usage of the multi-operating system in an organisation good mitigating strategy against cyber attack).

Broadly, there are two main phases of launching a cyber attack. The first phase is to perform a detailed mapping of the net, collecting data on active network devices to carry out a vulnerability analysis. In this respect, many networks worldwide detect a more or less regular activity of mapping, often performed by unidentified sources. In the second phase, the appropriate software weapon is released; however, release does not mean activation. The activation can be done later, programmed to occur at a certain time, under certain defined, logical conditions or following a specific command. In some cases, the test reaction can also be performed in advance, to evaluate the defence capabilities of the victim system.

Information and Communications Sector: In addition to the natural disasters, the primary threats to this sector are system failures and instabilities arising from the increased volume and complexity of interconnections. In the past, there have been documented deliberate attacks and intrusions through the software-based disruption of network devices and management systems. In recent years, the Public Switching Telephone Network (PSTN) has increasingly become software driven, remotely maintained and managed through computer networks, which has increased the vulnerability to electronic intrusion. The existence of mega-centres for operations support creates a single point of failure and makes the targeting of hostile action easier. As the Internet was basically not designed for high-level security purposes, all infrastructures based on IP (be it Internet-based or Intranet-based) are vulnerable by design.

Energy Sector: The federal government of the United States admits that electric power transmission is susceptible to cyber warfare. The United States Department of Homeland Security works with the industry to identify vulnerabilities and help it enhance the security of control system networks. The federal government is also working to ensure that security is built in as the next generation of "smart grid" networks is developed. In April 2009, reports surfaced that China and Russia had infiltrated the US electrical grid and left behind software programmes that could be used to disrupt the system. The North American Electric Reliability Corporation (NERC) has issued a public notice that warns that the electrical grid is not adequately protected from cyber attack. China denies intruding into the US electrical grid. One counter-measure would be to disconnect the power grid from the Internet to decrease the likelihood of attack. Massive power outages caused by a cyber attack could disrupt the economy, distract from a simultaneous military attack, or create a national trauma.

The level of vulnerability to this sector has been increased by the recent rapid proliferation of industrywide information systems based on open architecture used in the operating environment. This includes increasing reliance on communication links which sometimes run over public telecommunication networks. The national power grid in India is yet to see the light of day but vulnerabilities on account of using Commercially-Off-the-Shelf (COTS) hardware and software cannot be ruled out. COTS are considered risky because detailed specifications might not be available or may simply not be met by some of the components, causing limitations of functionality or faults due to law quality standards. They may sometimes, have built-in vulnerabilities and may pose problems of security and dependability.

NCW and Defence Intranets: India is rapidly moving towards developing Network-Centric Warfare (NCW[16]) capability. NCW is vital; a nation cannot survive for long against a good adversary without this capability today. It is

[16] NCW, a concept pioneered by the United States Department of Defence, relies on computer processing power and networking communications technology to provide shared information of the battlespace among the armed forces. This shared awareness increases synergy for command and control, resulting in superior decision- making, and the ability to coordinate complex military operations over long distances for an overwhelming war-fighting advantage, http://en.wikipedia.org/wiki/Network-centric_warfare

estimated that the Indian Air Force (IAF) would possess NCW capability by 2011-12. The backbone of this entire system will be a fibre optic-based network called Air Force Network (AFNET), of which the recently acquired Airborne Warning and Control System (AWACS) will be the sky link to integrate all ground and air-based weapon platforms and communication systems. For the IAF's net-centric operations, the Integrated Air Command and Control Systems (IACCS) riding on AFNET, will provide the connectivity for all the airborne platforms and ground platforms.[17]

If we were to think that all defence networks, are independent networks on dedicated Fibre Optical Cable (FOC) and so are immune to cyber attacks, this could only be wishful thinking.

If we were to think that all defence networks, including the Air Force Network (AFNET), Army Wide Area Network (AWAN)[18], and Navy Enterprise Wide Network (NEWN), etc are independent networks on dedicated Fibre Optical Cable (FOC) and so are immune to cyber attacks, this could only be wishful thinking. While these are amongst the first major initiatives undertaken to prepare the Indian armed forces for fighting in the digital battlespace, these Intranets are also exposed to enormous vulnerabilities. For instance, most of the hardware and software of these projects is of the COTS type, with the fault control and maintenance being undertaken remotely. The risk of not knowing all the details of the hardware, the possibility of hidden bugs in the system, and the controls being remote and at a single point pose threats to secure Command, Control, Communication, Computers, Information, Intelligence (C4I2). The sensitivity of information in defence C4I2 makes these independent Intranets vulnerable to the insiders' threat. Going by Murphy's Law, and given the fact that in all locations/ stations there are a few authorised Internet connections for the field commanders' use and for obtaining meteorological data, etc, the possibility of intermingling/ cross-connections (deliberate or inadvertent) of the Internet and AFNET/AWAN/

[17] Quoted as saying, Vice Chief of Air Staff Air Marshal P. V. Naik at the Nellis Air Force Base, while participating in the prestigious Red Flag exercise, dated 16/8/2008.

[18] Army Wide Area Network (AWAN), which has been designed to connect all Army formations, units, training establishments and logistic installations in the country. President Abdul Kalam congratulated the team of the Corps of Signals and Tata Consultancy Services for undertaking this project and completing it in time across 174 signal centres.

NEWN cannot be totally ruled out in spite of explicit written instructions and Standard Operating Procedures (SOPs) being in place.

There are also the vulnerabilities arising due to non-compatibility of data links of different defence Services Intranets.

There are also the vulnerabilities arising due to non-compatibility of data links of different defence Services Intranets. Sharing of real-time information is vital to execute Effect-Based Operations (EBOs) in a net-centric environment. Integration of old technology weapon platforms to modern Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) networks through interfaces has two distinct vulnerabilities: the limitation on operational capabilities and increased probability of system failure because of system complexity alone, without any external trigger.

The advent of advanced systems like the 'Suter' programme[19] which has been tested with aircraft such as the EC-130, RC-135, and F-16CJ and has been used in Iraq and Afghanistan by the US since 2006 and presumably by the Israeli Air Force to sneak into Syrian air space undetected in Operation Orchard on September 6, 2007[20], has opened up a plethora of new vulnerabilities for systems like the Integrated Air Command and Control Systems (IACCS) of the IAF and computer controlled integrated Air Defence Systems (ADS) around the world.

Banking and Finance Sector: This is, by and large, considered the safest

[19] A military computer programme developed by BAE Systems that attacks computer networks and communications systems belonging to an enemy. Development of the programme has been managed by Big Safari, a secret unit of the United States Air Force. It is specialised to interfere with the computers of integrated air defence systems. Three generations of Suter have been developed. Suter 1 allows its operators to monitor what enemy radar operators can see. Suter 2 lets them take control of the enemy's networks and direct their sensors. Suter 3, tested in summer 2006, enables the invasion of links to time-critical targets such as battlefield ballistic missile launchers or mobile surface-to-air missile launchers. http://en.wikipedia.org/wiki/Suter_(computer_program) and David A. Fulghum, "Why Syria's Air Defenses Failed to Detect Israelis", *Aviation Week and Space Technology*, October 3, 2007.

[20] US Air Force officials have speculated that a technology similar to Suter was used by the Israeli Air Force to thwart Syrian radars and sneak into their air space undetected in Operation Orchard on September 6, 2007. The evasion of air defence radar was otherwise unlikely because the F-15s and F-16s used by the IAF were not equipped with stealth technology. John Leyden (October 4, 2007). "Israel Suspected of 'Hacking' Syrian Air Defences", *The Register*, http://www.theregister.co.uk/2007/10/04/radar_hack_raid/. Retrieved on 2007-10-05

domain, the main vulnerabilities being of physical nature. India as a nation has put strong measures in place for securing these infrastructures and providing extensive redundancy. However, there remains some level of risk from disruption of telecommunication and electric power services. Besides large-scale infrastructure vulnerabilities, this sector also suffers from lucrative opportunities for theft and fraud in individual branches/institutions.

The most potent and persistent threat to the banking sector comes from the insiders, who might be authorised access to confidential information or operate systems, which could be used for personal profit. Another negative fallout is its intrinsic sensitivity and in order to maintain public confidence, financial institutions will often avoid reporting to the Computer Emergency Response Team (CERT)-In or any external agency. This reduces the transparency of the system, making analyses of intrusions and protection of the overall infrastructure more complicated.

Transportation Sector: As this sector is becoming increasingly reliant on ICT infrastructure, new cyber vulnerabilities are emerging every day, for example, the website of Eastern Railway was hacked on December 24, 2008, by a Pakistani group[21] claiming that the site was hacked in response to the alleged violation of Pakistani air space by the Indian Air Force.[22] These freak incidents may not seem alarming at face value, but certainly show the potential that cyber power holds in future wars in the region. It should serve as a wake up call to military planners to accrue the asymmetric leverage through cyber power in furthering national objectives.

The recent crash of two Washington DC Metro transit trains (June 22, 2009) in which the train ploughed into a stationary train ahead of it, killing

[21] The note posted on the hacked page of the railway website read "Cyber war has been declared on Indian cyberspace by Whackerz- Pakistan," http://www.dnaindia.com/mumbai/report_indo-pak-cyber-war-hots-up_1219482

[22] This hacking incident followed a similar defacement of the website of the Criminal Investigation Department (CID) of the Andhra Pradesh police, which had been compromised by Pakistani hackers soon after the 26/11 strikes. Soon after the attacks, an Indian group -- Guards of Hindustan -- hacked into the website of the Oil and Gas Regularity Authority of Pakistan and posted their logo and the Indian national emblem on it. In retaliation, the Pakistan Cyber Army, hacked the websites of the Indian Institute of Remote Sensing, the Centre for Transportation Research and Management, the Army's Kendriya Vidyalaya of Ratlam and the Oil and Natural Gas Corporation (ONGC). http://www.dnaindia.com/mumbai/report_indo-pak-cyber-war-hots-up_1219482

nine people and injuring more than 70, was the deadliest accident in the 30-year history of the Washington Metro and is being attributed to the failure of the computerised system to halt an oncoming train.[23] This is yet another example of vulnerabilities due to the rapidly expanding use of the intelligent transportation system to optimise and increase overall efficiency.

The most significant vulnerabilities are considered to be those associated with modernisation of the National Air Space System (NAS) for Air Traffic Control (ATC).

The PCCIP[24] report of the US states that the most significant vulnerabilities are considered to be those associated with modernisation of the National Air Space System (NAS) for Air Traffic Control (ATC). This includes plans to adopt the GPS as the sole basis for radio navigation in the country by 2010.

Indian air space management is still evolving. Its infrastructure, mainly shared by the civil aviation sector and Air Force, consists of a confusing mix of obsolescence and modern equipment and infrastructure. The ATC at most Air Force bases is mainly primary radar-based and, at civil airports, it is being done with the Monopulse Secondary Surveillance Radar (MSSR) equipment, with little redundancy in place. Planning of scheduled maintenance also requires ad-hoc change in procedures for controlling, and a breakdown of MSSR is immediately converted into a crisis for ATC. The metro airports have the satellite-based ADS systems, with the Services being provided by the sole provider to the global aviation industry, SITA[25]. The latest of the systems available, like the Controller Pilot Data Link Communication (CPDLC), are data link-based and are, thus, prone to unauthorised intrusions by programmes like 'Suter' which can not only observe or jam but can also manipulate (Suter 3) the data being fed through data links. Even the Modernisation of Airfields Infrastructure (MAFI) project of the IAF is based on the COTS hardware and software

[23] Brian Witte, Brett Zongker, Matthew Barakat, Gillian Gaynair, Alex Dominguez and Sagar Meghani, *Associated Press*, June 23, 2009.

[24] President's Commission on Critical Infrastructure Protection, US.

[25] SITA is a multinational information technology company specialising in providing IT and telecommunication services to the aviation industry. Originally known as the Société Internationale de Télécommunications Aéronautiques, http://www.sita.aero/.

products and shared communication networks. As a consequence, the risk of unauthorised access and the probability of malicious actions would only increase. Before we get our Indian Regional Navigational Satellite System (IRNSS)[26] in place, overreliance on GPS is a matter of concern and to be viewed with caution as access to the Global Navigation Satellite Systems, GPS, is not guaranteed in hostile situations. Besides India does not have ultimate control over GPS services; it is also prone to jamming (transmission of noise interfering with the original signal) and spoofing (broadcast of false GPS information).

THREATS

How do potential cyber disasters compare with disasters in the physical world? In the physical world, there is immediate loss of lives and infrastructure, like in Mumbai 26/11 or US 9/11, or a natural disaster like the Bhuj earthquake on January 26, 2001. On the other hand, the damage from a cyber attack does not necessarily and directly manifest in loss of lives or infrastructure like in the cyber attacks on Georgia and Estonia. However, it can jeopardise/compromise the essential services such as medical information system or transportation system, which, in turn, could affect lives. India, in the very near future is going to get so many of her essential services networked, and a cyber attack disrupting communication and electric power distribution would become a real and quite probable threat. Disruption of transportation (surface and air), shipping, and financial transactions by cyber means would become more frequent and intense. Interaction of the cyber and physical world with terrorist minds would bring out the force multiplier facade of cyber power to the fore. Think of the damage to a railway track being used to carry troops, with simultaneous disruption/altering of trains routing and reservation data by a cyber attack or an aircraft hijacking with a successful

[26] IRNSS is an autonomous regional satellite navigation system being developed by the Indian Space Research Organisation which would be under the total control of the Indian government. The requirement of such a navigation system is driven by the fact that access to the Global Navigation Satellite Systems, GPS, is not guaranteed in hostile situations.:"India to Build a Constellation of 7 Navigation Satellites by 2012", http://www.livemint.com/2007/09/05002237/India-to-build-a-constellation.html

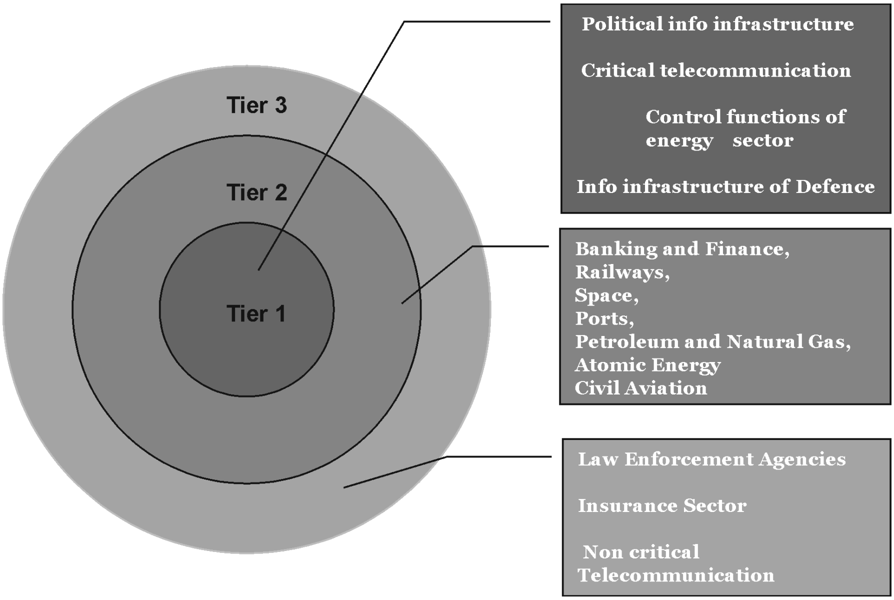
cyber attack on ATC systems. Obviously, the damage would be more catastrophic.

Persistent firepower coupled with persistent ISR cannot be maintained without a truly secure and robust networking of these assets.

Cyber Centres of Gravity: Giulio Douhet in his work *Command of The Air*, has suggested that massed effects against an enemy's centres of gravity can lead swiftly to bloodless victory. For the conduct of such Effect-Based Operations (EBOs), the basic enabler is Network-Centric Operations (NCO). Network-Centric Warfare (NCW) enables Intelligence, Surveillance and Reconnaissance (ISR) results to be applied in near real-time to execute EBO, thus, achieving rapid victory by attacking the coherence of the enemy's ability and will to fight. It is obvious that persistent firepower coupled with persistent ISR cannot be maintained without a truly secure and robust networking of these assets. This is where the cyber threat comes to the centre-stage of security concerns. So, how serious is the threat and how do we assess it? One traditional way (which may not be the best way for this asset, not bound by geographical boundaries and space) of looking at cyber security is that all the national cyber assets be grouped in tiers (say three tiers) on the basis of centres of gravity as shown in Fig 1.

Tier one, the innermost centre of gravity, would consist of those components of the National Critical Infrastructure (NCI) which are critical to national security and sustaining human life such as political information infrastructure, critical telecommunication sector, control functions of the energy sector and info infrastructure of the defence sector, etc. This must be made as robust as possible. The components of Tier two, the next centre of gravity, would consist of those cyber assets which are important to the country's economy even if they are not likely to cause physical harm if disabled, such as banking and finance, railways, space, ports, petroleum and natural gas, atomic energy and civil aviation, etc. The third tier, the outermost centre of gravity, would consist of systems whose disruption would cause considerable personal inconvenience or economic loss but would not present a threat to the existence of the society as a whole, such as law enforcement agencies, insurance sector, non-critical telecommunication sector, etc.

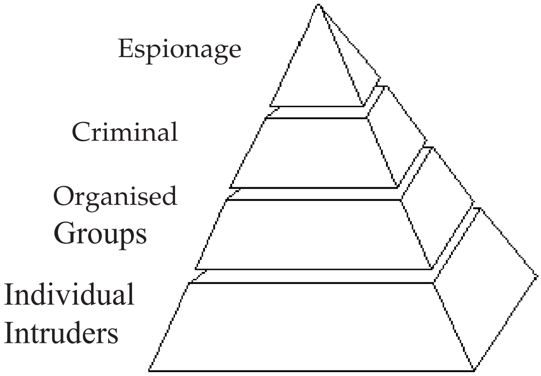
Fig 1: Cyber Centres of Gravity


Tier 3
Tier 2
Tier 1
Political info infrastructure
Critical telecommunication
Control functions of energy sector
Info infrastructure of Defence
Banking and Finance,
Railways,
Space,
Ports,
Petroleum and Natural Gas,
Atomic Energy
Civil Aviation
Law Enforcement Agencies
Insurance Sector
Non critical Telecommunication

CATEGORISATION OF INTRUDERS

Who are the actors? The canvas is very wide: there are professionals or amateurs or hobbyists who would spend nights on the computer to break into electronic systems. Often with no malicious intentions but for a personal challenge or just to grab media headlines. There are also those groups, including insiders, that are involved in industrial, economic or corporate espionage motivated by money or revenge. There are other individuals/corporations who are targeting for financial information resources or actively seeking a competitor's trade secrets, often using insiders. Furthermore, there are politically motivated state and non-state groups, ranging from government agencies like intelligence agencies or military units to terrorist groups; their goals could include information collection, propaganda, electronic surveillance, censorship and sabotage.

Fig 2: Intruder Categorisation Model[27]



To get an insight into both the patterns of activities and the scale and scope of general threats to systems and networks, a general categorisation of the intruders (not exactly hackers[28]) based on the motivations behind intrusions can be done, based upon Kent E. Anderson's model, as shown in Fig 2.

Individual Intruder: Usually acting independently in the pursuit of personal goals, the motive of these individuals is generally the challenge or thrill of gaining access to a computer system. They may cooperate to some extent in loose associations, sharing information and techniques. However, there is usually no strategic planning or organised tactics for penetrating systems or networks. Also, the resources available to this level of intruder are usually limited to popular, off-the-self PCs and peripherals.

Gary McKinnon[29] from north London has been accused of committing the "biggest military computer hack of all times", cracking open the systems

[27] Kent E. Anderson, "International Intrusions: Motives and Patterns" (Proceedings of the 1994 Bellcore/Bell South Security Symposium) May 1994, pp. 3-5.

[28] Due to the academic controversy with the word "hacker" and the common public misconception of a "hacker" as a bad guy, a malafide intentioned youth, the term *intruder* will be used to describe an individual who illegally accesses or makes unauthorised use of a system.

[29] Jon Ronson, in an interview to *The Guardian* on July 9, 2005, revealed that the most exciting thing he saw was a list of officers' names under the heading "Non-Terrestrial Officers" who he thinks are not earth-based. He also found a list of "fleet-to-fleet transfers", and a list of ship names which weren't US Navy ships, but believed to be some kind of spaceship, off-planet. news.bbc.co.uk/1/hi/technology/4715612.stm

of the Pentagon and National Aeronautic Space Agency (NASA). He caused damage and impaired the integrity of information. The US military district of Washington became inoperable and the cost of repairing the shutdown was $700,000 . If extradited to the US, he faces up to 70 years in jail.

Organised Groups: Organised groups vary from loose affiliations with common interests (and often separate, individual goals) to highly cohesive organisations with well-defined goals. The major motivation for this category is entering a computer system to gain access to specific information or system and network resources. Organised groups may have any number of interests in information such as political or environmental vandalism, access to proprietary technical information or personal information such as credit reports.

There are innumerable examples of organised groups, including the German Chaos Computer Club (CCC),[30] the Dutch Hack-Tic group[31], the English group 8lgm, the US Legion of Doom (LOD)[32] and participants of the Japanese Otaku.[33] A classic example of a group loosely organised around to have access to specific information is described in the US Government's Sentencing Memorandum for several Legion of Doom (LOD) members whose motive was to obtain power through information and intimidation.[34]

These groups typically have moderate to high (systems level) knowledge of computer and telecom systems, switches and networks. The resources available may include small networks, bulletin boards/voice mail systems and access to funds via membership dues, newsletter subscriptions and press speaking or book royalties.

Criminals: Currently, this is the highest growth area in terms of both number of intrusions and monetary damage, and the primary motive of the criminal category is to gain access to a system for profit or unfair market share. They have technical abilities ranging from very low to high, or may

[30] K. Brunnstein, "Report: 8th Chaos Computer Congress", *Risks-Forum Digest*, vol. 13, issue 03, January 10, 1992

[31] Ibid.

[32] US Government's Sentencing Memorandum, US v. Grant, Darden and Riggs, Criminal Action Number 1:90-CR-31, December 1990.

[33] K. Greenfield, "The Obsession of the Otaku" *Los Angeles Times*, , September 12, 1993, p. 40.

[34] n. 32.

recruit technical skills (either with or without the individual's knowledge of criminal activity). The crimes involving monetary gain include wire transfer theft, industrial espionage,[35] credit card theft,[36] or pseudo security consultants. It is believed that the development of the Tupolev Tu-144 supersonic aircraft, with its rapid design and similarity to the Concorde, was one of the most prominent examples of industrial espionage in the 20th century.

The 2004 E-Crime Watch Survey published by CERT estimated that companies lost $666 million from e-crimes in 2003. Recently, the Computer Security Institute and the Federal Bureau of Investigation (FBI) reported in their 2005 Computer Crime and Security Survey that 56 per cent of respondents experienced a security breach in 2004 and 13 per cent didn't know if they had a security breach. In the US, a recent annual survey of companies by the Computer Security Institute and the FBI revealed that 90 per cent of all firms have had some type of Information Technology (IT) security breach in the past year. Eighty per cent of respondents reported a financial loss and 74 per cent responded that the Internet was the most frequent source of attack.

Espionage: This category of intrusions has the greatest variety and complexity of methods and resources. Often, the resources available (equipment, manpower and technical knowledge) are only limited by cost versus the potential gain, similar to criminal activity. With the primary motive of access to systems or information for national economic or strategic objectives, this category has direct national security ramifications.

The Internet security company, McAfee, stated in their 2007 annual report that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities. It is a cyber Cold War, and with many countries

[35] The Government of France has been alleged to have conducted ongoing industrial espionage against American aerodynamics and satellite companies and vice versa. This list, compiled from public sources over the last fifteen years, is of the countries that are known to be customers of stolen US technology: Argentina, Brazil, France, India, Iran, Iraq, Israel, Japan, Lebanon, Libya, North Korea, Pakistan, People's Republic of China, USSR(Russia), South Africa, South Korea, Taiwan.

[36] The cost of credit card fraud reaches into billions of dollars annually. In 2006, fraud in the United Kingdom alone was estimated at £535 million or US$750–830 million at prevailing 2006 exchange rates.

engaged in clandestine activities, intelligence agencies are routinely testing networks, looking for weaknesses. These techniques for probing weaknesses in the Internet and global networks are growing more sophisticated every year.

Several examples of this type of activity have been reported concerning both the former East German intelligence service[37] and the former Soviet Union[38], with the major focus being on obtaining technology. More recently, many countries like China, Germany, Russia, the US, etc are believed to have an interest in obtaining access to proprietary technical information and information that could assist in advancing national economic objectives.

Proper and accurate threat assessments will allow computer security experts, vendors, and government agencies to better predict future vulnerabilities and mitigate damages.

Proper and accurate threat assessments will allow computer security experts, vendors, and government agencies to better predict future vulnerabilities and mitigate damages. Risk is generally defined as "the possibility of loss". As it applies to information technology, risk is "the possibility for loss of availability, integrity, or confidentiality due to a specific threat". Risk assessment is the analysis of the likelihood of loss due to a particular threat against a specific asset in relation to any safeguards to determine vulnerabilities. Assets are those objects, both physical (buildings, computer hardware, laptops) and virtual (e-mail, software, databases) having value to an organisation.

In considering infrastructure vulnerabilities, threats to both individual systems and the infrastructure itself must be evaluated when considering criminal activity. Both share similar enablers as a prerequisite to compromise, however, infrastructure attacks require a more concerted and coordinated effort and provide better data points for indicator and warning analysis. It is important to distinguish between the two types of attacks in threat assessments.

[37] "Economic Espionage", *Capital*, October, 1992.

[38] C. Stoll, *The Cuckoo's Egg*(New York: Doubleday, 1989).

TYPES OF ATTACK

Infrastructure Attack (IA): An attack designed to compromise significantly the function of a whole infrastructure rather than individual components.[39] A successful infrastructure attack could be capable of sustaining compromise beyond a temporary period. This will usually require attacking recovery systems as well. A successful IA may lead to cascading failure in other infrastructures. The longer the compromise is sustained, the further the effects will propagate. A successful infrastructure attack would most likely be viewed as a national security threat by most countries. However, an attack against an infrastructure that causes significant damage and cost, but is recovered without major disruption and does not affect other infrastructure components i.e. the disruption is localised and contained, would be called a limited infrastructure attack. A limited infrastructure attack could be compared with a major natural disaster such as a power outage experienced due to a heavy snowstorm.

Systems Attack: These are the attacks targeted against individual systems or control centres, which are not detrimental to the overall operation of a whole infrastructure or organisation. It is important to assess the potential and actual damage from these attacks. A successful system attack could be an intrusion where the basic integrity of a system is compromised. This compromise may lead to the loss of confidentiality, data integrity, or system resource availability. However, the attack does not target the infrastructure in which the computer operates.

Successful attacks against information infrastructures are possible though very difficult to carry out. One such known attempt was the attack against the French telecommunications infrastructure initiated by the Chaos Computer Club (CCC) in Germany in September 1995.[40] The CCC called for a denial of service attack against French telecommunications systems to protest against nuclear testing in the Pacific. However, at that time, this

[39] Kent Anderson, "Intelligence-based Threat Assessments for Information Networks and Infrastructures," *Network Risk Management, LLC,* pp. 3-5.

[40] M.A. Gasser, *Building a Secure Computer System* (New York: Van Nostrand Reinhold, 1988). Chaos Computer Club, "Stop the Test", http://www.zerberus.de/texte/aktion/atom/, September 1, 1995.

attack had no impact. If a successful attack were simple, a malicious code such as computer viruses or normal component failure would have already caused massive damage. Successful infrastructure attacks will require precise targeting, and successful, coordinated attacks against multiple system and control points, with exact timing to compromise system redundancy. Attacks may also require compromising multiple levels in the infrastructure architecture (i.e. applications, protocols, system software, and hardware) as well as recovery systems such as back-up operations. However, the virtual reality of cyber power is that the ability to cause damage that once required the military of a nation-state is now within the reach of much smaller, less organised groups.

Where do these Threats Come From (Insiders or Outsiders)? Traditional wisdom holds that insiders are the greatest threat to an organisation. This is based on two assumptions: first, insiders have access; and second, they have knowledge of a company's systems, applications and processes. However, the Internet and e-business are creating a new environment. Consider these facts:

- Companies are connecting to the Internet as quickly as possible. These connections occur with little planning and few controls, creating a whole new level of access from the outside.
- With the electronic connection of companies' businesses to their suppliers, customers and partners, the traditional boundaries are becoming blurred. A sub-contractor hired by one of the suppliers (without a background check and little management supervision) may now have access to, and knowledge of, some or all of a company's business applications and systems.
- Most companies no longer build their own proprietary business applications; instead, they purchase standard, off-the-shelf applications for things such as finance, customer relationship management and order management systems. This standardisation allows outsiders to use applications without detailed internal information.

These and other factors have altered the threats that companies now face. The distinction between an outsider and an insider is decreasing rapidly.

Online services are becoming prime targets for cyber criminals.

While statistics and experience show that the insider is still a significant threat, the outsider can no longer be ignored. Current security architectures are based on an organisation's ability to defend a perimeter, while network and application architectures have created information infrastructures without perimeters. In other words, current security architectures are inadequate to protect present information infrastructures**.**

GLOBAL CYBER TRENDS

Online services are becoming prime targets for cyber criminals. Cyber criminals continue to refine their means of deceit as well as their victims In general, the global threats affecting users today are: new and sophisticated forms of attacks, attacks targeting new technologies, such as VoIP (vishing – phishing via VoIP and phreaking, hacking telephone networks to make free long distance calls) and peer-to-peer services, attacks targeting online social networks, and attacks targeting online services, particularly online banking services. There is a new level of complexity in malware not seen before. These are more resilient, are modified over and over again and contain highly sophisticated functionality such as encryption (e.g. Nuwar[41] also known as 'Zhelatin' and 'Storm' worm' – with a new variant appearing almost daily). There is an increase in threats that hijack PCs with bots. Another challenging trend is the arrival of self-modifying threats. Broadly, there are three major emerging global trends of mischievous activities in cyber space, which have expanded from novice geeks to organised hi-tech criminal gangs:

- Growing threat to national security – web espionage becomes increasingly advanced, moving from curiosity to well-funded and well-organised operations aimed at not only financial, but also political or technical gains.
- Increasing threat to online services – affecting individuals and industry

[41] http://threatinfo.trendmicro.com/vinfo/secadvisories/default6.asp?vname=WAR+AGAINST+NUWAR: +FIGHTING+THE+LATEST+PROFIT-DRIVEN,+MULTI-COMPONENT,+FOCUSED+ATTACK

because of growth of sophistication of attack techniques.

- Emergence of a sophisticated market for software flaws – that can be used to carry out espionage and attacks on government and critical information infrastructure.

The North Atlantic Treaty Organisation (NATO) deployed a cyber defence management authority and a cooperative cyber centre of excellence in Estonia in May 2008 and has approached the Network-Centric Operations Industries Consortium (NCOIC) and BAE systems to help NATO in cyber space awareness and cyber defence issues.[42] The recent creation of the US Cyber Command (that will be fully operational in a year under a new post in the White House) is the outcome of the recognition of the cyber threat as one of "the most serious economic and national security challenges."[43] A glimpse of what is likely to follow in the future is given below:

- It is an inevitable reality that some countries will become safe havens for cyber criminals, and international pressure to crack down won't work well (e.g China's ghostnet[44]).
- In the next few years, governments are likely to get aggressive and pursue action against specific individuals/groups/companies, regardless of location.
- It is also likely that governments will start putting pressure on intermediary bodies that have the skills and resources, such as banks, Internet Service Providers (ISPs) and software vendors to protect the public from malware, hacking and social engineering.
- We may see industry sector codes of practice demanding improved security measures, backed probably by assurance and insurance schemes.

[42] Julian Hale "NATO to Shape Rapid Reaction Force", *Defence News*, July 6, 2009, p. 15.

[43] US President Barack Obama's speech on May 29, 2009, *Defence News*, July 6, 2009, p. 11.

[44] GhostNet (simplified Chinese: □□□; pinyin: YōuLíngWang) is the name given to a large-scale cyber spying [1][2[operation discovered in March 2009. It is based mainly in the People's Republic of China and has infiltrated high-value political, economic and media locations in 103 countries. Computer systems belonging to Embassies, Foreign Ministries and other government offices, and the Dalai Lama's Tibetan exile centres in India, London and New York City were compromised. Although the activity is mostly based in China, there is no conclusive evidence that the Chinese government is involved in its operation http://en.wikipedia.org/wiki/GhostNet, http://news.bbc.co.uk/1/hi/world/americas/7970471.stm. BBC News. March 29, 2009.

- Greater connectivity, and more embedded systems would mean less obvious perimeters of security in geographic terms.
- Compliance regulations will drive upgrades and changes and also increase system complexity and legal wrangles – increase in civil suits for security breaches is foreseen.
- Massive data storing patterns that ensure data never goes away (a boon to law enforcement agencies) will be the order of the day.

CHALLENGES TO NATIONAL SECURITY DYNAMICS

There are varieties of intruders such as individual, organised, criminal and espionage armed with different types of attack capabilities in the cyber space. Cyber space in military terms has its own centres of gravity depending upon the vulnerabilities upon which a successful attack would be decisive in a conflict situation. The concern of security policy-makers is to identify the possibilities/probabilities of criminal or espionage type of intruders attacking the innermost cyber centre of gravity.

The Internet has become a tool for political, military and economic espionage today. There has been an appreciable rise in organised cyber attacks in recent times, including the attacks on the US Pentagon in June 2007, Estonia in April 2007, computer systems of the German Chancellery and three Ministries, e-mail accounts at the National Informatics Centre of India, and highly classified government and computer networks in New Zealand and Australia. The software used to carry out these attacks indicates that they were clearly designed and tested with much greater resources than the usual individual hackers. Most government agencies and companies around the world use common computing technologies and systems that are frequently penetrated by criminal hackers and malware. Traditional protective measures are not enough to protect against attacks such as those on Estonia, as the complexity and coordination in using the botnets was totally new. National networks of countries like India with less sophistication in monitoring and defence capabilities could pose serious problems to national security.

Zero-day Threats[45] and Tools for Cyber Crime: With so many PCs now infected (around 5 per cent of all global machines are zombies), competition to supply botnets has become intense. The cost of renting a platform for spamming is now around US$ 3-7 per zombie per week. You can buy a Trojan that is built to steal credit card data and mail it you for as little as US$ 25 to 1,500. Malware is being custom written to target specific companies and agencies. Computer skills are no longer necessary to execute cyber crime. On the flip side, malware writers today need not commit the crimes themselves. People can subscribe to the tools that can keep them updated with the latest vulnerabilities and even test themselves against security solutions. The black market for stolen data (e.g. credit cards, e-mails, skype accounts, etc) is now well established and the cost of obtaining credit cards is upwards of US$ 5. Another black market that is causing alarm to governments is that of Zero-day exploits. In January 2006, a Microsoft WMF (Windows Meta File) exploit was sold for US$ 4,000.

The Internet has become a tool for political, military and economic espionage today.

Bot Networks and Cyber Arms Race: Bot networks are already generating attacks of overwhelming volume, in ways that are nearly impossible to stop or trace back to their origins. Bot networks are growing in number and power, to where they now pose a serious threat to governments, businesses and online consumers. According to Secure Computing, more than 250,000 personal computers are infected with bots each day, putting at least 10 million computers at the disposal of those with bad intentions. Bots are used by illegitimate businesses to generate billions of spam e-mails and to spread malware worldwide. Moreover, criminal organisations use bots for identity theft via phishing scams. Attacks like that in Estonia may be merely practice drills by crime factions to showcase their computing firepower and their ability to disrupt networks.

[45] A computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability, http://en.wikipedia.org/wiki/Zero_day_attack

Law enforcement and Internet infrastructure companies are cooperating to discover who is planting and orchestrating botnet attacks, but with limited success.

Law enforcement and Internet infrastructure companies are cooperating to discover who is planting and orchestrating botnet attacks, but with limited success. The Internet's very nature makes investigations difficult, especially after the fact. In what amounts to an arms race, operators of the Internet infrastructure are investing constantly to add capacity to handle the volumes of transactions generated by bot attacks. They are also adding teams of professionals and new systems to perform real-time network monitoring and rapid response. But there remains one aspect of the bot threat that cannot be addressed by centralised systems or government investigators—the end user. End users are a critical line of defence, in how they recognise and avoid deceptive tricks designed to download bots to their computers. User awareness is becoming even more critical as the Internet rapidly expands beyond the billion people online today, and reaches more than four billion people not yet online.

The Internet Corporation for Assigned Names and Numbers (ICANN), manager of the Internet domain name system, is implementing Internationalised Domain Names (IDNs) that will help the next billion Internet users enter web addresses entirely in their native language and character sets. If these new Internet users are not warned against downloading any patches or new applications unless they are dealing with a trusted website and scanning for viruses and malware, ICANN is inviting the "next billion" users to download the "next billion" bots capable of generating spam, phishing fraud, and the kind of denial-of-service attacks that brought down Estonia's Internet.[46]

Cyber Crime Review—India: Following its yearly assessment, CERT (Computer Emergency Response Team), the apex cyber security division under the Ministry of Information Technology of India, found that cyber crime in the country has accelerated about 50 times since 2004.[47] Highest growth

[46] Steve Del Bianco, Internet Caucus Advisory Committee, October 2007.

[47] Spam News Admin, Friday, April 18, 2008, http://spamnews.com/The-News/Latest-News/Cyber-Crime-Increases-50-Times-in-India-2008041811429/ Posted originally: 04/17/2008.

has occurred in computer related crimes that attack e-commerce businesses and financial service on the net. The agency recorded just 23 cyber crime incidents in 2004 in contrast to a huge 1,237 in 2007. These primarily included phishing attacks, distribution of viruses/malicious code and illegal infiltration to computer networks. Further, according to the CERT's annual report for 2007, there were 392 incidents of phishing, 358 cases of virus proliferation and 223 cases of network infiltration. Compared to this, there were only 3 phishing attacks, 5 cases of virus proliferation and 11 incidents of network infiltration reported in 2004. While spreading viruses comprise a familiar security issue, it is the large number of phishing attacks that India should be concerned about as these usually aim at middle-class consumers who bank or shop online.

CERT, which also tracks website defacement, found 5,863 Indian websites that underwent mutilation by global hackers in 2007.

CERT, which also tracks website defacement, found 5,863 Indian websites that underwent mutilation by global hackers in 2007. In addition, the agency also tracked 1,805 'open proxy' servers that allow anonymous browsing. It also detected more than 25,000 bot-infected computers. These statistics from CERT are, however, only indicative, without giving the actual picture of cyber crime in India, as the agency merely maintains records of cases that are notified to it. Furthermore, data of the government revealed that in January 2008, 87 security related incidents were recorded in contrast to 45 in December 2007. Of these, 47 per cent involved phishing, 25 per cent was related to worm/virus under the malware category, 21 per cent to unauthorised scanning, and 7 per cent to technical help under separate categories.

Implications for Security: Information security experts have traditionally studied threats on the scale of individual computers or organisational networks. While this is a valid practical approach, it does not reflect the reality of actual or potential threats. When computer misuse is evaluated from the view of the intruder, artificial boundaries such as organisational ownership or national borders are meaningless. A critical challenge to security experts, law enforcement and intelligence agencies is the ability to identify emerging new threats. This has been especially difficult in the arena of information security for several reasons:

- Law enforcement and information security experts for the most part do not use an intelligence-driven approach for prevention and control of computer crime. Investigations tend to be reactive and event-driven. While this has limited effectiveness for simple system intrusions, it will not be adequate for sophisticated or infrastructure attacks. Unless a more analysis-based process is employed, prevention will continue to lag behind the threat curve.
- The speed at which new technology is introduced creates a rapidly moving target for threat assessments. Each new technology requires high-level technical expertise to analyse. By the time vulnerabilities are identified, the technology has changed again.
- Key governmental and industry policy-makers lack the understanding of technology or the multi-dimensional aspects of information security. Many security professionals are biased toward a particular product such as intrusion detection systems or firewalls that limit the scope of proposed solutions.

Security Assurance and Role of CERT-In: CERT-In's primary function is to "alert, advice and provide assurance to ensure security of cyber space in the country" by enhancing the security of communications and information infrastructure through proactive action and effective collaboration aimed at security incident prevention, prediction, protection and security assurance.[48] Security assurance must be provided at every level of the security hierarchy, starting from the network level where the vulnerabilities of hardware and software and issues of access control are addressed. At the transmission level, the focus is on access control and data encryption, whereas at the operating system and application level, software loopholes and access issues need attention. The next higher level in the hierarchy of security assurance comprises the data level where privacy of data and its protection

[48] "Securing Indian Cyberspace: Issues and Challenges," http://www.cert-in.org.in

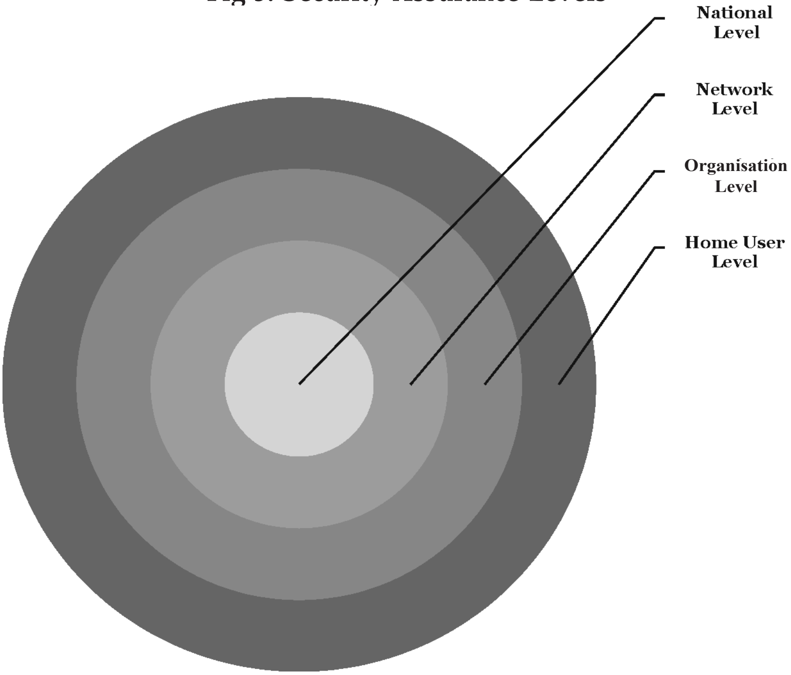
from unauthorised access/manipulation takes precedence, and at the people level, the focus has to be on training, and awareness about cyber security amongst users is crucial. At the organisation level, issues such as cyber security policy implementation and compliance, disaster recovery and legal compliance are important to achieve adequate security assurance.

Cyber Security Assurance Framework: At the national level, we need a strong cyber security assurance framework through which adequate confidence and trust can be built up in cyber power-driven infrastructures and systems. Though it is not possible to make the system 'intruder proof', we can devise a mechanism which can, to a large extent, anticipate potential problems, preempt through proactive measures, protect against considerable damage, and ensure recovery and restoration. This would enable the government, as a key stakeholder, to create the appropriate environment/ conditions by way of policies and legal/regulatory framework to address important aspects of data security and privacy protection concerns. Specific actions would include National Cyber Security policy, amendments to the Indian IT Act, security and privacy assurance framework, Crisis Management Plan (CMP), etc. This would also enable user agencies in government and critical sectors to improve the security posture of their IT systems and networks, and enhance their ability to resist cyber attacks and recover within a reasonable time if attacks do occur. Specific actions would include security standards/ guidelines, empanelment of IT security auditors, creating a network and database of points-of-contact and Chief Information Security Officers (CISOs) of the government and critical sector organisations for smooth and efficient communication to deal with security incidents and emergencies, CISO training programmes on security related topics and cyber security drills and security conformity assessment infrastructure covering products, processes and people.

At the national level, we need a strong cyber security assurance framework through which adequate confidence and trust can be built up in cyber power-driven infrastructures and systems.

Security Assurance Action Plan: With three clear strategic cyber security objectives i.e. to prevent cyber attacks against the country's critical information infrastructures, to reduce national vulnerability to cyber attacks, and to minimise damage and recovery time from cyber attacks, the security assurance action plan must be implemented at four different levels simultaneously (as depicted in Fig 3).

Fig 3: Security Assurance Levels



At the national level, security assurance can be provided through enactment and implementation of strong cyber laws (e.g. IT Act, 2000) that provide standard guidelines for compliance by all stakeholders in both the private and public sectors. There have to be strict provisions in the law for conformity assessment of IT infrastructure and security incident reporting. Presently, many organisations do not comply with these requirements in spite of existing standard guidelines. Traffic monitoring, routing and gateway controlling is increasingly becoming difficult in a country like India (unlike countries like China where the whole net traffic passes through state-owned information channels) due to multiplicity of service providers. Lawful interception and law enforcement require a proactive approach to avoid a situation where the law is always trying to catch up with the criminals. This would require sufficient and sustained investment of money and talent in the field of R&D on tools and technologies, products and services.

At the lower hierarchical levels (i.e. at the network level, organisation level, small business and home user level), security assurance is gaining more and more importance due to availability of newer malicious tools that target the end user. Compliance with best security practices (e.g ISO 27001) and service quality (e.g. ISO 2001) is essential to plug the gaps in cyber security. Further, illegal use of software is rampant in India and this results in vulnerabilities as most of such software is not updated at regular intervals.

CONCLUSION

If our government and other agencies concerned apply their focus and attention to providing ongoing modern IT security, then can the attackers be easily kept unemployed? The answer is, unfortunately, negative. As attackers are blocked from attacking one way, they will seek another. Attackers previously attacked networks and hosts until it became too difficult, so they switched their focus to attacking applications which were more vulnerable than hosts being blocked at the application level, and now attackers are preying on the end users directly. This can easily bypass most organisations' IT security protocols and processes. In the last few years, new attack patterns have emerged which take advantage of the fact that most individual users know nothing about IT security or their role in keeping things secure.

Our reliance on cyber space is only going to grow in the future. The network of networks spread over the wide spectrum of small and medium business, large enterprises, R&D centres, academia, defence Services, government organisations and national critical infrastructures is intensifying its grip with each passing day. This incremental dependence of the nation on cyber space must be managed with continuous efforts to secure the cyber systems that control our infrastructures. India as a big emerging economy is faced with a complex and evolving challenge more fiercely than the developed nations. Every day, so many new sectors are being networked covering social sectors oblivious of the security aspects of cyber space. This demands awareness and training on a continuous and large-scale basis. To achieve a three-pronged strategic objective of preventing cyber attacks against the country's critical information infrastructure, reducing national vulnerability to cyber attacks and minimising damage and recovery time from cyber attacks, we have to first have a robust system of detecting and assessing the threats and vulnerabilities in cyber space.

The vulnerability in the electronic space can be reduced. There are many products and strategies that can be deployed. There are many robust tools that log attacks and prevent them in real-time. These tools and strategies can provide security for a committed private or public organisation. As long as defence is treated as an ongoing process that is constantly updated and not as an end-state, the battle can be well waged. However, the enormity of the ensuing challenge demands a comprehensive national cyber security policy and strong funding on a continuous basis. Private-public partnership is the key to resolve the issues of talent, infrastructure and R&D facilities. The concept of weekend cyber warriors is worth implementing to outsource the specialised tasks to the large talent pool that exists in the private sector.

The ubiquitous nature of cyber space does not allow anyone to assume something as 'my cyber space' or 'your cyber space' so the need for national cyber security and international cyber security cooperation becomes the priority of our government. With the blurring boundaries between private and public information infrastructures, it requires a long-term effort on the part of both the private sector and the Government of India to use a variety of tools to implement this strategy. Adequate budget allocations are required to provide every department and agency involved in cyber security with resources to execute its responsibilities. In security matters, the past is no guarantee; the present is imperfect; and the future is uncertain. Failure is not when we fall down, but when we fail to get up.

NCW: THE DOUBLE-EDGED SWORD

SANJAY PODUVAL

What we are seeing, in moving from the Industrial Age to the Information Age, is what amounts to a new theory of war: power comes from a different place, it is used in different ways, it achieves different effects than it did before. During the Industrial Age, power came from mass. Now power tends to come from information, access, and speed. We have come to call that new theory of war network-centric warfare. It is not only about networks, but also about how wars are fought—how power is developed.

— Arthur K. Cebrowski

The conflicts of the 20th century are being replaced by hybrid wars and asymmetric contests in which there is no clear-cut distinction between soldiers and civilians and between organised violence, terror, crime and war.

— Alan Dupont

Warfare today is more complex than ever before. There is a blurring between peace and conflict, caused by the revolution in information technology. The revolution has enabled high speed dissemination of information over wide geographical areas almost simultaneously through dedicated networks. This was clearly seen in the conflicts in Kosovo and the Gulf, 2003, when the world woke up to the reality of Network-Centric Warfare (NCW) and the

* Wing Commander **Sanjay Poduval** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

multiplicative effects of information superiority that it provided. NCW, in some measure, has reduced the tyranny of distances, speeded up operations and has the potential to provide a seamless picture across the battlespace. However, this is by no means a silver bullet. It does have a flip side which was clearly brought out by the well coordinated 9/11 attack on the World Trade Centre. NCW has not truly met its match in the conventional sense; it is clearly dominated by the United States. This has led to wars of the present being more covert, with the adversaries leveraging the strengths of Information Technology (IT) against the proponents. As a result, most states today are perpetually at war; a war of a different nature, not against tangible elements but against bits and bytes. This information war is split between the offensive and the defensive. The advantage more often than not lies with the attacker who can choose the time and place of the attack. The blurring of offence and defence reflects another feature of the dual nature of NCW; it tends to defy and cut across standard boundaries, jurisdictions, and distinctions between state and society, public and private, war and peace, war and crime, civilian and military, police and military, and legal and illegal. This makes it difficult, if not impossible, for a government to assign responsibility to any single agency—e.g., military, police, or intelligence—to be in charge of responding. The wars over the net or netwars refer to an emerging mode of conflict and crime at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organisation and related doctrines, strategies, and technologies attuned to the information age. These protagonists are likely to consist of dispersed small groups who communicate, coordinate, and conduct their campaigns in an 'inter-netted' manner, without a precise central command. Thus, information age netwar differs from the traditional modes of conflict and crime in which the protagonists prefer formal, stand-alone, hierarchical organisations, doctrines, and strategies.[1] Conflicts of the present century are being replaced by hybrid wars and asymmetric conflicts in which there is no clear-cut distinction between soldiers and civilians and between organised

[1] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (RAND, 2001).

violence, terror, crime and war. In view of the above, the aim of this paper is to discuss the merits and demerits of NCW.

THE DUAL NATURE

In the military in the past 20 years, many astounding technological advancements in radars, directed energy, communication, space exploitation, miniaturisation, data processing, etc have taken place, which have not only influenced every aspect of our lives but have also altered the means of waging wars. Warfare can now be more efficient and effective. The integration of all these factors has essentially led to Network-Centric Warfare (NCW). Networking is a mechanism which improves operational tempo by accelerating the Observation-Orientation phases of Boyd's Observation-Orientation-Decision-Action (OODA) loop. The audacious second attempt on April 7, 2003, to decapitate the Iraqi leadership amply demonstrates this. The strike was especially noteworthy for the way it saw information on the whereabouts of the Iraqi dictator, which emerged at very short notice, transmitted rapidly to Allied air planners and then to the B-1B bomber aircraft. It took just 12 minutes for the crew to disengage from a previously assigned task and release their weapons on the new target.[2] The Iraqi leadership, however, escaped the attack, which implies that they too got wind of the impending attack equally fast.

The increasing dependence of societies and military forces on advanced information networks creates new vulnerabilities through means such as computer network attacks and directed energy weapons. The inherent implication here is that the universal nature of networked systems is in itself one of the key vulnerabilities. Provision of digital wireless connectivity between combat platforms is a major technical challenge which cannot be understated. While civilian networking of computers can largely rely on cabled links, be they copper or optical fibres, with wireless connectivity as an adjunct, in a military environment centred on moving platforms and field deployed bases, wireless connectivity is the central means of carrying

[2] "What Went Right?," *Jane's Defence Weekly*, April 30, 2003, http://www.oft.osd.mil/library/library_files/article_63_Jane.doc.

The fact that military networks and civilian networks are intertwined provides another set of vulnerabilities which must be addressed.

information and the area most vulnerable to interference.

Therefore, it is not surprising that anti-establishment forces, weaker forces and non-state actors have taken to the digital revolution with alarming alacrity. The low cost of entry (for example, a laptop connected to the Internet) and the ability to operate anonymously are factors responsible for asymmetrical operations from potential adversaries. A communication channel that broadcasts relevant and authentic data can also transmit irrelevant and false data. Network-centric deception supports any operation which has objectives that are a function of communication networks, irrespective of whether these are adversarial or friendly. In other words, if an adversary relies on communication networks to obtain, process, and analyse the Common Operational Picture (COP), the same can also be skewed or altered.

The fact that military networks and civilian networks are intertwined provides another set of vulnerabilities which must be addressed, for example, during Operation Iraqi Freedom, US and Coalition forces reportedly did not execute any computer network attacks against Iraqi systems, even though comprehensive Information Operations (IO) plans were prepared in advance. It is widely speculated that the IO plans against the Iraqi financial services were rejected because Iraq's banking network is connected to the financial communications network also located in Europe. Consequently, according to Pentagon sources, an information operations attack directed at Iraq might also have brought down banks and ATM machines located in parts of Europe.[3] This vulnerability has tremendous ramifications for the mischievous intents of anyone who wishes to take advantage of the situation.

The present information revolution is posing new security problems that could prove more severe for open societies than for closed ones. As we

[3] Charles Smith, "US Information Warriors Wrestle with New Weapons," NewsMax.com, March 13, 2003, http://www.newsmax.com/archives/articles/2003/3/12/134712.shtml .

become economically stronger, our dependence on other countries and on connectivity and computation would only increase and we could become more vulnerable to information warfare. Integration in the world economy, with its criss-crossing networks, enlarges the risk. The prospect of a disruption of the national economy due to attacks on the domestic information infrastructure could tilt the ambivalence of a nation in a distinctly negative direction, thus, emboldening a militarily inferior enemy.

As we become economically stronger, our dependence on other countries and on connectivity and computation would only increase and we could become more vulnerable to information warfare.

Greater dependence on information technology in military systems could imply greater susceptibility to information warfare during operations. The Revolution in Military Affairs (RMA) places a bull's eye on the Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR) that is critical to it. In the extreme, the ability to project power and to strike at will, would be undermined if an otherwise weaker enemy interfered with the links that network forces, fuse sensor data, and permit joint warfare. Even if the military establishment secures its own dedicated links and nodes, effective information warfare attacks on public telecommunications network, on which nearly all routine military traffic flows, could create havoc in a crisis and cripple a campaign.

THE PROS: THE 'RIGHT' EDGE OF THE SWORD

Operation Enduring Freedom (2001–02)

The network-centric capabilities of the US Central Command (US CENTCOM) elements during the conduct of Operation Enduring Freedom in Afghanistan proved vital in the battle against the Taliban and Al Qaeda forces. The operations were conducted in the mountainous, landlocked country which presented an extremely challenging environment. The long sought goal of networking weapons and sensor platforms came to fruition in the austere environment where both the needs and the advantages of NCW were readily apparent.

The Special Operations Forces (SOF) on the ground were networked with aircraft capable of delivering Precision Guided Munitions (PGMs). This combination proved extremely effective. However, networking the sensors and the shooters in real-time was only part of the requirement. Taliban and Al Qaeda targets during Operation Enduring Freedom were often fleeting, and weapons platforms had to be updated very quickly while in the air. The B-2 bombers (flying from bases in Missouri), and B-1 bombers (flying from other bases far from the theatre of operations), required the capability to change mission tasking en route to the target areas in Afghanistan. Carrier-based aircraft needed a similar capability to deal with the dynamic nature of their targets. Unmanned Aerial Vehicles (UAVs) were successfully used for this purpose to a greater degree than ever before. The ability to pass information gathered by Predator and Global Hawk UAVs to ground commanders in Afghanistan enabled near-real-time battlefield situational awareness. Satellite communications and related technologies enabled this networking capability to a degree not previously achievable.

Operation Iraqi Freedom (2003)

The impressive network-centric capabilities of US forces were clearly evident during the conduct of Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF). Many significant improvements in these capabilities were apparent by the time OIF began in March 2003. Network-centric capabilities provided, without question, a major contribution to the decisive victory of Coalition forces in Iraq.

Network-centric capabilities evident in US forces during OIF included not only technology and systems that enabled effective conduct of Network-Centric Operations (NCO), but innovative new concepts for the employment of technology and an enhanced understanding of the human side of the NCW equation as well—highly trained, motivated soldiers, sailors, airmen, and marines fighting as part of an integrated, networked joint force. Most of the groundwork for the information network and other network-centric capabilities that empowered the forces during OIF was actually completed during OEF. Technology enabled the rapid sharing of information at all levels with a capability to move intelligence rapidly from the sensor to either the decision-maker or directly to the shooter. The communications, C2, and ISR systems were hooked up to, and interoperable with, the Global Information Grid (GIG), and were adaptable to circumstances on the battlefield.[4]

Modern technology and new operational concepts enable networked units and individual platforms to operate together in ways not possible just a few years ago.

Therefore, as is evident, modern technology and new operational concepts enable networked units and individual platforms to operate together in ways not possible just a few years ago. NCW is characterised by the ability of geographically dispersed forces to attain a high level of shared battlespace awareness that is exploited to achieve strategic, operational, and tactical objectives in accordance with the aim. This linking of people, platforms, weapons, sensors, and decision-aids into a single network creates a whole that is clearly greater than the sum of its parts. The results are networked forces that operate with increased speed and synchronisation and are capable of achieving massed effects, in many situations, without the physical massing of forces required in the past. This increased speed and synchronisation directly impacts operations across the battlespace, from support areas through combat zones. NCW enhances the ability of a force to combine into a seamless, joint, coalition war-fighting force. As information moves down to the lower echelons, so does decision-making. Thus, smaller joint force packages can possess more flexibility and agility and are able to wield greater combat power than before. NCW generates new and extraordinary levels of operational effectiveness. It enables and

[4] "The Implementation of Network-Centric Warfare," http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf

leverages new military capabilities while allowing the use of traditional capabilities with more speed and precision.

CONS: THE OTHER EDGE

After the 34-day War with Israel in 2006, Hezbollah was described by some Israeli officials as a well-equipped, networked force still capable of commanding its combat units after weeks of high-intensity fighting. Hezbollah's units were supported by a well-fortified terrestrial communications network supplemented by satellite telephone and broadcast services which included the Al-Manar television network. Hezbollah units also reportedly had the capability to attempt eavesdropping on Israeli cellular networks.[5] Hezbollah guerrillas were able to hack into Israeli radio communications during the conflict, an intelligence breakthrough that helped them thwart Israeli tank assaults. This gave the guerrillas a picture of Israeli movements, casualty reports and supply routes. It also allowed Hezbollah anti-tank units to effectively target advancing Israeli amour.[6] The same networks which were providing information advantage to the Israelis, aided their adversaries.

Hamas was also reportedly inspired by the way Hezbollah fought against Israel in Lebanon. The organisation is continuing to receive increasing support from Hezbollah in the form of weapons, funding, and training. Hezbollah is also reportedly sharing with Hamas operatives many of the lessons they learned from the recent military engagement with Israel.[7] Cells of people that are under central direction, allow the organisation to be highly flexible, elusive and adaptable.

Al Qaeda too is evolving and coming to terms with the newer commercially available communication systems. Their dispersed cells may become more coordinated and self-organising, with increased situational awareness, and the possible future capability of conducting their own network operations in

[5] Barbara Opall-Rome, "Combating the Hezbollah Network," *Defense News*, October 9, 2006, p. 6.

[6] Noah Shachtman, "Hez Hacked Israeli Radios", http://www.noahshachtman.com/archives/002785.html

[7] Alon Ben-David, "Hamas Boosts its Weapons Stocks," *Jane's Defence Weekly*, October 25,2006.

ways similar to the network operations of current military units.[8] Al Qaeda is transforming itself into a virtual organisation, while creating new links to local franchisees. It is these new local groups that are now carrying out terrorist attacks, rather than Al Qaeda itself, and these smaller, local groups are more difficult for the military to anticipate, locate, and engage.[9]

Cyber terrorism is the biggest threat that India is likely to face because the network infrastructure of the country is vulnerable and may be attacked any time.

Another serious concern comprises the reports which state that Pakistani cyber criminals deface nearly 40-50 Indian websites every day. Nasscom surveys have pointed out that information security threats have created an unprecedented demand for qualified and experienced information security professionals but India is yet to comprehend this crucial issue.[10] Studies suggest that the slipshod attitudes of both the corporate sector and the government regarding cyber security impede any positive approach. Cyber terrorism is the biggest threat that India is likely to face because the network infrastructure of the country is vulnerable and may be attacked any time.[11] Asymmetric warfare, Counter-Insurgency (CI) or Counter-Terrorism (CT) operations, rather than conventional warfare, is the order of the day across the globe. An adversary will seek to wage asymmetric war and cripple the economic and energy infrastructure rather than engage military targets. Alternately, the adversary will launch cyber attacks to cripple the banking, railway or power grid systems. Today, the terrorist threat is real. Each terrorist network is part of a complex network of autonomous terrorist groups, thus, forming an international terrorist Internet. In India, there exists

[8] David Compert, "Battle-Wise: Gaining Advantage in Networked Warfare", Center for Technology and National Security Policy, National Defense University, January 2005, p. 15.

[9] "Business Lessons from Terrorists", World Economic Forum, January 21-25, 2004, [http://members.weforum.org/pdf/Session_Summaries2004/084e.pdf

[10] Amit Sinha, "Pakistani Hacking Onslaughts Makes India a Hapless Prey", http://www.littleabout.com/news/45008,pakistani-hacking-onslaught-india-hapless-prey.html

[11] "Cyber Terrorism Next Big Threat to India: Cyber Security Whizkid", http://www.thaindian.com/newsportal/sci-tech/cyber-terrorism-next-big-threat-to-india-cyber-security-whizkid-with-images_100279193.html, November 24, 2009

a nexus of terrorist and insurgent organisations which operate in Jammu and Kashmir, the northeast and the hinterland areas of Madhya Pradesh, Bihar, Andhra Pradesh, Chhattisgarh and Jharkhand which make extensive use of the Internet. These organisations have cyber savvy terrorists who use the worldwide web, e-mail and electronic bulletin boards and are involved in hacking of sensitive national websites.[12]

Many contemporary military theorists identify the greatest value of the digital revolution as being coordination, speed and precision, in the context of destroying an opponent's forces. In the modern day economy, the same speed and precision characteristic of a well implemented digital system means that many processes can be greatly accelerated and hitherto unseen levels of coordination between multiple players achieved. This is true of finance, stock markets, manufacturing, research and development. Therefore, those economic players who master the digital environment can potentially acquire a huge competitive advantage over those who do not. Therefore, the anti-establishment forces, weaker forces or the non-state actors have taken to digitisation with alarming speed. The ease of entry is a major factor responsible for asymmetrical operations from potential adversaries.

Another example of the double-edged nature of NCW is the use of the Global Positioning System (GPS) which is considered to be the enabler of NCW. The use of GPS guided munitions provided an asymmetric advantage to the Allied forces. They were able to precisely hit most of their targets at all times in all kinds of weather. Most of the expensive, cruise-type missiles in the US inventory such as the Tomahawk Conventional Air-Launched Cruise Missile (CALCM) and some land-attack versions of the Harpoon missile employ GPS for navigation purposes. The problem is that of GPS exploitation. Even during the Gulf War, it was reported that the Iraqis used commercial GPS equipment to assist in calibrating Scud launch sites. The real problem will come about when countries start dusting off their 50s and 60s technology cruise missiles and retrofit them with commercial GPS autopilots. Most of these weapons used combinations of inertial autopilot,

[12] Ibid.

radio command link and anti-ship radar homing guidance to attack either shipping or area land targets. In the latter instance, they were never taken seriously due their poor accuracy. However with GPS accuracies, they become very effective standoff weapons, a problem which could be extrapolated into the Indian context once the Indian Regional Navigation Satellite System (IRNSS) becomes operational. The September 11, 2001 terrorist attack on the US took a new turn on the destructive usage of GPS. Reports say that the US Federal Bureau of Investigation (FBI) is suspecting terrorists' use of GPS as their lethal weapon to precisely locate the ill-fated sites.[13] It is suspected that at least three of the 19 terrorists could have purchased a GPS device that year.[14]

The 9/11 planners and hijackers exploited the Internet to achieve their goals. Senior Al Qaeda coordinators involved in the suicide hijacking plot, such as notorious Al Qaeda training camp manager, Abu Zubaydah, exchanged thousands of encrypted messages, posting their operational plans on a password protected section of a website.[15] The extensive use of the Internet by the 9/11 hijackers and planners of attacks elsewhere illustrates how the Internet serves as a logistical tool for terrorist operatives.

Terrorist webmasters and militant extremists from dozens of countries are exploiting the anonymous, inexpensive, and easily accessible global reach of the Internet. Extremists are using the Internet media to recruit potential terrorist operatives, solicit funding for operations, train current terrorists with the latest in bomb-making knowhow, and plan operations against civilian targets worldwide. The success Al Qaeda and affiliated movements have had in exploiting the Internet as an operational centre illustrates that the Al Qaeda guerrilla movement has migrated from physical space to cyber space. With laptops, communication systems and the like,

[13] Arik Hesseldahl, "After The Attacks, New Attention on GPS", Forbes.com, October 2, 2001. http://www.forbes.com/technology/2001/10/02/1002gps.html

[14] Sue Kwon, "GPS Technology Could Help Taliban Fight U.S", KPIX Channel 5, U.S http://beta.kpix.com/news/local/2001/10/23/GPS_Technology_Could_Help_Taliban_Fight_U.S..html

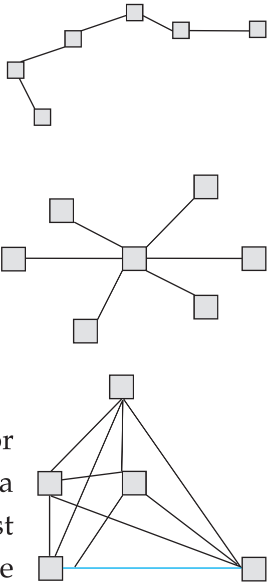
[15] "Anti-Defamation League, Jihad Online: Islamic Terrorists and the Internet" 9 (2002), http://www.adl.org/learn/internet/jihad_online.pdf

jihadists have sought to replicate the training, communication, planning, and preaching facilities they lost in Afghanistan with countless new locations on the Internet.[16]

THE FABRIC OF NETWORKS

The networks of these groups need to be analysed for a better appreciation of their operations and organisation. According to John Arquilla and David Ronfeldt, the network fabric is of three types; chain, hub and meshed.

- **The chain network** is typified by smuggling networks, where end-to-end exchanges (information, contraband, etc.) must travel back and forth between intermediary nodes. This is also a feature of a hierarchical network.
- **The hub, star or wheel network** as in a franchise or a cartel where a set of disparate actors is tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.
- **The all-channel full-matrix or meshed network** is a collaborative network where every individual actor is able to communicate fully with all other nodes in the network.



Each node/point in the diagram can refer to an individual, a group or an organisation or even a state. The nodes maybe loosely or tightly coupled to the central agency. The loosely coupled ones take orders from the central agency and after that they are largely on their own. These loosely coupled ones, once let loose, will be difficult to recall. They may revert to the centre only in extreme cases. The tightly coupled ones are more integrated with the central agency and a greater control can be exercised over them.

[16] Steve Coll & Susan B. Glasser, "Terrorists Turn to the Web as Base of Operations", http://commlaw.cua.edu/articles/v15/Davis.pdf

Each type may be suited to different conditions and purposes, and all three may be found among netwar related adversaries e.g., the chain in smuggling operations; the hub at the core of terrorist and criminal syndicates; and the all-channel type among militant groups that are highly internetted and decentralised. There may also be hybrids of the three types, with different tasks being organised around different types of networks. For example, a netwar actor may have an all-channel council or directorate at its core but use hubs and chains for tactical operations.

There may also be hybrids of network and hierarchical forms of organisation. For example, traditional hierarchies may exist inside particular nodes in a network. Some actors may have a hierarchical organisation overall but use network designs for tactical operations; other actors may have an all-channel network design overall but use hierarchical teams for tactical operations. Again, many configurations are possible, and it may be difficult for an analyst to discern exactly which type characterises a particular network.

The all-channel model is becoming increasingly significant as a source of organisational collaborative power. The all-channel network has no central leadership and no key node whose removal might disrupt the entire organisation. Instead, the network is completely decentralised, allowing for initiative and autonomy at lower levels in the organisation which may at times appear to be operating without anyone in charge, and at other times, multi-headed. The all-channel network is one of the most difficult to maintain because it requires a strong communications capacity to maintain ties between nodes. Moreover, nodal autonomy results in a distributed, consensus style of decision-making which is necessarily dependent on back-and-forth communication. As such, this form of organisation has only recently become feasible on a greater scale with the dawn of the information age.[17]

APPRECIATING THE PROBLEM

Infowar is inevitably, as any survival contest is, split between the offensive and the defensive. The advantage more than not often lies with the

[17] Arquilla and Ronfeldt, n. 1.

initiator, who is like a needle in a haystack, making things difficult for the defender.

In a conflict, many nations today are more willing to drop a laser guided bomb through an opponent's window than penetrate his computer system. This is because they and the public at large have failed to grasp the fact that cracking into an adversary's computer, or putting a hacksaw through a fibre cable, is acting no differently than if they were shooting off a ballistic missile or lobbing a satchel of charge into a munitions depot. It is an act of war, but not appreciated in that sense.

A government which sponsors crackers to bust into another country's computing infrastructure is performing at a minimum the equivalent to a special operations commando penetration of its opponent's military basing or government buildings. This is equivalent to a large scale bombing raid or special commando operation and should evoke an equivalent response; but it does not. The underlying cause for this clearly irrational posture is that the gravity of the act is undervalued, and it is, therefore, dismissed as being of substantially lower importance than it really is. Until such an attack produces a truly dramatic, Pearl Harbour category disaster, it is unlikely that the message will get across.

This issue is further complicated by the boundaries between military and civil operations. Whereas legislation may eventually allow a nation's armed forces to respond in kind, or respond preemptively to an information attack, with a like information attack, or conventional counter-strike, civilian agencies and commercial players are unlikely to be afforded such latitude. For instance, a security guard at a bank may open gunfire on an armed intruder trying to force his entry into a bank; however, a bank's system programmer launching a denial of service against a criminal attempting to break into the bank's internal network is, at this time, legally problematic. More than likely, it would result in the criminal's Internet Service Provider (ISP) successfully suing the bank in question. The issue of legislation is indeed a thorny one, and one which will take some time to sort out. If conventional, precedent-based legal practices are to apply, many of these issues will have to wait for test cases to produce rulings. In the meantime, a good measure of paralysis will exist.

Rules of Engagement

The legal issues are closely related to the issue of Rules of Engagement (RoE), the fundamental constraints and protocols which are applied to any military operation. These have been in existence since the epic periods of the *Ramayana* and *Mahabharata.* In conventional wars, such as those fought in the Persian Gulf in 1991, or over Serbia in 1999, the conflicts were waged under some frequently complicated and often very restrictive RoE. In conventional wars, the RoE are very carefully crafted to reflect political and operational constraints. What can and cannot be attacked, and under which conditions it can be attacked, is carefully (or not so carefully in some instances) defined and set down as inviolate constraints to military personnel. The purpose is primarily to set boundaries for military operations, either in terms of geography or types of targets to be engaged. A typical RoE package today includes constraints from the Law of Armed Conflict (LOAC), which are mostly aimed at preventing the loss of innocent civilian lives, or the destruction of significant historical or cultural artefacts. While much debate continues as to the merits of many RoE packages and philosophies, it is a fact that responsible states would go to war with some kind of RoE. Defining a meaningful RoE package for infowar is not an easy task, and is yet to be properly resolved. History is witness that RoE has been violated in the past by the belligerents and heavyweights and will also be in the future. In this scenario of networked operations, establishing the RoE is very important because of the diffused and seamless nature of networks, and should be construed as guidelines.

In this scenario of networked operations, establishing the RoE is very important because of the diffused and seamless nature of networks, and should be construed as guidelines.

Consider the scenario in which an opponent's electricity grid or communications network is taken down. Both are target sets which evoke much argument in conventional targeting, since it can be argued that denial of both services can indirectly cause civilian casualties, and impose unreasonable hardship upon the population. Taking down an opponent's finance infrastructure or stock market, plunging it into an economic collapse, could produce similar effects. Will this constitute a violation of established protocols designed to protect civilians from unreasonable hardship? Wrecking of a nation's economy via a systematic information attack on its finance infrastructure could produce wider repercussions by damaging countries with mutual economic dependencies with the target nation. These are not very different from physically wrecking its economy by large scale air raids. All these are interesting questions which need to be understood and properly addressed.

The other side of this coin is dealing with players who choose not to observe any RoE. For example, a clash with non-state actors or terrorist organisations or tin-pot dictators, with scant respect for international conventions, has been a source of concern. Players who fall into this category are unlikely to restrict their offensive information operations to target sets deemed legitimate under international law. Parking a surface-to-air missile launcher in the grounds of a hospital, or putting a civilian air raid shelter into the same facility as a military command post are both good examples of such behaviour.

Boundary Spanning Criminal Organisations

Boundary spanning/trans-national criminal organisations are empowered by the Information Technology (IT) form in the sense that it heightens their mobility, adaptability, and their ability to operate trans-nationally. These trans-national networks pose a problem for states operating in a conventional, inwardly focussed manner. For instance, drug cartels around the world draw power from their extended trans-national network resources, making it difficult for the governments to fight the cartels within the confines of their national boundaries. Thus, networking allows these organisations to easily operate across jurisdictions, evading national law enforcement agencies. Networks also make it more difficult to dismantle a criminal operation, given that there is less emphasis on a rigid, central leadership.

Media and Perception Management

The acquisition by terrorist groups of an offensive IO capability could represent a significant threat as the world becomes more dependent on information and communications flows. In addition to enabling networked forms of organisation, IT can also improve terrorist intelligence collection and analysis, as well as offensive information operations. The goals and motivation of terrorists vary widely from the fulfilment of some divinely inspired objective to issue-specific causes like education for girls. Despite these vast differences, all terrorist groups have one trait in common: they do not commit actions randomly or senselessly. Each wants maximum publicity to be generated by its actions. They seek to impress. They use the modern media as the principal conduit and, thus, the media 'unwittingly' form a vital part in the terrorists' calculus. Without media coverage, the impact of the act is wasted and could remain narrowly confined to its immediate vicinity.

Despite these vast differences, all terrorist groups have one trait in common: they do not commit actions randomly or senselessly.

The first group to successfully harness the power of the Internet was the Zapatista National Liberation Army (EZLN) or simply Zapatistas, an insurgent group. The Zapatista movement began as a seemingly traditional, hierarchical insurgency, but has transformed into an information-age conflict following setbacks in battles. The guerrillas switched tactics and began to exploit the network form, taking advantage of the Non-Governmental Organisations (NGOs) connections to mobilise global awareness and support for their reform movement, while putting pressure on the Mexican government. The Internet, which was in its infancy at the time, also became a key space for networking various groups from around the globe with the Zapatista movement. It made communication with the rest of Mexico and the world a high priority. The EZLN used technology, including cellular phones and the Internet, to generate international solidarity with sympathetic people and organisations. Its effective exploitation of the Internet in the beginning of the 1990s was subsequently emulated by other insurgent movements.

Getting a message out and receiving extensive news media exposure are important components of the terrorist strategy, which ultimately seeks to undermine the will of an opponent.

Terrorist groups seem to be adopting flexible, decentralised network structures as part of a shift away from formally organised, state-sponsored groups to privately financed, loose networks of individuals and sub-groups that may have strategic guidance but that, nonetheless, enjoy tactical independence. Past terrorist groups did incorporate autonomous cells, but they were largely coordinated in a non-networked manner. Newer terrorist movements such as Hamas, Hezbollah and Al Qaeda all employ less hierarchical, loosely interlinked organisational models. Rather than the rigid bureaucratic structures and nationalist agendas of the old terror groups, these new operatives are networked, relying on decentralised decision-making, with flexible ties between other individuals and radical groups sharing common values.

Given the importance of knowledge and soft power, it is not surprising that networked terrorists have also begun to leverage IT for perception management and propaganda to influence public opinion, recruit new members, and generate funding. Getting a message out and receiving extensive news media exposure are important components of the terrorist strategy, which ultimately seeks to undermine the will of an opponent. In addition to such traditional media as television or print, the Internet now offers terrorist groups an alternative way to reach out to the public, often with much more direct control over their message. The news media play an integral part in a terrorist act because they are the conduit for news of the violence to the general population. The 26/11 attack on Mumbai highlights this. As Bruce Hoffman has noted,

> Terrorism . . . may be seen as a violent act that is conceived specifically to attract attention and then, through the publicity it generates, to communicate a message.

Terrorists have improved their media management; in fact, some groups have even acquired their own television and radio stations to take direct control of the reporting of events. Hezbollah, through its television station, has broadcast footage of strikes carried out by its operatives and has a sophisticated media centre that regularly—and professionally—briefs foreign journalists. Hezbollah field units have even included specially designated cameramen to record dramatic video footage of Israeli casualties which are then aired in Lebanon and usually rebroadcast by Israeli television.

The Internet now expands the opportunities for publicity and exposure beyond the traditional limits of television and print media.

The Internet now expands the opportunities for publicity and exposure beyond the traditional limits of television and print media. Before the Internet, a bombing may have been accompanied by a phone call or fax to the Press by a terrorist group claiming responsibility. Now, bombings can be followed—should the terrorists so desire—by an immediate Press release from their own websites (at little cost).

Disruptive Attacks

If the ultimate goal of a terrorist is to influence his opponent's will to fight, IO offers additional means to exert influence beyond using simple physical attacks to cause terror. Netwar-oriented terrorists can also use IT to launch disruptive attacks—that is, electronic strikes that temporarily disable, but do not destroy, physical and/or virtual infrastructure. Disruptive attacks include "choking" computer systems through such tools as e-bombs[18], fax spamming, and hacking techniques to deface websites. These strikes are usually non-lethal in nature, although they can wreak havoc and cause significant economic damage. To date, disruptive strikes by terrorists have been relatively few and fairly unsophisticated—but they do seem to be increasing in frequency. For example, in 1996, the Liberation Tigers of Tamil Eelam (LTTE) launched an e-mail bomb attack against Sri Lankan

[18] An e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Today's Mujahideen have launched a cyber *jihad*, signalling that terrorists are also armed with a technical and strategic mastery of the Internet.

diplomatic missions. Using automated tools, the guerrilla organisation flooded Sri Lankan embassies with thousands of messages, thus, establishing a "virtual blockade." In 2000, a group of Pakistani hackers who call themselves the Muslim Online Syndicate (MOS) defaced more than 500 websites in India to protest the conflict in Kashmir. Pakistan's Lashkar-e-Tayyeba too claimed to have attacked Indian military websites in early 2000. E-attacks on Estonia[19] which shut down most of the country in May 2007, comprise another example of the same.

Disruptive rather than destructive actions take place for several reasons. Terrorists who rely on the Internet for perception management and communication purposes, may prefer not to take "the net" down, but rather to slow it down selectively. In addition, groups may want to rely on non-lethal cyber strikes to pressure governments without alienating their own constituent audiences. Terrorist groups may also follow the lead of criminal hackers and use the threat of disruptive attacks to blackmail and extort funds from private sector entities. In the early 1990s, hackers and criminals blackmailed brokerage houses and banks for several million British pounds. Money can also be stolen from individual users who visit terrorist websites.

Today's Mujahideen have launched a cyber *jihad*[20], signalling that terrorists are also armed with a technical and strategic mastery of the Internet. This knowledge enables terrorists to indoctrinate, recruit, and train new members for attacks, with little or no threat of discovery or capture. Al Qaeda and other terrorist groups are effectively using the Internet and an estimated 4,500 terrorist-related websites to advertise a global brand of terror to millions of sympathetic Web users.[21]

[19] "Estonia Hit by 'Moscow Cyber War", http://news.bbc.co.uk/2/hi/europe/6665145.stmm.

[20] Cyber *jihad* is a term coined to loosely describe (Islamic) extremist terrorists' use of the Internet as a communications, fund raising, recruitment, training, and planning tool in their battle against the enemy.

[21] Benjamin R. Davis, "Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for CyberGovernance", http://commlaw.cua.edu/articles/v15/Davis.pdf

MANAGING/MITIGATING THE PROBLEM

As far as security is concerned, there is no best firewall. The continuum lies between the two extremes: absolute security and absolute access. The closest to absolute security would be a machine unplugged from the network; power supply removed, locked in a safe, and placed at the bottom of the ocean. At the other extreme is a machine with absolute access which is extremely convenient to use: it's simply there, without questions, no authorisation and no passwords. Unfortunately, both are of no use. Every organisation needs to decide for itself where, between the two extremes of total security and total access, it needs to be. A policy needs to articulate this, and then define *how* that will be enforced.

Entities with vested interests are well on their way to acquire IT-based technologies and skills. It is, therefore, conceivable that the current groups will adopt more-offensive IT strategies in the future. New hacker/terrorist groups may also emerge to compound this problem. Some terrorist networks may have even become sophisticated enough to sustain and coordinate offensive campaigns in both the virtual and physical realms. We, therefore, need to be aware of, and develop, a policy to counter the dangers associated with exploitation of IT by elements with nefarious agenda.

The policies and tactics should be able to impede the speed with which the groups become "informationised" because groups facing a robust counter-terrorism campaign will have less time and resources to acquire new technologies.

- The first is to monitor changes in the use of IT by target groups, differentiating between organisational and offensive capabilities. The type of IT capabilities developed by each group, targeting its specific technological vulnerabilities, should be taken into account. Monitoring the shift in capabilities for each type of IT use and then examining trends in the aggregate can also help forecast future behaviour. Among the most significant trends to be carefully examined is the possible emergence of a new, and potentially dangerous, breed of terrorists—groups that are highly "informationised" along both the organisational and offensive axes. Evaluating how IT shapes their organisational processes and offensive activities will remain a critical component of the threat assessment. In this regard, a number of "signposts" should be identified and tracked. These could include monitoring the level of technical expertise of known leaders and their subordinates, frequency of disruptive attacks, type of IT equipment owned, and nature of relatively secure off-the-shelf information technologies purchased over a period of time.

- The second is to target the information flow. Since network designs are inherently information intensive, efforts should target the information flows of identified groups. Intercepting and monitoring information exchanges should remain a top priority. The agency responsible for national security in our country should develop and design systems to decode encryption software, tap cellular transmissions, etc. This, besides being a useful addition to signals intelligence, should be leveraged beyond passive monitoring to active disruption of such communications or planting misleading information. This could breed mistrust and compromise the integrity and relevance of the network itself, eliminating their key competitive advantage.
- The third step should be to deter IT-based offensive IO through better infrastructure protection. Changing/plugging the vulnerability of critical infrastructures can significantly alter a terrorist's IT calculus. If infrastructures, such as those that manage air traffic control were to become relatively more vulnerable, they would become more attractive as targets. They could be struck from a distance, generating as much—if not more—destruction as would have been caused by the use of traditional weapons. We should identify specific vulnerabilities to expected threats and develop security techniques that mitigate each. Counter-terrorist agencies may also want to consider the option of employing a large number of ethical hackers and leveraging their knowledge for defensive and possibly even retaliatory purposes.
- Fourth, to counter the wars over the net, we will need to adopt organisational designs and strategies like those of the adversaries. This

does not mean mirroring them but rather learning to draw on the same design principles of network forms. These principles depend to some extent upon technological innovation, on a willingness to innovate organisationally and doctrinally, and on building new mechanisms for inter-agency and multi-jurisdictional cooperation—essentially beating them at their own game.

The information revolution has ensured that conflicts will increasingly depend on information and communications matters.

Some Safe Practices: Looking at the types of attacks that are common, there are a few practices that can help prevent security disasters, and help control the damage in the event that preventive measures are not successful in warding off an attack.

- ***Have back-ups.*** Operational requirements should dictate the back-up policy, and this should be closely coordinated with a disaster recovery plan that will enable one to carry out proceedings from another location in case the original one has been attacked.
- ***Don't put data where it doesn't need to be.*** This will prevent unauthorised access to information, reducing the severity of a break-in
- ***Avoid systems with single points of failure.*** Any security system that can be intruded into by breaking through any one component isn't really very strong. Ensure a degree of redundancy as it could prevent a minor security breach from becoming a catastrophe.
- ***Stay current with relevant operating system patches.*** Exploiting old bugs is one of the most common (and most effective!) means of breaking into systems. The latest patches must be uploaded to overcome existing bugs.
- ***Security advisories.*** Watch for relevant security advisories from CERT and similar agencies. Personnel should be trained and should be familiar with security practices. They should keep themselves abreast with the latest developments and keep track of the various problems that arise.

CONCLUSION

Practically all ruses and stratagems of war are variations or developments of a few simple tricks like manipulation of beliefs, actions based on altered perceptions exploitation of the benefits from these actions *et al*. These have been practised by man through the ages. These deception concepts are now being employed within networks in order to deceive or condition a target's perception about the intent or purpose of actions.

The information revolution has ensured that conflicts will increasingly depend on information and communications matters. More than ever before, conflicts will revolve around "knowledge" and the use of "soft power." Adversaries will emphasise "information operations" and "perception management"—that is, media-oriented measures that aim to attract rather than coerce, and that affects how secure a society, a military, or other actor feels about its knowledge of itself and of its adversaries. Psychological disruption may become as important a goal as physical destruction. Thus, major transformations are coming in the type of adversaries, in the nature of threats they may pose, and in how wars will be waged. Information age threats are likely to be more diffused, dispersed, multi-dimensional, and ambiguous when compared to traditional threats.

As terrorist groups evolve towards loose, ad-hoc networks that form and dissipate unpredictably, counter-terrorism forces should also adopt a more flexible approach that crosses bureaucratic boundaries to accomplish the mission at hand. While it will be difficult for the military and government to do away with their hierarchies entirely, there is nevertheless much room for them to develop a more robust and dynamic organisational network than they currently have—a change that may offset some, if not all, of the advantages now accruing mostly to networked groups with vested interests.

In the era of information warfare, net wars, cyber warfare and nuclear backdrop, C4ISR systems should have physical and electronic security, survivability and adequate redundancy so that C4ISR and NCO systems are protected against deliberate or inadvertent, unauthorised acquisition;

disclosure, manipulation, loss or modification of sensitive information. The military is already keenly aware – both that it will have little ability to control the flow of information to and from the theatre and that the media will monitor every action of a soldier minutely. In a media intense environment, politicians and the public have become very unforgiving of even minor mistakes and transgressions by military forces. Events with minor operational effects often have disproportionately large effects on public opinion and, therefore, policy and outcomes. As a result, even the smallest aspect of military operations must now be planned with greater sensitivity to the public perception of the conflict. New techniques that allow manipulation of video images and sound recordings have created an even greater technical ability for potential opponents to conduct sophisticated psychological operations. The ability to influence such perceptions may mean the difference between victory and defeat. Governments no longer have the ability to control the flow of information to the public or their soldiers, in both peace and war-time. The biggest obstacle in the coming years will continue to be the technological illiteracy of those outside the computing community, and the closely related problem of poor appreciation of the implications of the digital revolution in the social, political and economic settings.

Even the smallest aspect of military operations must now be planned with greater sensitivity to the public perception of the conflict.

COMBAT SUPPORT OPERATIONS IN THE INDIAN AIR FORCE: A HISTORICAL APPRAISAL

A.B.S. CHAUDHRY

Till the time human beings compete for resources, power, or territory, there would be wars.

War is as old as human civilisation. As long as man, whether in groups, societies, communities, or nations, competes for resources and power, conflict and war will always exist as necessary elements of civilisation. History shows that armed conflict or warfare continues to be a recurring feature of mankind. From official and unofficial history, it is estimated that mankind has fought around 14,500 wars so far. According to one estimate, there have been only 270 years of peace in the last 3,500 years. From the end of World War II to the Falklands War of 1982, 148 armed conflicts have been fought in various corners of the globe, all in a span of 37 years;[1] or adding the more recent conflicts, we have had more than 150 wars in about 60 years. History clearly establishes the fact that wars will continue to plague mankind long into the future.

* Wing Commander **A.B.S. Chaudhry** is a Research Fellow at the Centre for Air Power Studies, New Delhi.

[1] Air Chief Marshal Fali Homi Major, "Indian Air Force in the Decades Ahead," *Air Power Journal,* vol. 3, no. 2, Summer 2008 (April – June), accessed through the link http://www.aerospaceindia.org/Journals

Over the next 100 years, air power developed exponentially to become the most critical element of national power of the most powerful nations.

The advent of air power at the turn of the 20th century changed the very complexion of military power, which was to transform the conduct of war enormously. More importantly, over the next 100 years, air power developed exponentially to become the most critical element of national power of the most powerful nations. Militarily, the advent of air power produced the most important and hitherto unknown dimension of war, the third or vertical dimension. The advent of flying machines changed the nature of warfare for all time. In a period of less than a century, military use of the air has moved from tethered balloons to aircraft and, now, to cruise missiles using satellite-based navigation systems. The third dimension of warfare has encompassed space itself. A detailed analysis of the evolution of air power into aerospace power would show that the last hundred years of technological and strategic developments were necessary to complete the understanding of the third dimension of warfare. The significance of air power is not only its characteristic of bringing in the third dimension into warfare but, more importantly, its ability to bypass all obstacles that are characteristic of land and sea warfare and make its effect felt deep inside on the entire nation-state rather than just the war-front.

AVIATION HISTORY IN INDIA AND EVOLUTION OF INDIAN AIR FORCE

Aviation History[2]

Joseph Lynn made the first balloon ascent in India from Lal Bagh Gardens, Mumbai, on September 24, 1877. The balloon rose to a height of 7,500 ft and came down at Dadar. After these developments, Indian aviation experienced a brief gap before heavier than air manned flight began when the Maharaja

[2] Group Captain Kapil Bhargava (Retd), "Beginning of Aviation in India: A Peep Into its Early History", accessed through http://www.bharat-rakshak.com/IAF/History/Aircraft/AviationIndia

of Patiala bought two airplanes in 1910. The first flight was carried out at Allahabad on December 10, 1910. The first military reconnaissance flight took place on January 16, 1911, at Aurangabad, where an aircraft was used to observe military manoeuvres. However, it was not a war-time mission. A distinctive event, the first aerial post in aviation history was undertaken by Henri Piquet in a De Havilland Humber bi-plane on February 18, 1911, from Allahabad to Naini. In December 1913, a Military Flying School was set up at Sitapur, UP, with five airplanes. The first Indian aviator and aircraft maker was Professor Venkata Subba Setti and the first Indians to join the Royal Flying Corps were Hardit Singh Malik, Indra Lal Roy, E.S.C. Sen, Naoroji and S.G. Welingkar. Most of these pilots credited themselves with distinction in World War I and Indra Lal Roy was awarded the Distinguished Flying Cross (DFC) for shooting down nine German aircraft. In the 1920s, aviation in India was mostly confined to the operations of the Royal Air Force.

Formation of IAF[3]

The Indian Air Force (IAF) was formed by a Gazette notification on October 8, 1932. On April 1, 1933, No. l Squadron was set up at Drigh Road, Karachi, with four Westland Wapiti aircraft and was designated as an "*Army Cooperation Squadron*". Subroto Mukherjee (later the first Indian Chief of the Air Staff), five other officers and 19 technicians formed the Indian complement. The squadron was initiated into military action in September 1937, in North Waziristan. Flying Officer (later Air Marshal) Engineer was the first IAF officer to be awarded a gallantry medal in these operations. The IAF saw action during World War II and the strength was increased from one to nine squadrons. For meritorious service during the Burma campaign, the British Monarch awarded the prefix "Royal" to the Indian Air Force.

India became a Republic on January 26, 1950, and on that day, the IAF shed the prefix "Royal". On April 1, 1954, exactly twenty-one years after the raising of its flight, one of its founder members, Subroto Mukherjee, took over as a Commander-in-Chief and the Chief of the Air Staff of the IAF.

[3] References from http://www.bharatrakshak.com and http://indianairforce.nic.in

Along with increase in fighter squadrons, it was also vital to develop the IAF transport capability at the earliest. A transport squadron of C-47 Dakotas was added in 1951, followed by the acquisition of the Fairchild C-119 Packet aircraft from the United States in 1954. Two more batches of Packets augmented the transport fleet in 1960 and 1963, respectively. The Packet functioned as the workhorse of the IAF for three decades. Modified in India with a "Jet Pack" for high altitude operations, the IAF Packets created history by landing on the airstrip in Ladakh and the Karakorams in a place called Daulet Beg Oldi at an altitude of 17,000 ft on July 22, 1962.

The modernisation of the IAF continued through the decades and today it has evolved as a trans-oceanic force. The inventory boasts of state-of-the-art fighters like the Su-30, Mirage-2000, MiG-29, Jaguars, etc. The transport fleet consists of IL-78 and IL-76 heavy lift aircraft, Boeing Business Jets, Embraers, An-32, Avro and Dorniers, while Mi-25s/35s, Mi-17s, Mi-8s, Chetak / Cheetah and ALH constitute the helicopter fleet. The IAF has been involved in joint exercises with the air forces of France, the US, Republic of Singapore and South Africa. The fighters flew non-stop thousands of miles, for the first time, with in-flight refuelling. The IAF has performed commendably in the international arena wherein the contingents have earned considerable praise for their exemplary contribution in United Nations Peace-Keeping Operations in Congo and Sudan. The IAF has also aided our civil authorities whenever called for during national calamities like floods, earthquakes, the tsunami, white tsunami in Srinagar or the earthquake in Bhuj. It is this capability of the IAF that enabled it to extend help to the United States during the disaster caused by Hurricane Katrina. The calls on the IAF transport fleet for operational logistic support or in aid of civil agencies during calamities and disasters are increasing. Towards this, the transport and helicopter fleets are being upgraded and modernised. Induction of 'force multipliers' like the Unmanned Aerial Vehicles (UAVs), Flight Refuelling Aircraft (FRA), Airborne Warning and Control System (AWACS) and Early Warning System would provide additional strategic reach and versatility for the offensive and defensive roles to the IAF.

In its 75 years of existence, the IAF has been called upon to employ its assets for national defence a number of times. Before attempting to describe the manner in which this aerospace power can be utilised in the future, it would be pertinent to highlight the aim and roles of the IAF.

> *The raison de`etre of the Air Force is to neutralise the enemy's war potential and protect one's own.*
>
> — Air Chief Marshal P.C. Lal

AIM AND ROLES OF IAF

The aim of the IAF is to organise, equip, train, sustain, deploy and employ the force to achieve national objectives. The IAF would continue to evolve itself into a potent force to meet the current and future challenges. Based on the threat perception, the IAF would equip itself to build the required capabilities and carry out requisite training to ensure potency of the force at all times. As dictated by national interests/objectives, the IAF would deploy and employ its forces either alone or in concert with the other Services so as to achieve the political objective in the most efficient manner.

Roles

The exact role that the IAF plays would depend on the nature of the threat and the unique nature of the campaign. Usually, the roles envisaged for the Air Force are as follows:

- Defence of national territory and of island territories, against attacks from air and space during both peace and war.
- Possess all round balanced capability to deter an aggressor from carrying out hostile acts and, if deterrence fails, to provide an effective response.
- Prepare in peace-time to achieve a potent offensive and defensive air capability.
- During operations, achieve control of the air to the required degree to provide full freedom of action to the air and surface forces.
- Apply direct pressure on the enemy's power of resistance by attacking his crucial centres of gravity.

- Synergise the combat potential of air power with that of the surface forces to achieve joint military aims and objectives. Further, to support the surface forces in their campaigns by neutralising the effectiveness of the enemy's surface combat power.
- Deploy and employ forces to protect and project national interests in any out of country contingency.
- Assist the government in disaster management or humanitarian relief tasks.
- Discharge international commitments requiring air power assets, consistent with our national policies and interests.
- Provide a viable second strike capability in case of a nuclear attack.

It would be worthwhile to extract some lessons from our participation in earlier conflicts. In the 1947-48 and 1962 Wars, the IAF was used mainly for airlift and in combat support roles. Combat support operations are as important as direct operations and this paper is an attempt to highlight the IAF's role in combat support operations.

Combat Support Operations

First, let us see what constitutes combat support operations. The IAF Doctrine defines combat support operations as "**those operations which are undertaken in support of air or surface combat forces to enhance their combat power and to sustain them**". The operations carried out to enhance the effectiveness of combat power are termed as combat support air operations and combat support air related operations. The effectiveness of combat power could be enhanced by increasing the mobility, surprise, lethality, accuracy, survivability, availability or flexibility of air and surface forces. Combat support air operations comprise air transported operations, Air-to-Air Refuelling (AAR), Surveillance and Reconnaissance, Airborne Early Warning (AEW), Electronic Warfare (EW) and Search and Rescue (SAR). Combat support air related operations include maintenance and integrated logistics, testing and evaluation, and Research and Development (R&D).

If air operations are to be successful, they need to be sustained and supported by dedicated ground activities. These are termed as combat support ground operations which include runway rehabilitation, Nuclear Biological Chemical (NBC) defence, ground defence, passive air defence, training and administration.

The detailed aspects of all facets of combat support operations would be covered in a later paper. This paper would be limited to combat support air operations, particularly to air transport operations and surveillance and reconnaissance operations.

Air Transported Operations

Air transported operations are defined as those operations that involve the movement by air of personnel and cargo through fixed wing or rotary aircraft within and between theatres of operations. Air transported operations for the IAF can be categorised into four major roles: airborne operations (which include airborne assault, air landed operations and special heliborne operations), air maintenance operations, scheduled services and casualty evacuation. There are essentially two categories of airlift:

- **Strategic Airlift:** Strategic airlift is the carriage of passengers or cargo between theatres (inter-theatre) or to any place within the area of interest. The traditional projection of power by land and sea was by definition a laborious and protracted process, often involving a degree of vulnerability en route that threatened the attrition or destruction of a force before it could even reach its objective. Although technological advances during this century have made surface deployment a speedier and more efficient process, the movement of the force by rail, road, and sea is still in many circumstances too slow, too restricted by geographical constraints or too susceptible to hostile interception. It was the growing perception of such limitations, coupled with an increasing awareness of what airlift could offer in terms of speed, reach and capacity that led to greater priority than hitherto being given to the build-up of a transport force to achieve strategic goals. The move of Indian troops by air from the Eastern to the Western theatre in 1971, and the Maldives operation in 1988 are examples of strategic airlift.

- **Tactical Airlift:** Tactical airlift is the carriage of passengers and cargo within a theatre (intra-theatre). Tactical airlift is resorted to for rapid and responsive movement within an area of operations to meet specific tactical goals.

The airlift task is undertaken by the transport and helicopter fleets of the IAF. The transport fleet maintains a capability for both strategic and tactical airlift. The fixed-wing aircraft enjoy higher transit speeds, carry heavier loads, are more reliable and are far cheaper to operate. However, helicopters have the capability to land anywhere, and troops and equipment can be delivered direct into action, thereby saving the need for ground lines of communication from airfields. Because of their greater ability to utilise terrain masking, they are also more survivable in the combat zone. Thus, both fixed wing and rotary wing aircraft are invariably needed in the overall air transport force mix.

Surveillance and Reconnaissance Operations.

Reconnaissance was the first military role assigned to air power. As wars progressed, this role was refined from visual reconnaissance to photo -reconnaissance. This further developed in the Cold War period to a day/night and all weather capability with the advent of IRLS and radar mapping. It was only when the sensors started producing digital data that the concept of dissemination of reconnaissance information in real-time to the user was born. Surveillance and reconnaissance operations involve the collection of information from space-based, airborne, and ground sensors on the activities, forces and resources of an enemy or potential enemy. Since surveillance is the systematic, repetitive gathering of information, the information gained from surveillance is normally used for strategic planning. Reconnaissance is observation of specific targets, interests and areas by visual/photo means or other detection methods at a particular time to gain information about the activities, resources and intentions of an enemy.

ROLE OF INDIAN AIR FORCE IN COMBAT SUPPORT OPERATIONS

The first role adopted by the IAF was of Tactical Reconnaissance (Tac-R), with instructions to take on targets of opportunity. During one such mission on August 7, 1940, Sqn Ldr Subroto Mukherjee (later the first Indian Air Chief) noticed a besieged friendly force in Daur Valley of Miranshah. The Army picquet had little or no ammunition, which they conveyed through gestures. Sqn Ldr Mukherjee instructed his gunner in the Wapiti to offload ammunition from the aircraft gun, stuff it in his socks, and then he dropped this precious load in a low pass over the Indian Army picquet. Other aircraft also did the same and the post held out effectively.[4] This is one of the early instances of combat support operations, or rather an instance of combat air support being extended to supply drop by the Wapitis.

Burma Campaign

Japan entered World War on December 7, 1941, and by the end of December, the Japanese were in the jungles of Burma, seriously threatening the Indian subcontinent. The combat support role of the Air Force was primarily in the form of reconnaissance missions. No. 6 Squadron created a record for the monthly average of sorties flown per pilot for the Allied operation in the 3rd Tactical Air Force. It had completed 1,000 reconnaissance sorties. During the war years, the steady expansion of the IAF had placed all emphasis on Army cooperation and tactical reconnaissance; it had continued to fly ageing aircraft such as the Hurricane when such aircraft as the Thunderbolt and Mosquito were being inducted in large numbers by other Allied forces in the theatre and it had, in consequence, suffered a sense of equipment inferiority. Nevertheless, assigned the least glamorous of tasks and flying obsolescent equipment, the Service established traditions of courage and efficiency second to none; its personnel had been awarded 22 DFCs and a host of other decorations, and in recognition of its achievements, it had been honoured by bestowal of the prefix "Royal" on its title in March 1945.

[4] Air Marshal T.M. Asthana, "Evolution of Tactics in the IAF: A Historical Perspective", paper presented at the capsule on National Security and Aerospace Power at Centre for Air Power Studies, New Delhi, July 13, 2009.

Lord Louis Mountbatten later said that in all his experience of the Southeast Asia Command and over the hump flights to China, he had never known of such an airlift being effected at such short notice.

Kashmir War of 1947-48

The partition had depleted the IAF in terms of both resources and manpower. Grappling to establish itself as an independent force and dealing with the brutal realities of partition, a mere two months later, the Air Force found itself in action against hostile invaders in Jammu and Kashmir (J&K). On October 22, 1947, Pakistan launched an attack on the Kashmir Valley to wrest the state of J&K. Four to five thousand tribals came rampaging through the Valley followed by regular troops in civilian apparel. The state of J&K became a part of the Indian territory on October 26, 1947, after Maharaja Hari Singh signed the Instrument of Accession with the Government of India and it was now incumbent on the government to respond to the Maharaja's plea for help against the plundering hordes. The situation was so grave that a very unusual rider to the operational instructions issued to the task force had to be included, viz, "To reconnoitre from the air and return to Jammu if the raiders had occupied the airstrip."[5] The Air Force flew the first contingent of the Indian Army into Srinagar on October 27. The first aircraft touched down at 0830 hrs, just in time to save Srinagar airstrip and the city. By the end of October, a brigade strength of men and material had been flown in and the Valley was saved. In this war, the size of the IAF transport fleet was small, hence, civil Dakotas, flown mostly by former IAF pilots, were requisitioned for this crucial air-bridge.

Lord Louis Mountbatten later said that in all his experience of the Southeast Asia Command and over the hump flights to China, he had never known of such an airlift being effected at such short notice. From then on, till the ceasefire on January 1-2, 1949, the Air Force continued giving intimate and regular support to the Army in one of the most difficult and hazardous terrains of the world.

Similarly, the attempt to capture Leh by the Pakistan Army was thwarted by timely, and what has become a "legendary airlift", by Air Cmde "Baba"

[5] "Striking Yaks", *Squadrons of the IAF*, Vol. 6 (College of Air Warfare, 2007), p. 7.

Meher Singh, during which, essential military supplies were delivered. Air Cmde Mehar Singh, landed a Dakota at Leh on May 24, 1948, on a sandy strip next to the Indus River at a height of 10,700 ft above mean sea level. Never before had a Dakota transport aircraft landed at such heights. An uncharted route over the Himalayas, where the hill peaks ranged anywhere between 15,000 and 24,000 ft, was opened. The Indian Army's faith in the Air Force was demonstrated by the fact that Maj Gen Thimayya (later Chief of the Army Staff) accompanied the AOC in the aircraft. This was followed by an airlift of troops to Leh which saved Ladakh.

Besides the defence of Srinagar and Leh, the Indian Air Force played a significant role in the battles for Kotli, Jhangar, Naushera, Tithwal, Rajori and Kargil. The Indian Army successfully executed one of the most glorious military operations in the most difficult circumstances and in a unique terrain. Had it not been for the timely airlift of troops on that fateful day of October 27, 1947, the history and map of India might not have been the same.[6] In the 15-month-long Kashmir campaign, air power displayed its unique characteristic of mobility and reach.

1962 War with China

This is the only war where we had to suffer many casualties and loss of territory. Significantly, this also happens to be the only war in which combat air power was not utilised. In 1962, during the India-China conflict, the IAF provided the much needed logistics support to the Indian Army fighting in some of the most trying environment. Without essential air support, the Indian Army faced overwhelming odds in their fight against well trained Chinese troops. The Indian leadership grounded the IAF for the majority of the war, fearing that if the IAF attacked the Chinese forces, the PLA Air Force (PLAAF) would retaliate on Indian cities (a feeling based on utter lack of information) and the perception that the Chinese Air Force could interfere with the IAF transport operations on which the Indian Army was critically dependent[7].

[6] Air Marshal Bharat Kumar, *An Incredible War: IAF in Kashmir War 1947-1948* (New Delhi: K W Publishers, 2007), Introduction by Air Commodore Jasjit Singh, p. xv

[7] Group Captain Sanjeev Bedi "Strategic Role of Air Power", *Air Power Journal,* vol. 3, no. 2, Summer 2008 (April – June).

The main source of supply for the troops was air maintenance by the Air Force. Both Dakotas and Packets were pressed into service to provide the required supplies, for the task of transporting troops and stores, evacuating casualties and to maintain air supply in the hazardous mountainous region of both Ladakh and the Northeast Frontier Agency (NEFA). The helicopters had to constantly run the gauntlet of Chinese small arms and anti-aircraft fire, while operating from tricky helipads in the mountains. Among the notable feats performed by the IAF during the conflict were the operation of C-119 Packets from airstrips 17,000 ft above sea level in the Karakorams and the airlifting of AMX-13 light tanks by An-12s to Chushul in Ladakh.[8] The IAF flew countless number of missions for airlift, airdrop and casualty evacuation. It was a remarkable achievement that not a single aircraft was lost during the whole operation.

1965 War with Pakistan

This war in August-September 1965 was the first full scale war which the IAF was involved in since independence. In this war, the first aircraft got airborne 29 minutes after the Army Chief asked for air support, and includes the time used in transmitting the Air Chief's orders to Western Air Command and the stations. Not many air forces have been able to match the less than 30 minutes from political decision to armed strike aircraft take-off that was managed by the IAF. [9] The IAF, along with the combat role, was employed in support roles like airlift, casualty evacuation, etc., which are listed below:

- No. 12 Squadron flew 730 hours and airlifted more than 1,000 tons of equipment and supplies.[10]
- No. 106 Special Reconnaissance (SR) Squadron flew photo reconnaissance

[8] "Transporting AMX tanks to the battle area posed a major hurdle as even the largest aircraft of the IAF, the An-12, with one tank would far exceed its maximum permissible take-off weight. The tanks were manhandled into the recently acquired An-12 transport aircraft, de-fuelled down to the barest minimum to make the round trip to Chushul in Ladakh, to give the Army a fighting chance against the Chinese onslaught." Air Commodore Jasjit Singh, *The Icon* (New Delhi: K W Publishers, 2009), p. 135.

[9] Ibid., pp. 182-183.

[10] n.5, p.22. .

missions and continued the recce missions even after the ceasefire, to assess the damage inflicted.[11]

- Dakotas of No. 43 squadron undertook casualty evacuation, transport support, news bearing to forward area bases and also special operations courier sorties.[12]
- Prior to the 1965 War, helicopters carried out reconnaissance and observation sorties. During the war, the helicopters undertook casualty evacuation and mercy missions, evacuating casualties from the battlefield in the midst of intense enemy fire and air raids.[13]

1971 Operations

The IAF's task in the east primarily involved direct support of the ground forces and air-bridging operations. Although Pakistan had initiated the war with preemptive air strikes against major forward air bases, the IAF rapidly gained the initiative and thereafter dominated the skies over both fronts.

The Tangail Paradrop[14]

In the Eastern theatre, the IAF gained total air superiority within 48 hours of going into action, a factor which directly contributed to the ultimate capitulation of the East Pakistan garrison. In order to cut off the withdrawal of Pakistani troops to Dacca from the Mymensing area, it was decided to airdrop a para battalion group with its supporting arms, north of Tangail. The aircraft used were An-12s, Packets and Dakotas. A dummy airdrop was carried out by two Caribous about 16 km away from the actual site. The main paradrop was undertaken by 48 aircraft on December 11. The entire operation was conducted with clockwise precision and was the first large-scale para-operation conducted by the IAF in war. Subsequently, on December 12, a pre-planned resupply for the Para Battalion was carried out by An-12s and Packet aircraft. In this

[11] "Lynx," *Squadrons of the IAF: Vol. 11* (College of Air Warfare, 2009), p. 8.

[12] "Ibexes," *Squadrons of the IAF: Vol. 10* (College of Air Warfare, 2007), p. 10

[13] "Siachin Pioneers," *Units of the IAF: Vol. 3* (College of Air Warfare, 2005), p. 6.

[14] *History of Indo-Pak War, 1971 Part-II* (History Division, Ministry of Defence, Government of India), accessed through the link http://www.bharatrakshak.com/Army/History/1971War

war, Indian Airlines' Boeings were also utilised for airlifting troops and stores.

The IAF's transport aircraft and helicopters undertook extensive casualty evacuation on their return flights from forward airfields and landing zones. Combat support missions like air maintenance sorties and casualty evacuation from Agartala to Gauhati (Guwahati), air maintenance sorties for troops at Sylhet, Daudkandi and Tangail and air maintenance sorties in the NEFA region continued throughout the war period.

Eight Mi-4 helicopters flew 164 sorties, helilifting 1,350 armed troops and 40,070 kg of weapons and equipment.

The Helibridges

Heliborne operations on a large scale were mounted in India, and perhaps in South Asia, for the first time during the 1971 War. They proved to be the key to rapid movement of the ground forces in the Bangladesh terrain criss-crossed with innumerable rivers and rivulets. The complete mastery of the air achieved by the IAF in the Eastern theatre enabled the helicopters to operate safely. Although there were only 14 Mi-4 helicopters in the theatre (for casualty evacuation and carrying senior commanders across different sectors), the heliborne operations were well planned and well executed. The pilots had to perform night landings on unprepared ground and on improvised helipads illuminated by torches.

The biggest helilift operation for transporting troops, arms and equipment was undertaken from Brahmanbari to Narsingdi and from Daudkhandi to Baidya Bazar between December 11 and 15. Eight Mi-4 helicopters flew 164 sorties, helilifting 1,350 armed troops and 40,070 kg of weapons and equipment. The important aspects of these special helicopter operations are:

- The helilift was undertaken from improvised helipads without any ground facilities.
- The pilots operated under the most trying conditions, both by day and night, without much prior training in this role.
- The landings on most occasions had to be done in the face of enemy small arms fire.

- These missions were completed with very marginal fuel reserves.
- All the battle-damaged helicopters were repaired in the field.
- In total, between December 7 and 15, the helicopters flew 409 sorties, lifting 3,803 troops and 100,070 kg of weapons and equipment between various sectors. And the task was performed by only eight to ten helicopters which were operational at any given time. Indeed, a great achievement by the IAF.

Air Operations in Support of the Navy

Dakotas and Avro HS-748s of the Indian Air Force were extensively utilised for maritime reconnaissance. These maritime air support sorties began on December 4, and continued on a daily basis thereafter.

"Where there were enemy strongholds, the IAF pounded them, where there were big rivers, the IAF airlifted troops and equipment, and where pressure was required to bear on the enemy to ask for ceasefire, the IAF was there to apply it".[15] Combat support operations were undertaken on a large scale in the form of tactical reconnaissance, airlift of troops, resupply tasks, etc. The success of counter-air operations and combat support operations was proved during this war.

Kargil Operations (1999): Operation Safed Sagar

By mid-July, IAF fighters had flown approximately 1,200 sorties with devastating effect. Helicopters made a significant contribution in the Kargil war and flew around 2,500 sorties, transporting large numbers of troops, casualties and hundreds of tons of load, besides flying attack missions. The IAF transport fleet also worked round the clock in meeting the task of moving squadrons to their operational locations, as also transporting men and equipment of the Army. In this operation, the IAF, despite severe constraints, proved to be the decisive force in evicting the invaders.

Though the Kargil War is more remembered for the downing of the MI-17 during offensive support, much of the innovative tactics are glossed over. For example, a successful offensive in the Gurej sector was primarily

[15] Ibid.

based on the move of four 130 mm artillery guns to a bowl from where direct fire on enemy positions could be undertaken. All this was done by two Mi-17s within nine hours, just before the main attack was launched.

OTHER OPERATIONS

Operation Meghdoot

It is a story of courage in the continuous, untiring and relentless support by the IAF to the forces deployed there, which is a challenge for both man and machine. Operation Meghdoot was undertaken in support of the Indian Army and paramilitary forces in northern Ladakh, to secure control of the heights dominating the Siachin Glacier, also referred to as the world's third pole and potentially a dangerous flashpoint on the disputed northern borders. Timely induction of own troops by airlift prevented the Pakistan Army from occupying the ridge at Saltoro. The IAF's Il-76s, An-12s and An-32s transported stores and troops, airdropped supplies to high altitude airfields while Mi-17, Mi-8, Chetak and Cheetah helicopters ferried men and material to heights far above the limits set by the helicopter manufacturers.[16] In fighting for this "roof-of-the world" since April 13, 1984, the IAF's incredible performance at the extremes of temperature and altitude remains a continuing saga of fortitude and skill, where transport aircraft and helicopters have been stretched to their limits in providing unhampered air-link in support of the Army and civilians.

Sri Lanka Operations; Operation Pawan

Following the Indo-Sri Lankan Accord on July 29, 1987, the Indian Peace-Keeping Force (IPKF) was inducted into Jaffna area, to assist the Sri Lankan government in their fight against the Liberation Tigers of Tamil Eelam (LTTE) guerrillas. This operation lasted almost 30 months and about 70,000 sorties were flown by the IAF's transport and helicopter force to and within Sri Lanka, without a single aircraft lost or mission aborted. The IAF utilised all its assets to provide aerial reconnaissance and mobility to fight the insurgency; An-

[16] Accessed from http://indianairforce.nic.in June 8, 2009.

32s carried out airlift and casualty evacuation in one of the most inhospitable terrains against hardcore militants. The Mi-8s became the critical lifeline for the field forces as well as providing air transportation to the Sri Lankan civil administration.

Operation Falcon

After India's conversion of Arunachal Pradesh from a Union Territory to a state, tensions between China and India escalated. By early April, China had moved eight divisions to eastern Tibet, and reinforcements on the Indian side began with Operation Falcon in late 1986, and continued through early 1987. This massive air-land exercise involved ten divisions of the Indian Army and several squadrons of the IAF. The Indian Army moved three divisions to positions around Wangdung, where they were supplied solely by air. The 1987 episode was, to a large measure, logistically supported by the newly inducted Mi-17s.

Operation Cactus—Maldives

In response to a request from the Government of Maldives, the Indian Air Force mounted special air-landed operations on the night of November 3, 1988, to airlift a parachute battalion group from Agra, non-stop over 2,000 km to the Maldives. The IL-76s carrying elite commando forces landed at Male under the cover of darkness and the coup bid was foiled. The operation was carried out with flawless coordination and precision, leading to complete success of the mission. The most immediate reality that emerged from this brief and bloodless action was the swift and effective Indian military response, made possible by the IAF's strategic airlift capability.

Strategic Airlift

The IAF has been utilised for protection of aircraft and ships evacuating the Indian population during the Gulf War of 1991: 1,13,000 of the 3,00,000 Indian citizens resident in the Gulf region were flown back home on aircraft of the Indian Air Force, Indian Airlines and Air India in what remains till today the second largest airlift in world history after Berlin 1991.[17]

There is a need to plan ahead in order to ensure that a credible airlift capability is maintained.

CONCLUSION

The "Third or Aerospace Dimension" would become a very critical factor affecting the military, economic, and technological capabilities of a nation-state. The transformation of air power into aerospace power over the last hundred years has resulted in the third dimension emerging as the dominant factor in modern wars. From the Bekka Valley operations to the Gulf and Afghan Wars, it has rapidly developed into an overwhelmingly dominant dimension. In order to be a dominant regional player and a prominent global player, we should be capable of looking far ahead, identifying troubled spots, planning early, reaching out with the required load, and delivering the load with precision. Thereafter, we should have the ability to sustain in the hostile area, achieve goals within time-frames and de-induct efficiently.

There is a need to plan ahead in order to ensure that a credible airlift capability is maintained. The capacity gap that exists between the An-32 and the IL-76 payloads also needs to be bridged in order to optimise operations. Today, the IAF is expected to maintain the capability to deliver up to battalion strength (about 800 paratroopers) into a conflict area. In order to accomplish this objective, the air effort required by Il-76 and An-32 aircraft is quite large, with an appropriate number of standby aircraft of each type, as also a big element of offensive combat aircraft to protect the mission. Any such operation would be at the cost of other roles that the aircraft are expected to perform at the critical stages of a conflict. Such a drop was possible during the para-drop in 1971 mentioned above, because the IAF had total air dominance wherein there was not even a single aircraft airborne from the opposing side. Air dominance might not be a possibility in future wars and, hence, an alternative for the

[17] Air Vice Marshal Kapil Kak, "Joint Capability Requirements of India's Armed Forces: 2008-2033", *Air Power Journal*, vol. 3, no. 1, Spring 2008 (January-March), pp. 26-27.

Army would be to choose a company size force dropped by smaller fixed wing aircraft or an even a smaller size force dropped by a rotary wing platform. On the part of the IAF, a 20-ton class of aircraft, when inducted, can lead to substantial reduction in the number of aircraft that would be required for the drop, thus, improving the chances of survivability and success of the whole operation. Several new operational technologies are now available in modern military transport aircraft. These are essential to give the required operational punch to the Indian armed forces to take the complexities of the future battlefields in their stride.

A 20-ton class of aircraft, when inducted, can lead to substantial reduction in the number of aircraft.

The wars of 1962, 1965 and 1971, and the quarter century of peace thereafter, will always serve as reminders of the famous dictum: "If you want peace, be prepared for war". With this backdrop, the IAF has no option but to keep pace with the regional air powers and upgrade its capabilities to meet any threat that may arise in the future. India has a very long border against two implacable foes. A million-strong Army is strewn all along the entire length of this border. Where and when a pressure point might erupt cannot be forecast. Therefore, we must have the means to concentrate our land forces, wherever and whenever necessary in the shortest possible time. In its sizeable transport fleet, the IAF has both tactical as well as strategic airlift capabilities. Coupled with the other national air transport resources, the Indian Air Force is capable of bringing to bear the combat power of the land forces quickly both within a theatre as well as outside.

CLIMATE CHANGE AND NATIONAL SECURITY: CONTRARIAN OR INTERRELATED?

MANOJ KUMAR

The geo-politics associated with climate change negotiations in the recent past, has offered a bitter picture for the world to behold. The yearning for opulence in the present-day world is so deep-rooted that saner thoughts of an inhabitable future are being banished from consideration. Since the world is defying nature by delaying the mitigating actions to halt the march towards climate change doom, the consequences are now becoming clear. There is near unanimity in the world that climate change would lead to scarcities of basic natural resources that are essential for the human race to survive. Availability of food, water and land would reduce considerably due to various factors such as sea level rise (global warming), increased desertification, droughts/ floods (glacial melt), all caused due to climate change. This fact is mentioned in successive reports prepared by the Intergovernmental Panel on Climate Change (IPCC) in the last two decades or so. Though the broad connections can be drawn between climate change and future security challenges caused by the complexities of resources distribution, this is only relevant if the source information is accurate and reliable enough to be able to drive real changes in strategy, policy and operations. Therefore, the first critical step in establishing a relationship

* Wing Commander **Manoj Kumar** VSM, is a Research Fellow at the Centre for Air Power Studies, New Delhi.

between climate change and security must be to analyse the information needs of decision-makers around the process of climate change.

The IPCC is an international multi-disciplinary body of more than 1,000 scientists and specialists drawn from all member countries of the United Nations Environment Programme (UNEP) and World Metreological Organisation (WMO) working in three different working groups. The reports of the working groups on the dynamics of the earth's climate system, potential impacts of climate change, and the possible responses to the threat of climate change, including adaptation, are rigorously reviewed by more than 2,500 scientists and experts. Therefore, their findings (Working Group 2)[1] on the impact of climate change, which directly implicate these resource scarcities to come into play, are accepted worldwide without prejudice. There are many other independent and non-governmental organisations within India and abroad that have reached more or less the same conclusions.

Each inhabitant of this planet aspires, and rightly so, to his share of the earth's resources. No sovereign nation or individual can claim total control of these resources. Their scarcities would, therefore, throw up the larger question of proportional division, with diverse views on how and who is to decide the proportion. In the same context, the debate on viewing the carbon contribution of any country on per capita vis-à-vis total emissions basis is still raging between the developing and developed countries. One is reminded of the famous words of Benjamin Franklin "We must hang together, or we shall assuredly hang separately".

A parallel case study would indicate that the imperatives of maintaining supply of fast depleting fossil fuels and other natural resources by the energy hungry West has been a reason for the developed nations to coercively impress their political will in Asia (Middle East) and Africa. This scenario needs to be juxtaposed with the present Indian situation wherein almost 300 million people do not even have regular access to electricity (by a conservative estimate of the states facing energy deficiency) and these acts of the Western countries seem totally superfluous. Now if this scarcity was to

[1] The IVth assessment report came out in 2007. It can be assessed at www.ipcc.ch/publications.

be that of something as basic as food or water for more than half the world's population residing in the developing nations, the tumultuous societal stresses that would accrue and their scale, would most definitely dwarf any rationale for peaceful coexistence. If the energy required to maintain only the quality of life and progress of a nation is a strong enough reason for nations to go to war, then deficiency of basic necessities of survival such as water, food or even basic habitat, due to the consequences of incremental and sudden climate change events, would most definitely qualify for causing worldwide disturbances and conflicts. The timelines for the eruption such conflicts cannot be accurately predicted; but it is within our ability to avoid it to a large extent. Thus, climate change and national security are serious and interrelated topics that the policy-makers need to take into consideration.

If the energy required to maintain only the quality of life and progress of a nation is a strong enough reason for nations to go to war, then deficiency of basic necessities of survival would most definitely qualify for causing worldwide disturbances and conflicts.

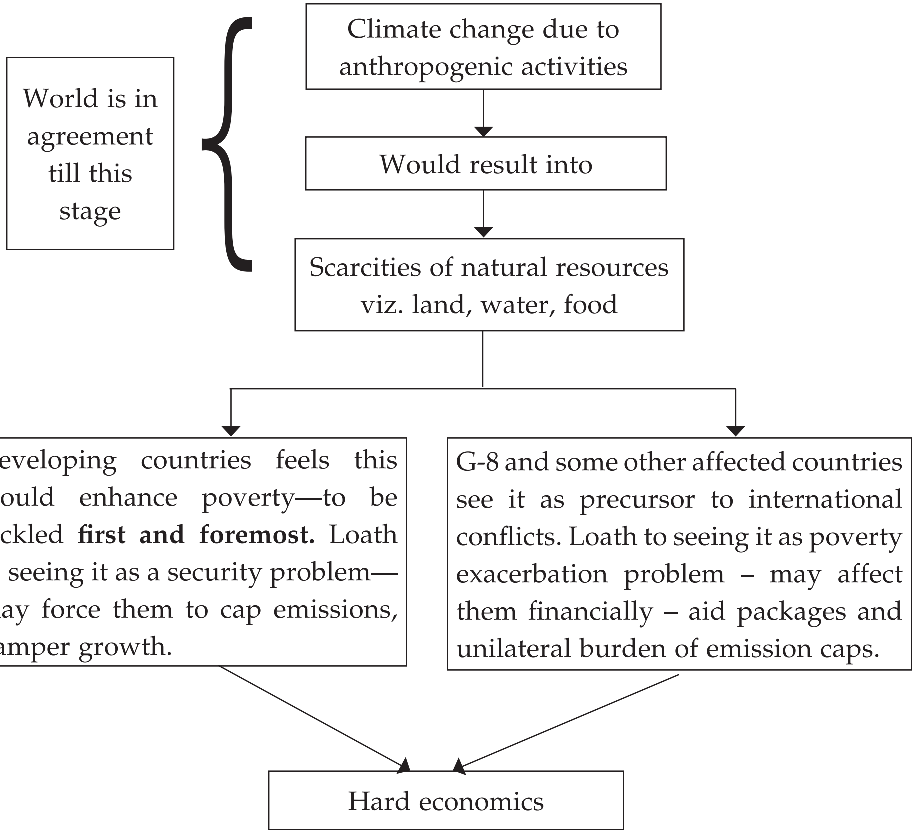
"Climate Change and Security" has been the topic of many scholarly studies in the European Union (EU) and the US in the last few years.[2] One thing which stands out as common in almost all these Western studies is the focus on international security as a consequence of climate change. It has been postulated that nations would go to war as the scarcity of resources and onslaught of national calamities caused by climate change like droughts, storms or floods, are faced by them. Situations in Darfur and other such hotspots are quoted in these reports. The Indian, and, for that matter, the developing countries' position has been at loggerheads with this line of thinking. They feel that it is the existing poverty in their country, caused by uneven distribution of wealth amongst nations, and which would get

[2] An official EU paper, *Climate Change and International Security;* German Advisory Council on Global Change (WBGU) paper titled *Climate Change as a Security Risk;* the US Council on Foreign Relations Special Report, *Climate Change and National Security;* the CSIS / Center for a New American Security Publication, *The Age of Consequences: The Foreign Policy and National Security Implications of Global Climate Change; American think-tank CNA paper on Climate Change and Security.*

exacerbated due to climate change, that needs to be eradicated / tackled primarily. It is also felt that the developed countries are sidestepping these issues of poverty eradication by bringing in the dimension of international conflicts due to climate change. It is being feared that with the security concerns firmly on the agenda, the developed countries would be able to push for binding emission cuts across the globe by linking these with trade sanctions and pressures in other similar forums, thereby affecting the growth and progress of the poorer nations. Two events lend credence to this line of thinking. In April 2007, the UK moved an agenda point in the UN Security Council for discussions on climate change and its security implications. This move was vehemently opposed by India, China and some other nations as they were against securitisation of climate change, deeming the Security Council as an incorrect UN agency to discuss the issue, having ramifications on how the issue is being and has been treated till now. The second event is more recent. The US House of Representative passed the American Clean Energy and Security Act on June 26, 2009, by a very narrow margin (219-212). It was passed after an amendment called the Waxman-Markey Amendment was introduced which calls for trade sanctions on countries that do not meet their carbon emission targets after 2020. The target that is laid down under the Act for the US itself is not substantial and does not meet the aspirations of the concerned global community. It is another matter that this form of trade protectionism has been rejected by President Obama. But these two events emphasise the presence of hidden motives by the developed countries in the securitisation of the climate change debate, watched by a circumspect developing countries caucus. These developments have blurred the underlying truth that climate change is actually a human security issue that confronts the entire globe.

On the face of it, the two positions mentioned above adopted by the developed and the developing country caucuses are incongruent, giving rise to the present debate on the interrelation between climate change and security. However, a deeper analysis would show that these two viewpoints are convergent and the parties concerned are drawing different conclusions from the same set of situational variables. Consider the following Fig 1:

Fig 1


World is in agreement till this stage
Climate change due to anthropogenic activities
Would result into
Scarcities of natural resources viz. land, water, food
Developing countries feels this would enhance poverty—to be tackled **first and foremost.** Loath to seeing it as a security problem—may force them to cap emissions, hamper growth.
G-8 and some other affected countries see it as precursor to international conflicts. Loath to seeing it as poverty exacerbation problem – may affect them financially – aid packages and unilateral burden of emission caps.
Hard economics

From the figure, it is clear that the driver for the differing perceptions of the same problem is actually the economic impact of pursuing a particular thought process. Whatever be the compulsion in opting for a particular public posture, the bottom line remains that every nation would have to take into account the direct domestic impact of incremental and abrupt climate change on its security.

CLIMATE CHANGE: NATIONAL SECURITY CONCERN—AN INDIAN PERSPECTIVE

There is a major implication for the Indian security due to climate change. The cause for concern is the presence of unfriendly, fragile and unstable

The rising sea level coupled with the onslaughts of extreme weather events that regularly visit the Bangladesh coastline have forced large scale migration of people.

states surrounding India. Be it Bangladesh, Pakistan, Myanmar, Sri Lanka or Nepal, all of them are going to be adversely affected due to the impact of climate change. The resulting societal stresses—economic or social—would force, and are forcing, their populations to depend upon a comparatively stable and progressive neighbour: India. The consequent drain on India's resources would bring about chaos due to the sharpening of class distinctions. This would also provide a breeding ground for terrorism and other forms of class struggle in these countries and cause an adverse impact on India's national security. How these consequences of climate change events pan out in terms of security problems for India would be briefly discussed so that the point is well appreciated.

Land Scarcity

It does not require a deep analysis to understand the conflicting claims by nations over Arctic territories and waters. When the Arctic ice cap melts due to global warming, it will open new navigable routes and it is also expected that the vast oil and natural gas reserves concealed would show up. Control over these resources would most definitely prove to be economically beneficial for whosoever can claim a larger chunk of the Arctic pie.

This scenario becomes abject when seen in the context of the untold miseries it would cause to the millions who will see their dwellings being submerged as the ocean level rises with the melting of polar ice caps and glaciers. It would see large scale migration of people from coastal areas to inland ones or across international borders, if there is no support structure within the state. The poorest would be hit the hardest as access to fertile land will decrease and become a major engine of climate driven conflict. In the Indian subcontinent, a less developed country like Bangladesh has already been adversely affected. The rising sea level, coupled with the onslaughts of extreme weather events that regularly visit the Bangladesh coastline have forced large scale migration of people to the inland areas and across the borders. Since the country is poor, a large mass of people has moved in to India to eke out a living. States in close proximity like Assam, West Bengal and Orissa in east India which have similar language/culture, were fertile ground for their absorption and livelihood. However, the problem has attained such a large proportion with so many adverse climate events having lashed the coastlands of Bangladesh that even Mumbai (western India) has seen a large influx of these 'climate refugees'. India being the second most populous country, can ill afford such pressure on its own resources. The resentment against these migrants, be it in Mumbai or Assam, has come to the fore with political and armed movements against them, resulting in ethnic conflicts. These poor people are also easy fodder for vested interests that are inimical to Indian progress and are misguided to wage proxy wars. The chain of events outlined above is very evident in India. The souring of relations with these countries is a natural corollary. This is one of the security problems that India would have to cope with when climate change forces unfavourable alterations in its geographical proximity. This security concern has both internal and external ramifications.

Economics of Water

We have heard that future wars would be fought not for oil but for fresh water. The main sources of fresh water on earth are the polar ice caps, permafrost and glaciers. With global warming, these sources are depleting much faster than what has been witnessed in the past. It will cause (is causing) sea level rise, and floods in the plains in the near future and, finally, water scarcity would be felt by the middle of the century. The water scarcity would be exacerbated by reduced rainfall caused due to the changing weather pattern as a result of global warming. As per the IPCC fourth assessment report (Working Group 2) fresh water availability in Central, South, East and Southeast Asia, particularly in large river basins, is likely to decrease due to climate change and, along with population growth,

Forty-seven per cent of the world's population is dependent upon water sourced from the Tibetan Plateau which in itself is not inexhaustible.

it is likely to adversely affect more than a billion people in Asia by 2050. It will also affect marine and coastal ecosystems and more than a million people along the coastal region.[3]

Analysts have always postulated that water wars are not very likely as such disputes are and have been normally settled through adopting superior technology, better water management practices and closer international cooperation. The challenge is in applying these in politically sensitive and developing regions without raising political tensions and driving conflict; this will require strong support and preventive intervention from the international community. It is likely that most agreements will fail under the higher impacts of climate change, especially in glacier-fed river systems. Therefore, this theory would witness a change in the coming years. The Tibetan Plateau is a source of much water. It is Asia's principal watershed and the source of 10 of its major rivers, including the Yalong Tsangpo/ Brahmaputra and Indus. Forty-seven per cent of the world's population is dependent upon water sourced from the Tibetan Plateau[4] which in itself is not inexhaustible. The upper, mid and lower riparian nations in Asia like China/ India/ Bangladesh/ Pakistan have been facing water shortages and negotiating their quotas of water from rivers flowing from Himalayan glaciers, though not much success has been achieved in resolving all the issues. With China wanting to divert the Brahmaputra's water towards its arid north, the mid and lower riparian nations like India and Bangladesh respectively are crying foul. However, what needs to be actively considered is that the situation has not yet deteriorated to a level where water scarcity would start affecting life in these nations. Once that happens in the future, these tensions will have the potential to cause, firstly, internal conflicts between states and then the still worsening situation may force nations to resort to violent actions to seek their share.

[3] www.ipcc.ch/ar4-wg2

[4] www.atimes.com/atimes/China/JL09Ad01.html

Similarly, Bangladesh has been calling India's decision of constructing the Farraka Barrage on the Ganges (11 miles from the Bangladesh border) to divert water in the Hoogly River for flushing silt, totally ill-conceived.[5] The present situation is one of distrust. China, India and Bangladesh have dithered in sharing water flow data at various points on different rivers (Lohit and Ganges). The situation is so serious that this data has not been shared accurately even between neighbouring states in India lest it is used to demand a higher share by one of them. On a few occasions, the water tribunal and central governments bodies have had to intervene and resolve the related issues. India has already seen civil strife in the southern states over water. It is altogether another matter, though related to climate change, that presently these states are facing floods while a traditionally flood prone state like Assam is facing a drought like situation.

For example, a 0.5°C rise in winter temperature would reduce wheat yield by 0.45 tonnes per hectare in India.

Food Security

World Food Day celebrated every year on October 16 gives an impetus to food security, but there are major challenges to be surpassed for human welfare. In reality, India is passing through a transition from surplus production supply to greater demand for staple food commodities. When India, which has traditionally been a food exporter, reaches the international food markets for imports, the food prices start to go through the roof. This would be observed with more frequency due to many incremental and extreme weather events that are likely to visit South Asia in the near future as a result of global warming. As per the IVth IPCC report there would be a substantial drop (up to 30 per cent by 2050) in cereal production in Central and Southeast Asia. Crop simulation modelling studies based on future climate change scenarios indicate that substantial losses are likely in rain-fed wheat crops in South and Southeast Asia.[6] For example, a 0.5°C rise in winter temperature would reduce wheat yield by 0.45 tonnes per hectare in

[5] www.sydneybashi-bangla.com

[6] Fischer et al., 2002

Any change in rainfall patterns poses a serious threat to agriculture, and, therefore, to the country's economy.

India.[7] More recent studies suggest a 2 to 5 per cent decrease in yield potential of wheat and maize for a temperature rise of 0.5 to 1.5°C in India.[8] Enhanced variability in hydrological characteristics is likely to continue to affect grain supplies and food security in many nations of Asia.

Intensification of agriculture will be the most likely means to meet the food requirements of Asia, which is likely to be affected by projected climate change. The arrival and performance of the monsoon is not an insignificant matter in India. It is avidly tracked by the national media because agriculture in the country is largely dependent on rainfall for irrigation and even the national budget to some extent is based on it. Any change in rainfall patterns poses a serious threat to agriculture, and, therefore, to the country's economy. Scientists are predicting that because of global warming, this already fickle weather system could become even more undependable, with failure of the monsoon as one of the climate 'tipping points'**.**

With such a threatening food security situation developing in the agriculturally most active region of the world, the poor and vulnerable population all over the world would be adversely affected. Seen in conjunction with other scarcities like of water and land, this paints a chilling scenario in which the failed weak states and economically deprived population will become fodder for the international terror organisations. Feeble states unable to sustain themselves, may even make this a part of their state policy, with covert or overt support. The foreign policies of the affected and stable nations have to consider these realities in their decision matrix and, thus, see climate change and the related security consequences together, as cause and effect. It is, therefore, not surprising that the US and other European nations have already started detailed analysis of emerging security situations due to climate change, and their policies – both economic and foreign affairs—are being formulated in this inclusive context.

[7] Lal et al., 1998; Kalra et al., 2003

[8] Aggarwal, 2003

THE SECURITY PROGRESSION

Some of the hesitation that India and others have in securitisation of the climate change debate is also based on hard facts of the problem. The global scenario of incremental and, to an extent, sudden climate change events, does pose a serious human security problem at present. So as the Green House Gases' (GHG) emissions rise due to the developed nations not honouring their commitments under the Kyoto Protocol, and with some developing countries carrying on with business as usual, the ambient earth temperature would increase. This would cause scarcities as outlined above, along with health hazards, loss of bio and marine eco-diversity, causing changes in the earning profile of a vast global population, hence, migration and other similar social impacts. The social impacts would include the consequences of adaptation techniques that countries are adopting for mitigation of climate change. For example, if any state in India like Chhattisgarh or Jharkhand is made to continue with its substantial forest cover in place of industrialisation, for mitigating climate change and for India to meet its forest cover target, it would amount to consciously not allowing alternate land use and the population being deprived of economic development. This scenario would imply that the poor tribals in these states would never see development and when they realise the reason for the same, the consequences would be ominous. The scarcities of resources at the present level have not yet assumed serious proportions. But they have resulted in adversely impacting the quality of life of, and causing misery to, a vast populace, be it in India or the US. These are human security issues which are being faced due to climate change.

At present, there are many lakes in the higher reaches in Bhutan that are formed due to the melting of glaciers. With global warming, the melting has increased to an extent that there is a serious danger of these lakes bursting their natural dams and causing flash floods of catastrophic magnitude.[9] With a worsening of the climate change scenario, the number of such sudden atmospheric events like cyclones and storms would increase. This would exacerbate scarcities of resources, cause large scale misery to people, and

[9] balwois.com/balwois/administration/full_paper/ffp-762.pdf by Dr D Dey

With worsening of the water, land and food situation, not only would neighbouring nations be affected but countries far off would face the heat.

nations would be faced by an increasingly defiant populace; the human security problem outlined above would then degenerate into an internal security problem. With increasing inter- and intra-state migrations, the class distinctions would become fiercer. The earning-a-livelihood scenario would see a sea-change. Water resources would decline to an extent that upper riparian states within India, Pakistan, Bangladesh or China would be loath to sharing water in adequate quantity with the lower riparian states. This would seriously test the respective federal government's authority. Not only water but paucity of land also, due to sea level rise, would cause problems in governance. For example, the divide between tribal (Buddhist) natives and Bengali settlers in the Chittagong Hills of Bangladesh, is due to the paucity of land. This can only become worse with rising sea levels which would inundate the coastal areas of Bangladesh. Its adverse impact would first be felt internally, with the peace accords signed between warring citizens and the government facing serious questions.

The scenarios outlined above have the potential, in timelines that cannot be predicted with any surety, to degenerate into international conflicts. With worsening of the water, land and food situation, not only would neighbouring nations be affected but countries far off would face the heat. Thus, if Bangladesh and Maldives start to send 'climate refugees', some of them would find their way into the prosperous Western countries too. The social fabric in these countries would be severely tested. The Indus Water Treaty between India and Pakistan has withstood three major conflicts. This should not be construed as an extraordinary event as the pressure to renege on the same did not exist due to the availability of adequate quantity of water with the respective countries. However, now the Ravi River has almost been reduced to a mere stream in Lahore and there is pressure on the water systems of the western rivers, including the Indus, due to increase in population. With agriculture being seriously hampered in the two countries due to paucity of water – both in the rivers and underground—the Pakistani media is full of stories of impending desertification. This situation has the potential to deteriorate into an inter-state conflict once the rivers start running dry after the melting of glaciers in the "third pole" – the Tibet Plateau. The rate of melting is increasing in each decade and some of the glaciers are melting at almost 15 m per year. Some glaciers in Himachal Pradesh, the source of the Ravi, have receded by almost 800 m in five years (2006 data recorded by Indian Space Research Organisation glaciologist Mr Anil V. Kulkarni)[10]. Similarly, once the water is actually diverted by China (for its arid north) before entering Assam and it results in drying up of the Brahmaputra, India and Bangladesh would be severely affected. Water is also a source of contention between Israel/ Palestine and India/ Bangladesh, with water sharing being termed as not just. The potential of conflict is, thus, brewing. Similarly, large scale migration of people between countries due to climate change events, which also challenges the ethnic and religious divide, has the potential to again cause international conflicts.

Once the water is actually diverted by China before entering Assam and it results in drying up of the Brahmaputra, India and Bangladesh would be severely affected.

From the above, it is clear that at present, the impact of climate change is limited to the human security issue. However, with the passage of time and if the world community cannot come up with a collaborative answer to mitigation efforts required to halt climate change, the situation would deteriorate to an extent that internal disturbances in the nations would overwhelm the governments. With dwindling resources and more adverse anthropogenic intervention in our environment, the situation is fraught with the danger of further escalating into armed conflict between nations over the distribution of resources.

CLIMATE CHANGE AND THE INDIAN MILITARY

The impact of climate change on India's security as described above would definitely call for the Indian defence forces to incorporate this variable in their

[10] http://archives.digitaltoday.in/indiatoday/20061106/environment2.html

Due to the phase-out of certain ozone depleting chemicals used in military hardware, their management is a challenge that would have to be coped with.

future military planning. Some of the direct impacts of climate change that the Indian military would have to contend with are listed below, in brief.

- The melting of glaciers and global warming would change the logistics of supplies to our forces in Siachin and other higher reaches in Himachal Pradesh, Arunachal Pradesh and Sikkim. Some land routes would be available and some lower Army posts would become better sustainable. However, due to increasing temperatures, the load carrying capacity of our air maintenance aircraft would be adversely affected. This would amount to more airborne resources having to be pitched in.
- The rising sea levels may affect the coastal naval assets in Goa and the Andamans, to name a few, which would have to be suitably relocated.
- Increased desertification would see water shortages in more parts in northwest India. This would have to be adequately catered for in the Army's training and operational planning.
- Due to the phase-out of certain ozone depleting chemicals (Montreal Protocol) used in military hardware, their management is a challenge that would have to be coped with.
- The Indian military would have to have a proper health care programme in place for its personnel and their families as the rise in health hazards caused by sudden climate change events as well as increased vector-borne diseases would have to be factored. This is specially relevant for military personnel as they are called to operate in some of the most inhospitable places in the country and abroad.
- Due to increase in ambient temperatures, the snow melting at the higher reaches would show a change in the pattern. Its implications on the situation across the Line of Control in Jammu and Kashmir (J&K) would need to be studied by the military. These issues are actually being faced presently by the Army.
- Last, but definitely not the least, would be the pressure on the military to cope with encroachments on the land due to the rising influx of poor migrants from

across the borders. This problem is acute in a democratic environment and is actually being faced presently in states like Assam and West Bengal.

EMERGING OPPORTUNITIES: SUSTAINABLE DEVELOPMENT

After learning of the consequences of climate change, it would only be prudent that the global community synergises efforts in mitigating the climate change effects. The oft repeated position, of the 'developed countries, being the real culprits behind climate change due to industrialisation, hence, they should bear the onus of mitigating it', the principle of 'common differentiated responsibility', is fine and accepted. But this should automatically deter other countries (read India, China, Brazil, etc) from following the same unsustainable path towards development. The Brundtland Report, Stern Report and many such documents by the developed countries on sustainable development are mostly prismatic views. The real test of leadership of the emerging economies, like those of the countries mentioned above, lies in charting their own path to showcase their commitments towards a safe and secure climate. There are many opportunities which are available on this path which would ensure that 'business as usual' is not allowed to continue.

An extract from an article published in *The Times of India*, on August 10, 2009, by Mr Yvo de Boer, Executive Secretary, United Nations Framework Convention on Climate Change (UNFCCC) and the force behind the "Bali Action Plan", places the abovementioned line of thinking in the correct perspective:

> Judging by recent media reports, one cannot escape the impression that developing countries are being assailed with demands to accept legally binding GHG emission 'caps'. The fact is that not a single industrialised country is asking major developing countries to accept binding mid-term emission reduction targets. The international community, in drawing up the broad parameters for a climate change deal two years ago, acknowledged that industrialised countries must accept binding emission reduction targets. But developing countries are asked only to **limit growth of emissions in line with sustainable development needs and only if supported through finance and technology from developed countries.**

In effect, this can be interpreted as following:

- India can keep increasing its emissions in line with its development needs but by not following the developed countries' or 'business as usual' model.
- It can lower its dependence on fossil fuel for its energy needs by changing over to cleaner technologies paid for by the developed nations. The developed nations have to show their true commitments on this front if these mitigation techniques are to succeed. The modalities for such finance would require serious negotiations as it is here that the whole model may fall flat.
- The developed nations have to commit on periodic/ short-term verifiable emissions reduction targets, to see if their long-term targets (by 2050) are within the achievable realm.
- According to UN data, millions of new green jobs would be created globally by following these mitigation technologies. A country like India which has a huge base of technology intensive human resource is best placed to take advantage of, and use, this opportunity to match the emerging field of jobs as it did a couple of decades ago in the Information Technology (IT) sector. One estimate is that in India alone, nine lakh and one lakh jobs would be created by 2025 in the biogas and solar photovoltaic sectors respectively.

CONCLUSION

The Hindu philosophy of *Karma* is very apt in this context "Do not only aspire for results but act and only then there would be a result". The time for action is now because tomorrow will be too late. The climate change and security relationship is here to stay and it would be myopic on the part of the security establishment not to take cognisance. The political compulsions of public postures need not deter the establishment from gearing up to the changing security scenario in their backyard. Failing to recognise the conflict and instability implications of climate change and responding by investing in a range of preventive action could be very costly in terms of instability, human lives and retarded development.

INDIA-AFGHANISTAN RELATIONS DURING SOVIET INTERVENTION IN AFGHANISTAN

K.N. TENNYSON

> *No international incident spurted as much diplomatic enterprise in New Delhi as did the Soviet military intervention in Afghanistan. Never before in the history of Indian diplomacy was there so much groping for ideas and directions. Never before was India's foreign policy an act of sterner choice.*
>
> — Bhabani Sen Gupta[1]

The politics of India and its neighbouring countries witnessed unprecedented changes in the late 1970s. On March 24, 1977, India's elected government resigned prematurely due to the political crisis within the ruling Congress Party. Thereby, India suffered unstable coalition politics until Mrs. Indira Gandhi came back to power after an "unprecedented victory" in the January 1980 general election. At the same time, the politics of Pakistan was taken over by the military leader Gen Muhammad Zia-ul-Haq on July 5, 1977, and Martial Law was declared in the state. The changed political scenario in India and Pakistan coincided with the 1979 Islamic revolution in Iran. In the midst of all these developments, the Soviet Union intervened in Afghanistan in December 1979, complicating the volatile political environment in the region.

* **K.N. Tennyson** is an Associate Fellow at the Centre for Air Power Studies, New Delhi.

[1] Bhabani Sen Gupta, *The Afghan Syndrome: How to Live with the Soviet Union* (New Delhi: Vikas Publishing House, 1982), p. 106.

......anyone who controls Afghanistan controls the land routes between the Indian subcontinent, Iran, and resource rich Central Asia. Almost every major power, therefore, wanted a slice of the pie.

Soviet military intervention in Afghanistan marked a turning point in the politics of the region, as it not only brought the Cold War politics to the threshold of the Indian subcontinent but also led to a polarisation of the regional politics. With the Soviet Union taking over the politics of Afghanistan, the US embroiled itself in the regional politics to thwart Soviet infiltration into the oil rich Persian Gulf region. Thus, by the beginning of the 1980s, "the epicenter of world tensions" shifted from "Europe to Asia."[2]

According to Shelton U. Kodikara, the impact of the Soviet action on US foreign policy was immense and threatened vital US interests. These interests revolved largely around the Middle East as "oil is the only economic interest which the US would have to fight for."[3] This fact was clearly highlighted by the then US Special Envoy Clark Clifford to reporters at New Delhi where he said that if the Soviet Union "moves towards the Persian Gulf," the US will not hesitate to prevent Soviet action through military means (war).[4] One of the main reasons why Afghanistan continues to play an important role in the politics of the world is that though geographically Afghanistan does not have any economic value,

> ......anyone who controls Afghanistan, controls the land routes between the Indian subcontinent, Iran, and resource rich Central Asia. Almost every major power, therefore, wanted a slice of the pie. Today, flanked by Iran on the west, Pakistan on the east and the Central Asian Republics of Turkmenistan, Uzbekistan, and Tajikistan in the north (and a very small

[2] Annual Report 1981-82 (India: Ministry of External Affairs) p. iv.

[3] Shelton U. Kodikara, "Role of Extra-Regional Powers and South Asian Security," in Sridhar K. Khatri,ed., *Regional Security in South Asia* (Kathmandu: Centre for Nepal and Asian Studies, Tribhuvan University, 1987), p. 49.

[4] John G. Merriam, "Arms Shipments to the Afghan Resistance," in Grant M. Farr and John G. Merriam, eds., *Afghan Resistance: The Politics of Survival* (Boulder: Westview Press, 1987), p. 75.

stretch of border with China in the northeast), the country's geo-strategic importance has multiplied manifold.[5]

It was in this context that the US began to formulate its policy towards South Asia and the Indian Ocean Region in search of a steadfast ally for establishment of its military bases and facilities. Consequently, the US came in contact with Pakistan because it is strategically located to the north of the Arabian Sea—a strategic entry point to the oil-rich Persian Gulf, where about "80% of oil meant for South-East Asia and the Mediterranean, passes through Pakistan's strategic port of Karachi."[6] Besides, Pakistan is geographically linked to the Soviet Union and Afghanistan.

Agreeing with Selig Harrison, Kaushik adds that it was the outcome of the "American intrigues against the USSR in South-West Asia following the overthrow of the Afghan monarchy by Daoud in 1973."

The above mentioned points vindicate that the fear of Soviet domination of the oil rich Persian Gulf region was the main reason for the US to embroil itself in the Afghan crisis. However, Arvind Gupta points out that the Soviets did not intervene in Afghanistan "owing to the historic drive towards warm water ports of the Indian Ocean" or the Persian Gulf, but to contain the instability in Afghanistan because, according to the Soviet Union, instability in its southern borders—Afghanistan—posed a considerable threat to its own security.[7]

Sharing similar views, Devendra Kaushik is of the opinion that the Soviet military intervention in Afghanistan was not the result of the Soviet "fear of the rise of an Islamic fundamentalist regime in the vicinity of the southern territory of the Soviet Union inhabited by 35 million Muslims (as propagated by some scholars and political analysts) nor the drive towards the warm waters of the Gulf and its rich oil wells."[8] Agreeing with Selig Harrison, he

[5] "Why Afghanistan is Important to India," http://www.rediff.com/news/2005/aug/30spec4.htm

[6] Lawrence Ziring, "Bhutto's Foreign Policy 1972-73," in J. Henry Korson, ed., *Contemporary Problems of Pakistan* (Leiden: E. J.Bill, 1974), p. 65.

[7] Arvind Gupta, "Soviet Military Intervention in Afghanistan in Perspective," in K. Warikoo and Dawa Norbu, eds., *Ethnicity and Politics in Central Asia* (New Delhi: South Asian Publishers, 1992), pp. 281-282.

[8] Devendra Kaushik, "Soviet Union's Pakistan Policy: A Study and Appraisal," in Surendra Chopra, ed., *Perspectives on Pakistan's Foreign Policy* (Amritsar: Guru Nanak Dev University Press, 1983), p. 265.

adds that it was the outcome of the "American intrigues against the USSR in South-West Asia following the overthrow of the Afghan monarchy by Daoud in 1973."[9] This fact was brought out by Leonid Brezhnev in his speech before the voters of the Baumansky Constitution in Moscow on February 22, 1980:

> Absolutely false are also the allegations that the Soviet Union has some expansionist plans with regard to Pakistan, Iran or other countries in that area. The policy and mentality of colonialism are alien to us. We do not covet the lands or wealth of others.[10]

Pakistan's military rulers joined hands with the US not because of its animosity to Soviet policies but because of its increased isolation from the international community.

PAKISTAN'S TREACHEROUS PLOT

Taking advantage of the political developments in the region, "determined efforts" were made by "Pakistan to project the threat from the Soviet intervention in Afghanistan as not only a threat to its security, but also to the free world."[11] Shalini Chawla similarly urges that the Soviet military intervention in Afghanistan "was a major strategic development which Pakistan's defence planners utilised fully to further highlight the threat perception." Quoting Ayesha Siddiqa-Agha, she says, "Pakistan propagated the conventional wisdom that the Soviet Union had intentions of reaching the 'warm water' through Pakistan, after establishing its control over Afghanistan."[12] Subsequently, Pakistan's leaders succeeded in influencing the US policy-makers, as it provided an easy access to the Persian Gulf, Central Asia and the Middle East. Thus, Pakistan ingeniously joined hands with the US and became a frontline state of the US for the containment of Soviet power in the region.

[9] Ibid.

[10] K. Volkov, K. I. Gevorkyan, A. Mikhailenko, Polonsky and V. Svetozarov, *The Truth About Afghanistan: Documents, Facts, Eyewitness Reports* (Moscow: Novosti Press Agency Publishing House, 1980), p. 22.

[11] Aabha Dixit, "India, Pakistan and the Great Powers," in Air Commodore Jasjit Singh, ed., *India and Pakistan: Crisis of Relationship* (New Delhi: Lancer Publishers, 1990), p. 31.

[12] Cited in Shalini Chawla, *Pakistan's Military and Its Strategy* (New Delhi: K W Publishers, 2009), pp. 107-108.

Most intriguing is the fact that Pakistan's military rulers joined hands with the US not because of its animosity to Soviet policies but because of its increased isolation from the international community, thereby, willing to forswear some of its own larger interests in exchange for international legitimacy. Husain Haqqani, citing Pakistan's military leader Brigadier Yousaf wrote that Pakistan's military ruler Gen Zia ul-Haq's motive in agreeing to support the US against the Soviet Union "was not exclusively related to global security," but was more of a plan for its political survival and "Pakistan's traditional policy paradigm of seeking leadership in the Muslim world...and obtaining economic and military assistance." Haqqani further stated:

Pakistan joined hands with the US because the "only possibility of acquiring American military and economic aid" was through converging Pakistan's views with those of the US.

> In 1979, Zia had just provoked worldwide consternation and condemnation by executing his former prime minister [Zulfikar Ali Bhutto]; his image both inside and outside Pakistan was badly tarnished, and he felt isolated. By supporting a *jihad*, albeit unofficially, against a communist superpower, he sought to regain sympathy in the West…[13]

Ayesha Siddiqa-Agha says that Pakistan joined hands with the US because the "only possibility of acquiring American military and economic aid" was through converging Pakistan's views with those of the US.[14] The US offered covert assistance worth about "$ 3.2 billion" in economic and military aid, "which was accepted in 1981, effective for the next five years."[15] Other reports indicate that in the 1980s, the US supplied arms worth about $ 630 million annually to the Mujahideen.[16]

[13] Husain Haqqani, *Pakistan Between Mosque and Military* (Lahore: Vanguard Books, 2005), p. 185.

[14] Ayesha Siddiqa-Agha, *Pakistan's Arms Procurement and Military Buildup, 1979-99* (New York: Palgrave, 2001), p. 14.

[15] Kodikara, n. 3, p. 50.

[16] Mahendra Lama, "The Afghan Refugees," *The Hindu*, February 5, 2002.

This unprecedented militarisation in the region created a serious foreign policy problem for India.

According to Kalim Bahadur, in connivance with the US Central Intelligence Agency (CIA), Pakistan's Inter-Services Intelligence (ISI), was able to mobilise about "35,000 Muslim militants from forty Islamic countries for the war in Afghanistan between 1982-1992."[17] The covert action of America and Pakistan of mobilising Muslim militants to counter the Soviet presence in the region was made easier by the availability of huge numbers of Afghan refugees in Pakistan, said to be around "three million Afghans."[18] Mohammad Amir Rana stated that the CIA provided military training, financial help and armaments to a "huge contingent of Mujahideen" stationed in Pakistan.[19] Besides, the US also deployed the "aircraft carrier *Nimitz* and two nuclear cruisers to the Indian Ocean via the Cape to supplement its naval task forces already stationed in the Persian Gulf area."[20]

This unprecedented militarisation in the region created a serious foreign policy problem for India. The Indian government feared "the risk of converting the subcontinent into a theater of Great Power confrontation and conflicts as well as threaten the security of India," and thus, voiced its concern against "induction of arms into Pakistan" by the US and other countries.[21] J.N. Dixit, former Indian Ambassador to Afghanistan noted:

> Indian Prime Minister Indira Gandhi's reservation about the Soviet intervention in Afghanistan in December 1979 was tempered by the valid perception that this intervention had taken place only because Pakistan and Saudi Arabia, backed by the US, were trying to subvert a critical exercise being undertaken by a segment of Afghan society to transform their country from its semi-medieval predicament into a modern society and stage.[22]

[17] Kalim Bahadur, "US and Islamic Militancy in Pakistan," in Riyaz Punjabi, ed., *USA and the Muslim World Cooperation and Confrontation* (Middlesex: Brunel Academic Publishers, 2004), p. 221.

[18] Mohammad Amir Rana, *The Seeds of Terrorism* (London: New Millennium Publication, 2005), p. 18.

[19] Ibid., p. 18.

[20] Kodikara, n. 3, p. 49.

[21] *Annual Report 1979-80* (India: Ministry of External Affairs), pp. iii-iv.

[22] J.N.Dixit, *India's Foreign Policy 1947-2003* (New Delhi: Picus Books, 2003), p. 137.

India's Ministry of External Affairs (MEA) reports indicate that India's stand on the Afghan issue was guided by the following principles:

- Opposition to all forms of external interference or intervention in the domestic affairs of the countries of the region;
- Opposition to the extension of the quarrels of other countries and the induction of Cold War tensions into the region;
- Respect for the independence, sovereignty, territorial integrity and non-aligned status of the countries of the region; and
- Preference for a negotiated political solution of problems through dialogue among the parties concerned.[23]

Yet, Indian leaders acted cautiously and did not openly condemn the Soviet action. According to Bhabani Sen Gupta, the objectives of India's diplomacy with regard to the Afghan crisis were determined by three fundamental premises in Mrs. Gandhi's strategic thinking:[24]

- The Soviet intervention, though unfortunate and regrettable, was essentially a defensive move to secure the Afghan revolution and defeat US-sponsored efforts to destabilise the international situation;
- For India, far more dangerous than Soviet military presence in Afghanistan would be the rearming of Pakistan by the US and China and the conversion of Pakistan into a Cold War base; and
- In a new Cold War confrontation in which the United States, China and Pakistan joined forces to contain the USSR, India's national and regional interests dictated the pursuit of a single policy: to try to defuse confrontation in the South Asian region by keeping close to the USSR without completely identifying India with Soviet policies and actions.

Brajesh Mishra, India's representative to the United Nations, speaking at the United Nations General Assembly on January 11, 1980, justified Soviet action to the world community by saying:

[23] *Annual Report 1983-84* (India: Ministry of External Affairs), p. 3.

[24] Sen Gupta, n. 1.

> We are against the presence of foreign troops and bases in any country. However, the Soviet government has assured our government that its troops went to Afghanistan first at the request of the Afghan government on December 26, 1979, and repeated by his successor on December 28, 1979…We have no reason to doubt assurances, particularly from a friendly country like the Soviet Union with whom we have many close ties.[25]

However, the Afghans felt let down by India's low key response to the Soviet action. What disheartened the Afghans was that Indian policy-makers, instead of followings its independent foreign policy at the time of the Soviet military intervention, seemed to turn towards the Soviet policy. As a result, some Afghans reacted adversely. The Government of India's apprehension of a raid on the Indian Embassy at Kabul by local Afghans who had reacted adversely to India's stand (in the UN on a resolution calling for withdrawal of Soviet troops) led to additional precautions at the Indian Embassy in Kabul to avoid any untoward incident.[26] Maj Gen Samay Ram, Indian Military Attaché in Afghanistan at the height of the crisis, said that the Afghans were disappointed with the Indian government "for the lack of support when they most needed it and always expressed their feelings though in a guarded manner so as to show no disrespect to our country (India) or us."[27]

As the political crisis in the region deteriorated, the United Nations General Assembly, taking serious note of the political developments in Afghanistan and their implications for international peace and security, in its 7th Plenary Meeting on January 14, 1980, appealed

> ...to all states to respect the sovereignty, territorial integrity, political independence and non-aligned character of Afghanistan and to refrain

[25] Quoted in Dennis Kux, *Estranged Democracies: India and the United States 1941-1991* (New Delhi: Sage Publications, 1993), p. 367.

[26] "Additional Precautions at Indian Embassy," *The Hindu* , January 18, 1980.

[27] Maj Gen Samay Ram, *The New Afghanistan: Pawn of America* (New Delhi: Manas Publications, 2004), p. 17.

> from any interference in the internal affairs of [Afghanistan]. [It also calls] for the immediate, unconditional and total withdrawal of the foreign troops from Afghanistan in order to enable its people to determine their own form of government and choose their economic, political and social systems free from outside intervention, subversion, coercion or constraint of any kind whatsoever.[28]

Similarly, the Organisation of Islamic Countries (OIC), taking a hard stand on the political developments in Afghanistan, in its First Extraordinary Session of the Islamic Conference of Foreign Ministers held at Islamabad in January 1980, passed a resolution strongly condemning the Soviet military aggression. It demanded "immediate and unconditional withdrawal of all Soviet troops stationed on Afghani territories," and suspended Afghanistan from the membership of the organisation. Further, the OIC asked member countries not to recognise the Soviet backed Babrak Karmal regime and to sever all diplomatic relations until a complete withdrawal of Soviet troops from Afghanistan.[29] In view of the gravity of the political developments in Afghanistan on the politics of the region, the Secretary General of the Commonwealth Secretariat, Mr. Shridath S. Ramphal, said that the developments in Afghanistan were not singularly a Commonwealth problem but "in a real and true sense, a global problem."[30]

The Soviet action clearly indicated that though India had cordial relations with the Soviet Union, it did not take India into consideration when it intervened in Afghanistan.

INDIA'S REACTION AND ACTIONS

"When Soviet troops directly intervened in Afghanistan…India was not altogether surprised, but the suddenness of the intervention was unexpected,"

[28] "The Situation in Afghanistan and its Implications for International Peace and Security," General Assembly – Sixth Emergency Special Session Resolutions, ES-6/2, January 14, 1980, http://www.securitycouncilreport.org/atf /cf/ {65BFCF9B -6D27-4E9C-8CD3-CF6E4FF96FF9}/Afgh%2 0ARESES6% 202.pdf

[29] This resolution was passed at the First Extraordinary Session of the Islamic Conference of Foreign Ministers held at Islamabad in January 1980. "First Extraordinary Session of the Islamic Conference of Foreign Ministers," http://www.oic- oci.org/english/conf/fm/All%20 Download/frmex1.htm

[30] Ramphal, "Afghanistan not Regional Problem," *Patriot* (New Delhi), March 29, 1980.

said J.N.Dixit.[31] Dixit's statement was supported by the fact that "[t]he Soviets did not care to inform India of their intervention until 25,000 troops had already moved into Afghanistan."[32] The Soviet action clearly indicated that though India had cordial relations with the Soviet Union, it did not take India into consideration when it intervened in Afghanistan. But, Pakistani policy-makers and scholars, following their age-old antagonistic policy towards India, alleged that India "tacitly" supported the Soviet military incursion into Afghanistan.[33]

The disheartening fact was that the Pakistani leaders and scholars not only refused to entertain India for joint diplomatic efforts to facilitate the withdrawal of Soviet troops from Afghanistan, but also pointlessly perceived the Soviet action as an India-Soviet plot to balkanise Pakistan.

On the contrary, though India and Pakistan differed in their foreign policy objectives, sensing an adverse impact of the deteriorating political situation in Afghanistan on the peace and security of the region, Indian leaders sought Pakistan's help. India, true to its friendship with Afghanistan and adherence to the Panchsheel principles of non-interference and peaceful coexistence, sent Sardar Swaran Singh to Islamabad seeking President Zia ul-Haq's cooperation to bring about an early amicable solution to the Afghan crisis.[34] Reports indicate that on January 10, 1981, the then Indian Ambassador to Pakistan, Natwar Singh, had delivered a letter from Indian Prime Minister Indira Gandhi to President Zia "strongly" urging Zia to normalise the relations between India and Pakistan and to build "an atmosphere of peace and stability, especially in the context of the disturbed situation in Afghanistan and the developmental aspirations of the people of the subcontinent."[35] Regrettably, the Pakistani leader, instead of

[31] Dixit, n. 22, p. 134.

[32] Sen Gupta, n. 1, p. 110.

[33] Basharat Hussain, "Indo-Afghan Relations: Pre-and Post-Taliban Developments," *Regional Studies*, vol. XXII, no.3, Summer 2004, p. 34.

[34] Mahavir Singh, "India's Relations with the USSR and its Successor State, the Russian Federation: More of Continuity Than Change," in Nalini Kant Jha, ed., *India's Foreign Policy in a Changing World* (New Delhi: South Asian Publishers, 2000), p. 92.

[35] J. N. Dixit, *Anatomy of a Flawed Inheritance: Indo-Pak Relations 1970-1994* (Delhi: Konark Publishers, 1985), p. 66.

joining hands with India to bring about an amicable solution to the ongoing political crisis in Afghanistan, refused to cooperate with India. Touquir Hussain a Pakistani writer observed:

> Pakistan was deeply conscious of the power disparity in the [Indian] subcontinent and was actively looking for ways to redress it. The heightened security concerns and [the] need for economic development compelled Pakistan to reach out to the United States, which was trying to promote a strategic alliance of Asian states to check the expanding lines of Soviet influences.[36]

The disheartening fact was that the Pakistani leaders and scholars not only refused to entertain India for joint diplomatic efforts to facilitate the withdrawal of Soviet troops from Afghanistan, but also pointlessly perceived the Soviet action as an India-Soviet plot to balkanise Pakistan, although, the Soviet Union invaded Afghanistan unilaterally, without India's knowledge and India had no role to play.

Since the political environment in the region began to deteriorate further, the leaders of the world began to look towards India seriously as a major regional power. One witnessed many visits of high officials from different countries to India in the post-Soviet intervention period to review the prevailing political crisis in Afghanistan. Clark Clifford, the Special Envoy of the US President, visited India in January 1980. According to Dennis Kux, Clifford specially came to India to allay New Delhi's "concerns about renewed US arms aid to Pakistan and to urge Mrs. Gandhi to use her influence in Moscow to press for a Soviet withdrawal from Afghanistan." Kux added that, on the contrary, Mrs. Gandhi expressed her displeasure with the US for arming Pakistan and blamed other external powers for escalating the political crisis in Afghanistan.[37] French President Valery Giscard d'Estaing also visited India in January 1980 and issued a joint declaration stating:

[36] Touquir Hussain, "US-Pakistan Engagement: The War on Terrorism and Beyond," *Regional Studies*, vol. XXXIV, no. 1, Winter 2005-06, p. 5

[37] Kux, n. 25, pp. 369-370.

> .....inadmissibility of the use of force in international relations, intervention or interference in the internal affairs of sovereign states and the need to prevent further escalation in areas of tensions through states refraining from actions which could intensify Great Power rivalries and revive the Cold war through dangerous arms build-ups which are liable to threaten peace and stability in sensitive regions. It reiterated the need to restore conditions in which independence, sovereignty and territorial integrity of all states could be preserved and the right of their people to freely determine their own destiny without outside interference assured. Finally, it appealed to all states, particularly the most powerful ones, to recognise the gravity of the danger and to exert efforts to avert it.[38]

Later, when the Soviet Union faced stiff resistance from the world community for its defiant action, almost all Russian high officials came to India to seek its support. On February 11, 1980, Russian Foreign Minister Andrei Gromyko visited India and held talks with various Indian leaders, including Prime Minister Indira Gandhi on the prevailing political situation in the region. A joint statement was subsequently issued at the end of Gromyko's visit. However, while the joint statement did not make any specific mention of the prevailing political condition in Afghanistan, it rhetorically stated that the talks "were held in an atmosphere of mutual trust and cordially reviewed the international situation, including the developments in the region and around it."[39] In return, Indian Foreign Minister Narasimha Rao visited Moscow in June 1980. It was reported that "[o]ne of the [main] objectives of [Rao's] trip was to persuade the Soviet Union to withdraw from Afghanistan as soon as possible."[40]

In mid-December 1980, Soviet President Leonid Brezhnev along with a "300-strong delegation" visited India and met various Indian leaders. The then President of India Sanjeeva Reddy once again reiterated India's views and reminded the Soviet President of India's opposition "to any form of intervention, covert or overt, by outside forces in the internal affairs

[38] *Annual Report 1979-80* (India: Ministry of External Affairs) pp. ii-iii.
[39] "Joint Statement," *Asian Recorder*, vol. XXVI, no. 11, March 11-17, 1980, p. 15356.
[40] Dixit, n. 22, p. 139.

of the region." Reddy was also said to have pleaded for the restoration of durable peace through negotiated political solutions ensuring "independence, sovereignty, territorial integrity and non-aligned status of the countries of the region."[41]

President of India Sanjeeva Reddy once again reiterated India's views and reminded the Soviet President of India's opposition "to any form of intervention, covert or overt, by outside forces in the internal affairs of the region."

Yet, the Soviet President ingeniously sidetracked the Afghanistan issue in his talks with the Indian leaders and instead voiced the Soviet concern on the emerging danger in the Persian Gulf and Indian Ocean. The five-point doctrine of peace and security for the Persian Gulf laid down by President Brezhnev in his address to the Indian members of Parliament on December 10, 1980, clearly manifests this point.[42] Astonishingly, the Indo-Soviet joint declaration issued on December 11, 1980, at the end of President Brezhnev's visit, like the previous February 1980 India-Soviet joint statement, only expressed serious concern about "all forms of outside interference in the internal affairs of the countries of South-West Asia," and "made no reference to Afghanistan and glossed over the main point of difference" between Soviet and Indian leaders over the presence of Soviet troops in Afghanistan.[43]

Though the joint declaration consciously did not mention the Soviet intervention, to send a strong message of disapproval of the Soviet action, the Indian government refused to take part in the 10th anniversary celebration of the Indo-Soviet Treaty organised by the Friends of the Soviet Union in 1981 at Moscow.[44] The then Indian Prime Minister Indira Gandhi addressed the Non-Aligned Foreign Ministers' Conference held in New Delhi in February 1981, urging the external powers not to interfere in the politics of the region and to withdrew "their young (military) men back"

[41] "President L. Brezhnev's Visit," *Asian Recorder*, vol. XXVII, no. 2, January 8-14, 1981, p. 15827.

[42] The five-point doctrine of peace and security for the Persian Gulf can be seen in "President L. Brezhnev's Visit," *Asian Recorder*, vol. XXVII, no. 2, January 8-14, 1981, p. 15827.

[43] Text of the "Joint Declaration," can be seen in *Asian Recorder*, vol. XXVII, no. 2, January 8-14, 1981, pp. 15828.

[44] Singh, n. 32, p. 92.

to their country.[45] This indicated an impending *volte face* in India's attitude towards the Soviet Union's policy in the region. This change in Mrs. Gandhi's attitude towards the Soviet Union was surprising because it was alleged by some Indian leaders that Mrs. Gandhi's tilt towards the Soviet Union was so strong that even her "Cabinet personnel have to be approved by Soviet Prime Minister Kosygin."[46] Subsequently, in her keynote address at the 42nd Commonwealth Nations Summit held in Melbourne on September 30, 1981, she once again expressed that India was "gravely concerned over the use of Afghanistan as a pretext for massive external-funded militarisation of its neghbourhood."[47] Further, on August 2, 1982, Mrs. Gandhi in her address at the luncheon hosted by the Foreign Policy Association and the Asia Society, in cooperation with the Far East American Council of Commerce and Industry and the Indian Chamber of Commerce of America at New York, said, "There is no alternative [on the Afghan issue rather than] to a political settlement which will take into account the concerns of all the parties involved." She also vividly brought out India's views on the Soviet military intervention in Afghanistan saying:

> We are against foreign interference, military or otherwise, in any country. It is unfortunate but true that there has been, and is, interference in many developing countries, to which American and other publications have drawn attention. On this or other international matters, we do not lean to one side or another, neither to the so-called East nor West. We judge issues from the Indian point of view and in terms of humankind's right to a peaceful and fuller life.[48]

In the midst of these developments, the United Nation Secretary General (UNSG) Perez de Cuellar visited New Delhi in February 1983

[45] "Non-Aligned Foreign Ministers' Conference," *Asian Recorder*, vol. XXVII, no.11, March 12-18, 1981, pp. 15924-15925.

[46] Kuldip Nayar, *India The Critical Years* (Delhi: Vikas Publications, 1971), p. 3.

[47] "Commonwealth Summit in Melbourne, " *Asian Recorder*, vol. XXVII, no. 45, November 5-11, 1981, p. 16308.

[48] Recorded in Satish Kumar, ed., *Yearbook on India's Foreign Policy 1982-83* (New Delhi: Sage Publications, 1985), p. 223.

and held talks with Indian leaders, including Prime Minister Rajiv Gandhi. Cuellar, was reported to have told Prime Minister Rajiv Gandhi that he was "keeping a close watch on the [political] situation in Afghanistan".[49]

A month later, in March 1983, the Seventh Conference of Heads of the Non-Aligned States was held in New Delhi by mere chance as the conference had been scheduled to be held at Baghdad, "But because of the continuance of the Iran-Iraq War, and more importantly, Iran's opposition to its being held in Baghdad," the venue was shifted to New Delhi from March 7-12, 1983.[50] In New Delhi, besides taking up other important issues, the Heads of the Non-Aligned States reviewed the outcome of the New Delhi Ministerial Conference held in February 1981 and called "for a political settlement on the basis of the territorial integrity and non-aligned status of Afghanistan and strict observance of the principle of non-intervention and non-interference by external powers. They also reaffirmed the right of the Afghan refugees to return to their homes in safety and honour and called for a speedy solution to the vast humanitarian problem."[51]

Numerous regional and international meetings were held and agreements were passed, yet, "[t]he conflict of attrition continued, with increased financial, and military assistance to opposition groups" in Afghanistan. As a result, a mid-term review meeting of the Indo-Afghan Joint Commission was held in Kabul in October 1983.[52] The Heads of State of the Commonwealth Countries "expressed grave concern at the situation in and around Afghanistan and its implications both for the region's peace and stability and for international security."[53] The Communiqué of the Commonwealth Summit held at New Delhi in November 1983 stated:

[49] "UN Keeping Close Watch on Kabul," *The Times of India* (New Delhi), February 28, 1983.

[50] M.S. Rajan, "The Seventh Non-Aligned Summit," in Kumar ed., n. 48, p. 53.

[51] *Supplement to the Annual Report of the Ministry of Eternal Affairs 1982-83* (India: Ministry of External Affairs) p. 5

[52] *Annual Report 1979-80* (India: Ministry of External Affairs), p. 3.

[53] "Commonwealth Summit Communiqué," *Asian Recorder*, vol. XXVII, no. 48, November 26-December 2, 1981, p. 16340.

> Heads of Government continued to be gravely concerned at the situation in and around Afghanistan and its implications both for the region's peace and stability and for international security. [The Commonwealth countries also] called for an urgent search for a negotiated political settlement on the basis of withdrawal of foreign troops and full respect for the independence sovereignty and non-aligned status of Afghanistan and strict observance of the principles of non-intervention and non-interference, which would leave the Afghan people free to determine their own future.[54]

Despite the deterioration of the political situation in the region, Afghanistan-India relations, especially on trade, continued uninterruptedly. The signing of an agreement on February 20, 1984, at Kabul, between the two countries, that envisaged several "measures for expanding and diversifying bilateral trade and for establishing direct operations contacts between the banks of the two countries" with a view to facilitating smoother bilateral trade and technical cooperation operations, being one such example.[55]

One of the reasons binding India and Afghanistan together despite all the problems and crises in the region was the strong sense of affinity between the leaders of the two countries. The Afghan President, Babrak Karmal, was deeply moved by the untimely demise of Indian Prime Minister Indira Gandhi and said that he had "lost an elder sister who had been such a source of strength" to him. The then Chief of the Afghan Intelligence Services (the "KHAD") Dr. Najibullah, expressed anguish over the assassination of Mrs. Gandhi and termed it "a crime." Dr. Najibullah not only called for "justice" on the crime, but went a step further and demanded "decisive and salutatory retribution against those who are determined to destabilise and break up India."[56]

In a significant development, notwithstanding India's strong support to President Babrak Karmal, many Afghans defected and sought political

[54] "Final Communiqué," *Asian Recorder*, vol. XXIX, no. 52, December 24-31, 1983, p. 17528.

[55] Satish Kumar, "India and the World-Trends and Events," in Satish Kumar, ed., *Yearbook on India's Foreign Policy 1983-84* (New Delhi: Sage Publications, 1986), p. 25; "Trade Agreement with India," *Asian Recorder*, vol. XXX, no. 12, March 18-24, 1984, p. 17653.

[56] Quoted in Dixit, n. 35, p. 83.

asylum in India. The United Nations Human Rights Commission (UNHRC) granted "political protection" to three members of the Afghan soccer team, Noor Mohammed Mukhtar, Mohammad Bahadur Alikhail and Farid Ahmed who had defected and sought refuge in India in September 1984.[57] Eight months later, on April 26, 1985, a judge of the Afghan Supreme Court, Mr. Mohammad Yusuf Azmi, too announced his defection on reaching New Delhi.[58]

Indian policy-makers viewed peace and stability in Afghanistan as an important foreign policy objective.

Indian policy-makers viewed peace and stability in Afghanistan as an important foreign policy objective. That was the reason why former Indian Prime Minister Rajiv Gandhi "asserted that India could not remain indifferent to the developments which had brought the confrontation of major powers to its doorstep."[59] Criticising the external powers for jeopardising peace and development in the region, Prime Minister Rajiv Gandhi, in his address at a joint session of the Congress Party in June 1985, said:

> Outside interference and intervention have put in jeopardy the stability, security and progress of the region. We stand for a political settlement in Afghanistan that ensures sovereignty, integrity, independence and non-aligned status, and enables the refugees to return to their homes in safety and honour.[60]

Signifying close relations between the two countries, the Foreign Minister of Afghanistan, Shah Mohammad Dost, and other senior Afghan officials visited India in August 1985 and attended the seventh session of the Indo-Afghan joint committee on economic trade and technical cooperation, held in New Delhi from August 6-8 in 1985.[61] During Shah Mohammad Dost's visit, a cultural exchange programme for 1985-87 between the two

[57] "UNHRC Grants 'Political Protection' to Afghans," *Asian Recorder* , vol. XXX, no. 52, December 23-31, 1984, p. 18098.

[58] "Judge Defects," *Asian Recorder*, vol. XXXI, no. 22, May 28-June 3, 1985, p. 18335.

[59] Satish Kumar, ed., *Yearbook on India's Foreign Policy 1989* (New Delhi: Sage Publications, 1990), p. 31.

[60] Quoted Kodikara, n. 3, p. 50.

[61] *Annual Report 1985-86* (India: Ministry of External Affairs), p. v.

India did not want to "indulge in one-sided criticism of the Soviet Union"; rather, it wanted "non-intervention in Afghanistan by all external forces and the creation of a democratic non-aligned government in Afghanistan."

countries was signed in New Delhi on August 7, 1985. According to the agreement, India agreed to "provide ten scholarships to Afghan nationals for doctoral studies and other fellowships for visiting scholars for training in public cooperation and child development." India also agreed to impart "training to Afghan nationals in repair and preservation of historical monuments and rare manuscripts and also in the field of sports." Further, for the development of education, both the countries agreed to "undertake joint research and teaching programmes" and India agreed to "strengthen the programme of Afghan studies, hold film weeks and supply textbooks."[62]

Technically, India agreed to "assist Afghanistan in the expansion of its health institutions and provide equipment worth Rs.20,00,000," and "setting up a 300-bed maternity hospital and expanding the India aided institute of child health in Kabul," which included "construction of a new surgical ward and a new outpatient department. India will supply every year medicines worth Rs. 2,00,000. India will add 10 more sheds to an industrial estate in Kabul and provide equipment worth Rs. 20,00,000 for a facility."[63]

The top secret documents of the Soviet Union, "Soviet Briefing on the Need to Counter-Balance Yugoslav Endeavors Concerning the Afghan Question in the Non-Aligned Countries," declassified by the American think-tank Woodrow Wilson International Center, reveals that prior to the 25th anniversary of the Bandung Conference, Yugoslavia campaigned with the non-aligned countries to summon a Conference of Foreign Ministers or a session of the Coordination Bureau to discuss the Afghan question at the conference commemorating the 25th anniversary of the Bandung Conference.[64] It was reported that the Yugoslav proposal was rejected by

[62] "Cultural Exchanges with Afghanistan," *Asian Recorder*, vol. XXXI, no. 44, October 29-November 4, 1985, p. 18580.

[63] Ibid.

[64] "Cold War International History Project (CWIHP)," www.CWIHP.org,

India and many other non-aligned members. India refused to entertain the Yugoslav proposal because it was one-sided and as such it did not take into account the role that other countries like the US, Pakistan and Saudi Arabia had played in escalating the crisis in the region. Therefore, India did not want to "indulge in one-sided criticism of the Soviet Union"; rather, it wanted "non-intervention in Afghanistan by all external forces and the creation of a democratic non-aligned government in Afghanistan."[65]

In the light of this background, as the then Chairman of the Non-Aligned Movement (NAM), India Prime Minister Rajiv Gandhi, during his statement in September 1986, did not mention the Afghan issue, while referring to almost all other international problems, including South Africa and Namibia, nuclearisation, Iran and Iraq, Israel and Palestine and South-South cooperation. Rajiv Gandhi strongly condemned the autocratic action of the Pretoria regime in South Africa and called for economic sanctions to weaken it. According to him, "Outside economic sustenance only reinforces Pretoria's intransigence." Therefore, he was of the view that "[s]anctions will compel Pretoria to relent." [66] Further he added:

> The Frontline States [Namibia and South Africa] have been subjected to subversion, economic aggression and armed attack. Their security is jeopardized by a regime which suborns their stability, arms and finances mercenaries, abets puppet rebels, bombs neighbours with impunity, and even invades them with its troops…The actions of the Pretoria regime constitute a clear and present threat to international peace and security, within the meaning of Chapter VII of the United Nations Charter.[67]

Three years earlier, on October 26, 1983, speaking at the 2488th Meeting of the Security Council, the President of the African National Congress similarly called "for the immediate imposition of comprehensive and

[65] Dixit, n. 22, p. 136.

[66] K. Ramamurthy & Dr. Govind Narain Srivastava, eds., *Eight Non-Aligned Summit Harare-1986: Selected Documents* (New Delhi: Indian Institute For Non-Aligned Studies, 1986), p. 10.

[67] Ibid.

mandatory sanctions against the Pretoria regime"[68]

As the political reconciliation began to take place, Afghan Foreign Minister, Abdul Wakil, visited New Delhi at his own initiative on February 7, 1987, and briefed Indian leaders, including Prime Minister Rajiv Gandhi, "on the national reconciliation moves initiated in Afghanistan" and discussed with them the upcoming peace talks on Afghanistan.[69] It was reported that the Indian government "welcomed the initiatives of the Afghanistan government to bring about a national reconciliation" in Afghanistan. Three months later, in May 1987, the Eighth Session of the Indo-Afghan Joint Commission was held in Kabul where "the two countries decided to establish direct banking arrangements, closer cooperation between their trading organizations, and to intensify their industrial cooperation." Besides, India agreed to "set up a cultural centre in the Indian Embassy [in Kabul] to project Indian culture."[70]

India's External Affairs Minister N.D. Tiwari met Afghan Foreign Minister Abdul Wakil on May 3, 1987, and clearly stated "there could be no military solution to the Afghan problem." He reiterated "India's opposition to all kinds of interference and intervention in Afghanistan."[71] Afghan President Najibullah along with Afghan Foreign Minister Abdul Wakil visited New Delhi on December 24, 1987. During the course of the Afghan leaders' visit, the leaders of the two countries analysed the political developments in Afghanistan.[72]

Amidst all these developments, the United Nations General Assembly (UNGA) debated the Afghanistan question at its 41st session and adopted a Resolution by 122 votes to 19 with 11 abstentions. Once again, India abstained on the UNGA resolution but called for an immediate withdrawal of the Soviet military personnel from Afghanistan. India's delegate Shri Vyalar Ravi urged that "the resolution was less than fully constructive and supportive

[68] United Nations Document S/PV. 2488

[69] *Annual Report 1986-87* (India: Ministry of External Affairs), p. 9.

[70] Satish Kumar, "India and the World: Survey of Events," in Satish Kumar, ed., *Yearbook on India's Foreign Policy1987/1988* (New Delhi: Sage Publications, 1988), p. 45.

[71] "Kabul Reconciliation Plan Yields Result," *Hindustan Times* (New Delhi), May 4, 1987.

[72] Kumar, n. 70.

of the efforts being made by the SG and his special representative."[73] Since, the Soviet intervention in Afghanistan, India continuously abstained from the UNGA resolutions condemning the Soviets, because the resolutions did not take into account the flow of arms to the Afghan Mujahideen from the US, Pakistan and other Muslim countries. That is why Mrs. Gandhi said that she "would prefer to see the estimated 100,000 Soviet troops leave [Afghanistan, but, at the same time she] also stressed that as long as outside support to the insurgents continued, conditions would not be conducive for a Soviet withdrawal."[74]

Mr. V.R. Krishna Iyer, former Supreme Court judge, said the Government of Afghanistan is "sincerely pursuing a policy of national reconciliation" and is making several gestures to the Afghan refugees in Pakistan to make them return home. But he was pessimistic about the willingness of Pakistan to allow this to happen and said, "Islamabad had a vested interest in keeping the refugees in Pakistan and is physically obstructing their return because it is getting over $4 billion from the United States on the basis that it is supporting these refugees." Pakistan feared that the flow of funds from the US would stop if the refugees left that country. The US for its part was "unwilling to have the issue disappear."[75]

Soviet Prime Minister N.I. Ryzhkov visited New Delhi in December 1987 and met various Indian leaders, including Indian Prime Minister Rajiv Gandhi and held discussions on various important topics confronting the region. Six agreements were signed dealing with trade, tourism, higher education and training. On Afghanistan, Mr. Ryzkov said that the Soviet Union "was for the withdrawal of a limited contingent of Soviet troops from Afghanistan provided outside interference was stopped."[76]

The year 1987 marked an important event in the history of the region. On July 29, 1987, the Indo-Sri Lanka Accord was signed at Colombo to establish

[73] *Annual Report 1986-87* (India: Ministry of External Affairs), p. 51.

[74] William Claiborne, "Fear Over Afghanistan seen as Factor Pushing Pakistan Toward India," *International Herald Tribune*, November 19, 1982.

[75] "Afghan Government is Earnest about Reconciliation, says Krishna Iyer," *The Hindu* (Madras), April 3, 1987.

[76] "Soviet Prime Minister's Visit," *Asian Recorder*, vol. XXXIV, no. 2, January 8-14, 1988, pp. 19820-19822.

peace and normalcy in Sri Lanka.[77] The agreement was significant because the ethnic conflict in Sri Lanka posed a “formidable challenge” directly or indirectly to India’s security as India had a substantial Tamil population in its southern state. But the accord manifested a serious drawback as the Liberation Tigers of Tamil Eelam (LTTE), with whom Sri Lanka had been at war, was not taken into confidence. Therefore, the peace accord was just an eyewash as it did not bring about any significant changes in the life of the Sri Lankans.[78]

While India was euphoric about the new development in the region, another “major development of considerable concern to India” in May 1987, was the coup in Fiji. Indian concern arose out of the fact that 50 per cent of the population of Fiji is of Indian origin. The Fijian Indians naturally looked towards India for support.[79] What concerned Indian leaders was that while they actively advocated for peace and cooperation in the region, the politics of its neighbouring countries (Fiji, Maldives and Sri Lanka) went through political turbulence, creating serious political and security problems for India.

On February 8, 1988, the Soviet Communist Party General Secretary, Mikhail Gorbachev declared that Soviet troops in Afghanistan would begin withdrawing from May 15, 1988, if the UN sponsored talks between Afghanistan and Pakistan could bring about any amicable solution by March 15, 1988.

THE GENEVA AGREEMENT AND ITS IMPACT ON REGIONAL POLITICS

On January 6, 1988, the UN mediator Diego Cordovez reported about the Soviet Union’s willingness to find an early political solution on the ongoing Afghan crisis. He stated, “The Soviet Union wanted the [proposed upcoming] Geneva round to be the last, and that a withdrawal time-table,

[77] Text of the Indo-Sri-Lanka Peace Agreement to establish peace and normalcy in Sri Lanka can be seen in *Foreign Affairs Record*, July 1987; Satish Kumar, ed., *Yearbook on India’s Foreign Policy 1987/1988* (New Delhi: Sage Publications, 1988), pp. 233-235.

[78] A brief analysis of the development of the signing of the 1987 Indo-Sri Lankan peace accord can be seen in Ibid., pp. 28-40.

[79] Ibid., p. 11.

a time-frame of less than twelve months, would be offered" at Geneva. He also brought out the fear of the Soviet Union that the United States and Pakistan "may bring up the date before agreeing to their half of the bargain—a cut-off of the flow of arms to the Afghan Mujahideen." [80]

A month later, after the reports of the UN mediator Diego Cordovez of Soviet willingness to withdraw from Afghanistan, on February 8, 1988, the Soviet Communist Party General Secretary, Mikhail Gorbachev declared that Soviet troops in Afghanistan would begin withdrawing from May 15, 1988, if the UN sponsored talks between Afghanistan and Pakistan could bring about any amicable solution by March 15, 1988. He acknowledged that the years long "military conflict" in Afghanistan had become "one of the most bitter and painful regional conflicts." Claiming that the Soviet troops would begin withdrawing from Afghanistan, he said:

> Seeking to facilitate a speedy and successful conclusion of the Geneva talks between Afghanistan and Pakistan, the Governments of the USSR and Afghanistan have agreed to set a specific date for beginning the withdrawal of Soviet troops—May 15, 1988—and to complete their withdrawal within 10 months. The date is set based on the assumption that agreements on the settlement would be signed not later than March 15, 1988, and that, accordingly, they would all enter into force simultaneously two months after that. If the agreements are signed before March 15, the withdrawal of troops will, accordingly, begin earlier.[81]

Regrettably, though the Afghan government expressed "its willingness to participate in the trilateral talks with Pakistan and Iran" as early as 1981, and despite "seven rounds of talks that took place between the Foreign Ministers of Afghanistan and Pakistan in Geneva" between 1982 and 1987, peace seem to be a distant dream. What impinged in the successful conclusion of the peace talks was that though the Afghan government was willing to participate in the peace process, "Pakistan refused to recognise the Soviet-backed regime, and

[80] "Soviet Pull-out Plan," *Asian Recorder*, vol. XXXIV, no. 7, February 12-18, 1988, p. 19871.
[81] "Troop Pull-out Deadline," *Asian Recorder*, vol. XXXIV, no. 11, March 11-17, 1988, p. 19915.

Iran insisted that the Mujahideen should be included in the talks."[82]

However, after six years of failed negotiations, a peace accord known as the "Geneva Accord" was signed on April 14, 1988, with the hope to bring peace and stability in Afghanistan. The Geneva Accord, in fact, contains four accords:

- Between the Soviet Union, the United States, Pakistan and Afghanistan on the withdrawal of Soviet forces from Afghanistan.
- Between the United States and the Soviet Union, to guarantee the above.
- Between Pakistan and Afghanistan on non-interference and non-intervention.
- Between Pakistan and Afghanistan on the return of the refugees.

Besides, a separate Memorandum of Understanding on arrangements for monitoring the Soviet withdrawal under UN auspices was also signed.[83] It is an unpleasant reality that the peace process which was initiated by the UN, took such a long time to come to an agreeable conclusion. India's national newspaper, *Patriot*, commenting on why the UN failed to bring about an amicable solution to the ongoing Afghan crisis, wrote, "UN mediators can negotiate when peace is on the agenda but not when war is actively stoked. Because of Pakistan's and the United States' insistence on their right to provide military supplies to Afghan rebels, the authority of the UN has been badly undermined."[84] What was disheartening about the Geneva Accord was that owing to differing foreign policy objectives of the two superpowers, "there was no agreement on the setting up of any coalition government in Kabul."[85] At the same time, like the 1987 India-Sri Lanka peace accord where the LTTE did not take part, the Afghan Mujahideen refused to take part in the signing of the accord. Iran also backed out of "the Geneva deliberations and continued to demand" the

[82] S.K. Shukla, "Prospects in Afghanistan," in Satish Kumar, ed., *Yearbook on India's Foreign Policy, 1989* (New Delhi: Sage Publications, 1990), p. 107.

[83] Research Institute for Peace and Security, Tokyo, *Asian Security 1988-89* (London: Brassey's Defence Publishers, 1988), pp. 50-51.

[84] "What on Durand Line," *Patriot* (New Delhi) March 31, 1989.

[85] n. 83, p. 51.

installation of “a purely Islamic regime at Kabul” manifesting a serious political drawback.[86]

Unfortunately, even before the peace accord could be put into practice on July 25, 1988, Afghanistan expressed its displeasure to the UN of the violation of its terms for the withdrawal of Soviet troops by Pakistan and the US. Afghan Foreign Minister Abdul Wakil in a letter to the UN Secretary General cited “the new wave of ferocious and adventurist actions by extremists linked with the Peshawar-based alliance of seven (rebels groups) who have created appalling tragedies with missile barrages on Kabul.”[87] It may be recalled that the seven Mujahideen groups formed an alliance on May 17, 1987, with an agreement “to establish an elected 230-member council *Shura*.”[88] Nevertheless, despite charges and counter-charges between the Soviet, Pakistan and the US, accusing each other of violating the accord, the Soviets began to withdraw from Afghanistan on May 15, 1988. Finally, on February 15, 1989, Lt. Gen. Boris Gromov of the (Soviet) Red Army contingent, the then Commander-in-Chief of the Soviet troops in Afghanistan, crossed over to the Soviet side, across the bridge on the Amu Darya River, completely withdrawing from Afghanistan, marking a new turning point in the history of Afghan politics.[89]

India welcomed the adoption of the draft resolution at the 43rd General Assembly without vote and without debate. The Prime Minister of India, committing to the principle of peace and stability in the region, sent India’s Foreign Secretary K.P.S. Menon to Islamabad as a special emissary for a discussion on the Afghanistan situation with President Zia and other Pakistani leaders on May 3, 1988. Further, as part of the revival of India’s cooperation programme, in 1988, various economic and cultural programmes were initiated by India in Afghanistan, like preparing a feasibility report on a 300-bed maternity hospital in Kabul by the Hospital Services Consultancy Corporation and the construction of 10 additional industrial sheds at the India aided industrial estate project in Kabul by the Central Public Works

[86] Shukla, n. 82, p. 107.

[87] “Afghanistan Protest Pakistan, US Pact Violations,” *Patriot* (New Delhi) July 27, 1988.

[88] Shukla, n. 82, p. 106.

[89] “Soviet Pull-out Complete,” *Asian Recorder*, vol. XXXV, no. 15, April 9-15, 1989, p. 20519.

Department (CPWD). The Ministry of External Affairs also reported that decisive progress was achieved towards the supply of equipment, for example, medicines worth Rs. 20 lakh per annum and consultancy services for the construction of the Indira Gandhi Institute of Child Health Expansion Project in Kabul, besides setting up of Common Facilities Centres (for small-scale industry) with India's assistance.

The President of Afghanistan, Mohammed Najibullah, visited India from May 4-6, 1988. India pledged assistance worth Rs. 10 crore for the relief and rehabilitation of the Afghan refugees. This was followed by a mid-term review meeting of the Indo-Afghan Joint Commission on Economic, Technical, Trade and Cultural Cooperation, held in Kabul in June 1988.[90] Subsequently, a protocol on cooperation in the field of television between Doordashan (India), the Ministry of Information and Broadcasting, Government of India and the State Committee for Radio, Television and Cinematography of the Republic of Afghanistan was signed on July 22, 1988. As relations between the two countries began to improve considerably, a seven-member troupe from India including Ms. Kaushalaya (Kuchipudi) and Manjushi Chatterjee (Kathak) visited Afghanistan and preformed in various places in Afghanistan from August 11-20, 1988.[91] Abdul Wakil, the Foreign Minister of Afghanistan, visited India from September 1-4, 1988.

In February 1989, the Soviets withdrew completely from Afghanistan. With this, the shadow of colonialism and foreign occupation was temporarily brought to an end in the war-torn state.

The Soviet President, Mikhail Gorbachev, accompanied by his wife Raisa, visited India on November 18, 1988, and met various Indian leaders and discussed the prevailing international developments. The Indian government, in recognition of Soviet President Gorbachev's "bold and imaginative proposal to initiate a positive and practical process of nuclear disarmament: and his vision of a non-violent world free of nuclear weapons",

[90] *Annual Report 1988-89* (India: Ministry of External Affairs), p. viii.

[91] Ibid., p. 8 and p. 86.

awarded him the Indira Gandhi Peace Prize for peace, disarmament and development on November 19, 1988. This award came after the signing of the Geneva Agreement between Afghanistan and Pakistan for the smooth withdrawal of Soviet forces from Afghanistan. During this visit, India and the USSR signed various agreements on long-term cooperation in exploration and use of outer space for peaceful purposes, avoidance of double taxation, financial and technical cooperation. And as a sign of close relations between the two countries, a life-size bronze statue of the Russian poet and revolutionary, Alexander Pushkin, was unveiled at the Rabindra Bhavan in New Delhi on November 20 by the Russian Minister for Culture, V.G. Zakharov. At the end of President Mikhail Gorbachev's visit, a joint statement was issued between the two countries reiterating:

> ....their support for the Geneva Accords on Afghanistan and call for their strict and sincere implementation by all parties concerned. The two countries deplore the obstructionist policy of certain forces which are violating the Accords. They express concern over the continued bloodshed in Afghanistan and affirm that the process of national reconciliation should be encouraged.[92]

In February 1989, the Soviets withdrew completely from Afghanistan. With this, the shadow of colonialism and foreign occupation was temporarily brought to an end in the war-torn state. Subsequently, the then Afghan President, Mohammad Najibullah, declared a state of emergency and took over the affairs of the state to prevent subversive activities in the aftermath of Soviet withdrawal.[93] In the midst of all these developments, the resistance groups formed an Afghan Interim Government in February following a S*hura* that had been convened in Rawalpindi. Foreign Ministers of the Organisation of Islamic Conference (OIC), on March 16, 1989, recognised the interim government formed by the Mujahideen fighting the Soviet backed Kabul government, giving it

[92] For details of Soviet President M. Gorbachev's visit to India, see *Asian Recorder*, vol. XXXIV, no. 52, December 16-22, 1988, pp. 20343-20348.

[93] "Emergency Imposed," Ibid., p. 20520.

the vacant Afghanistan seat. Gulbuddin Hekmatyar, Foreign Minister of the Afghan interim government took the seat at the meeting of the 46-member organisation to sustained applause and cries of "Allahu Akbar."[94]

Indian leaders were in touch with the Government of Afghanistan from the beginning of the Soviet intervention in their pursuit to solve the crisis in Afghanistan. That is why the Afghan leaders sought India's help in the mitigation of the political crisis in their country. On March 3, 1989, Shah Mohammad Dost, then Afghanistan's Ambassador to the UN, in his address to the media at the UN, said, "India is a leading country of the region and has a vital stake in what happens there. It has an important role in ensuring that the problems of the region are resolved." A day later, on May 4, 1989, Afghan President Dr. Najibullah visited India and discussed the Geneva Accord with Indian Prime Minister Rajiv Gandhi and the two countries called for the proper implementation of the Geneva Accord.[95] During the visit, besides the political issues, various other social and economic issues were also discussed by the leaders of the two countries. On the economic front, it was reported that Afghanistan "agreed to enter into a long-term arrangement for the import of packet tea from India," and an agreement for "the supply of 2,000 tonnes of packet tea" was finalised. On September 5, 1989, an agreement "to establish a Joint Business Council" was signed on between the Indian Chambers of Commerce and Industry (FICCI) and the Afghan Chambers of Commerce and Industry "to provide for an institutional framework for augmenting India's trade with Afghanistan."[96]

Regular high level exchange visits between India and Afghanistan continued throughout the 1990s. Abdul Wakil, Foreign Minister of Afghanistan, visited India from June 11-15, 1990, for the meeting of the Indo-Afghan Joint Commission, which was followed by President Najibullah in August 1990. During this visit, an agreement on the prevention of trafficking

[94] "OIC Recognizes Mujahideen Government," *Bangladesh Times* (Dacca) March 17, 1989.

[95] Satish Kumar, ed., *Yearbook on India's Foreign Policy, 1989* (New Delhi: Sage Publications, 1990), p. 31.

[96] A brief analysis of the Afghan President Dr. Najibullah's visit to India is discussed in Ibid., pp. 31-32.

in narcotic drugs and psychotropic substances, cooperation between agricultural institutes, and cultural exchanges were signed between the two countries.[97] The 9th session of the Indo-Afghan Joint Commission was held for two days on June 12 and 13, 1990. A "comprehensive protocol envisaging cooperation in areas ranging from agriculture to commodity assistance and telecommunications" was also reported to have been signed during the meeting.[98] With the reconstruction of Afghanistan as the aim, various new projects like the "construction of a 300-bed gynaecological and obstetrics hospital, additional industrial sheds, cooperation in agriculture, cartography, metreology and tourism" were identified by India for project assistance and supply of equipment to Afghanistan. India also agreed to depute 35 experts to Afghanistan and train 50 nominees.[99]

Lt. Gen. Kamal Matinuddin, then Director of the Institute of Strategic Studies in Islamabad says, "Afghanistan had always looked to India for support, but India's interest in Afghanistan was purely to pincer Pakistan. Now India is on thin ice. Rajiv is forced to support Najibullah, or risk the displeasure of Moscow. But now, he must face the prospect of an Afghanistan which is much closer to Pakistan than to India."[100] Mr. Javed Larinjani, Former Deputy Foreign Minister of Iran and present adviser to the Iranian President, said his country would ensure that "India is never victorious against Pakistan." He claimed that a "hegemonistic India will inevitably threaten Iran's security." This would lead to a "natural joint alignment" of Iran and Pakistan.[101]

CONCLUSION

India since its inception has followed a non-aligned foreign policy. However, owing to the unfavourable geo-political environment in the region, it tilted its foreign policy towards the Soviet Union and has relied on the Soviets

[97] Ibid., p. iv.

[98] Ibid., p. 10.

[99] Ibid., p. 75.

[100] Rehman Rashid, "Kabul-New Bugbear in Indo-Pakistan Ties," *New Straits Times* (Kuala Lumpur), June 15, 1988.

[101] Quoted in "Iran to Ensure Pakistan Victory Against India," *The Times of India*, January 28, 1990.

for its economic and military development for most of its existence. At the same time, due to Pakistan’s antagonistic policy towards India, especially on the Kashmir issue, India also came into contact with the Muslim countries like Afghanistan and Iran. Subsequently, throughout the Cold War period, both India and Afghanistan depended on the Soviet Union.

India’s foreign policy was put to a serious test at the time of the Soviet military intervention in Afghanistan.

India’s foreign policy was put to a serious test at the time of the Soviet military intervention in Afghanistan. It is unfortunate that though India was one of the South Asian countries closest to the Soviet Union, the Soviet did not take India into consideration at the time of the military intervention in Afghanistan. At the same time, India was ignored by the Carter Administration and he“did not consult India before responding to the Soviet action by offering substantial military aid to Pakistan and sending his Defence Secretary, Harold Brown, to Peking to solicit Chinese help in the rearming of Pakistan.”[102] The above fact clearly indicates that when the superpowers’ “interests were at stake, they cared little for the sensitivities of medium powers not committed to their respective alignments.”[103]

J.N. Dixit has noted that even in relations with its neighbouring country, Afghanistan, the policy stance adopted by the Indian leaders, specially Mrs. Indira Gandhi “suffered from a basic flaw which one discerns with the benefit of hindsight.”[104] Afghanistan is one of the closest Muslim countries to India. The convergence of interest between the two countries enabled Indian policy-makers to maintain relations with successive regimes of Afghanistan uninterruptedly. However, one finds that India’s relations with Afghanistan have been shaped less by its own proactive policy and more by the state of Pakistan-Afghanistan relations prior to the Soviet intervention in Afghanistan.

India’s policy towards Afghanistan, as it was during the Soviet intervention, does not witness any significant change. By virtue of its economy, military and geographical location, India has acquired considerable

[102] Sen Gupta, n. 1, p. 110.

[103] Ibid.

[104] Dixit, n. 22, p. 138.

international influence and prestige amongst the countries of the region. Successive Indian leaders have continued to uphold the principles of non-alignment, support for decolonisation and disarmament. Therefore, most of the countries of the world expected India to condemn the Soviet military action. However, while India did not condemn the Soviets openly, successive Indian leaders conveyed their disapproval of the Soviet policy. This attitude of India not only led countries to criticise India for following double standards in its foreign policy objectives, but also disappointed the Afghans.

Brajesh Mishra tried to convince the world community by deliberating at the UN General Assembly on March 11, 1980, that "Soviet troops will be withdrawn when requested to do so by the Afghan government."[105] But, on the contrary, the then Indian Ambassador, J.N. Dixit categorically stated that Russian Ambassador Tabeev had told him in March 1982 that the Soviets had come to Afghanistan "to stay." Dixit further added that Ambassador Tabeev expressed the view that the Soviets "will maintain necessary force levels to keep [Afghanistan] under control; [which the Soviets hope to] achieve by August/September, 1982"[106] This clearly reveals that India's Afghan policy suffered from serious flaws during the Soviet military intervention in Afghanistan.

[105] Quoted in Kux, n. 25, p. 367.

[106] J.N.Dixit, *An Afghan Dairy: Zahir Shah to Taliban* (New Delhi: Konark Publishers, 2000), p. 67.

FORM IV (SEE RULE 8)

Statement about ownership and other particulars about newspaper (Air Power to be published in the first issue every year after the last day of February .*

1. Place of Publication	**New Delhi**
2. Periodicity of its publication	**Quarterly**
3. Printer's Name	**Air Commodore Jasjit Singh (Retd)**
Nationality	**Indian**
(a) Whether a citizen of India?	**Yes**
(b) If a foreigner, the country	**Not Applicable**
of origin Address	**P-284, Arjan Path, Subroto Park,**
	New Delhi 110010
4. Publisher's Name	**Air Commodore Jasjit Singh (Retd)**
Nationality	**Indian**
(a) Whether a citizen of India?	**Yes**
(b) If a foreigner, the country	**Not Applicable**
of origin Address	**P-284, Arjan Path, Subroto Park,**
	New Delhi 110010
5. Editor's Name	**Air Commodore Jasjit Singh (Retd)**
Nationality	**Indian**
(a) Whether a citizen of India?	**Yes**
(b) If a foreigner, the country	**Not Applicable**
of origin Address	**P-284, Arjan Path, Subroto Park,**
	New Delhi 110010
6. Names and addresses of individuals who own (Trust) the newspaper and partners or shareholders holding more than one per cent of the total capital	**Forum for National Security Studies** **P-284, Arjan Path, Subroto Park,** **New Delhi 110010**

I, **Jasjit Singh**, hereby declare that the particulars give above are true to the best of my knowledge and belief.

Date: **March 2010**	**Sd/- Jasjit Singh**
* Journal	Signature of Publisher

RESEARCH FELLOWSHIPS – 2010-2012

Centre for Air Power Studies, New Delhi invites applications from Indian citizens for research fellowships to undertake a 2-year study on Indian defence and aerospace issues, including China's military modernisation and Pakistan's military, at three levels:

(i) **Senior Fellow**, with a Ph.D. and over 5 years research experience or 15 years experience in defence;

(ii) **Research Fellow**, with a Ph.D or 10 years experience in defence; and

(iii) **Associate Fellow** with minimum 3 years experience in research or 5 years experience in defence. Remuneration according to experience and expertise (within the scales of Rs. 14,300-450-22,400; 12,000-375-18,000 and 8,000-275-13,500 respectively).

Applications along with a Project Proposal of not more than 1500 words must be sent to **Director, Centre for Air Power Studies, P-284, Arjan Path, Subroto Park, New Delhi-110 010** not later than **April 30, 2010** by post or Email to diroffice@aerospaceindia.org complete with the bio-data giving full details.

NOTES FOR CONTRIBUTORS

Articles submitted to Air Power Journal should be original contributions and should not be under consideration for any other publication at the same time. If another version of the article is under consideration by another publication, or has been, or will be published elsewhere, authors should clearly indicate this at the time of submission.

Each typescript should be submitted in duplicate. Articles should be typewritten on A4/ Letter paper, on one side only, **double-spaced (including the notes)** and with ample margins. All pages (including those containing only diagrams and tables) should be numbered consecutively.

There is no standard length for articles, but 5,000 to 8,000 words (including notes and references) is a useful target. The article should begin with an indented summary of around 100 words, which should describe the main arguments and conclusions of the article.

Details of the author's institutional affiliations, full address and other contact information should be included on a separate cover sheet. Any acknowledgements should be included on the cover sheet as should a note of the exact length of the article.

All diagrams, charts and graphs should be referred to as figure and consecutively numbered. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text.

Articles should be submitted on high-density 3~ inch virus free disks (IBM PC) in rich text format (RTF) together with **an exactly matching double-spaced hard copy** to facilitate typesetting; notes should be placed at the end of each page. Any diagrams or maps should be copied to a separate disk separately in uncompressed TIF or JPG formats in individual files. These should be prepared in black and white. Tints should be avoided, use open patterns instead. If maps and diagrams cannot be prepared electroni-cally, they should be presented on good quality white paper.

Each disk should be labelled with the journal's name, article title, author's name and software used. It is the author's responsibility to ensure that where copyright materials are included within an article, the permission of the copyright holder has been obtained. Confirmation of this should be included on a separate sheet included with the disk.

Copyright in articles published in ***Air Power*** rests with the publisher.

STYLE

Authors are responsible for ensuring that their manuscripts conform to the journal style. The Editors will not undertake retyping of manuscripts before publication. A guide to style and presentation is obtainable from the publisher.

Current Journal style should be followed closely. Dates in the form January 1, 2000. Use figures for 11 and above. British spellings are to be used. Authors should provide brief biographical details to include institutional affiliation and recent publications for inclusion in About the Contributors. Sub-headings and sub-sub-headings should be unambiguously marked on the copy.

NOTES

Notes should be **double spaced** and numbered consecutively through the article. **The first line of a note must align with subsequent lines. Each note number should be standard size and have a full point**.

a) References to books should give author's name: title of the book (italics); and the place, publisher and date of publication in brackets.
   e.g. 1. Samuel P. Huntington, The Common Defense (NY: Columbia UP, 1961), Ch. 2, pp. 14-18.
b) References to articles in periodicals should give the author's initials and surname, the title of the article in quotation marks, title of the periodical (italics), the number of the volume/issue in Arabic numerals, the date of publication, and the page numbers:
   e.g., Douglas M. Fox, "Congress and the US Military Service Budgets in the Post War Period," Midwest Journal of Political Science, vol. 16, no. 2, May 1971, pp. 382-393.

AIR POWER

Journal of Air Power and Space Studies
Centre for Air Power Studies, P-284, Arjan Path, Subroto Park, New Delhi 110010

AIR POWER

Journal of Air Power and Space Studies
Centre for Air Power Studies, P-284, Arjan Path, Subroto Park, New Delhi 110010

AIR POWER Journal

SUBSCRIPTION FORM

In India

□ **Rs. 275/- per copy**

□ **Rs. 1100/- per annum (4 Issues)**

Overseas

□ **US $ 35 per copy**

□ **US $ 130 per annum (4 Issues)**

PLEASE PRINT

Name...

Complete Address...

....

....

....**Pin** ....**Phone**..................................

Please find enclosed cheque/draft number:................ **dated**...................**drawn on**...**favouring KW Publishers Pvt. Ltd., for** **Rs** **US$** ....

Please mail this form to**: KW Publishers Pvt. Ltd., 4676/21, Ansari Road,
Daryaganj New Delhi 110 002 T: +91.11.23263498 / 43528107
E: mail@kwpub.in / knowledgeworld@vsnl.net W: www.kwpub.in**

AIR POWER Journal

SUBSCRIPTION FORM

In India

□ Rs. 275/- per copy

□ Rs. 1100/- per annum (4 Issues)

Overseas

□ US $ 35 per copy

□ US $ 130 per annum (4 Issues)

PLEASE PRINT

Name...

Complete Address...

....

....

....Pin ....Phone..................................

Please find enclosed cheque/draft number:................ dated...................drawn on...favouring KW Publishers Pvt. Ltd., for Rs US$ ....

Please mail this form to: KW Publishers Pvt. Ltd., 4676/21, Ansari Road,
Daryaganj New Delhi 110 002 T: +91.11.23263498 / 43528107
E: mail@kwpub.in / knowledgeworld@vsnl.net W: www.kwpub.in