AIR POWER

Journal of Air Power and Space Studies

Vol. 8 No. 3, Monsoon 2013 (July-September)

AIR POWER

CENTRE FOR AIR POWER STUDIES

New Delhi

AIR POWER is published quarterly by the Forum for National Security Studies for Centre for Air Power Studies, 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 Marshal **Vinod Patney**, SYSM PVSM AVSM VrC, (Retd)
Consulting Editor Lt Col **R Ghose**, SM (Retd)
Distributor KW Publishers Pvt. Ltd.

All correspondence may be addressed to

Editor-in-Chief
AIR POWER
Arjan Path, Subroto Park, New Delhi 110 010
Telephone: (91.11) 25699131-32 Fax: (91.11) 25682533
e-mail: diroffice@aerospaceindia.org
capsnetdroff@gmail.com
website: www.centreforairpowerstudies.com
www.centreforairpowerstudies.in
www.centreforairpowerstudies.org
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 Marshal Vinod Patney (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 Marshal Vinod Patney (Retd).

RNI REGN No. DELENG/2006/18450

CONTENTS

Vol. 8 No. 3, Monsoon 2013 (July-September)

EDITOR'S NOTE

This is the first issue of the *Air Power* journal that is being published after the sad demise of Air Cmde Jasjit Singh, the founder Director of the Centre for Air Power Studies. Single-handedly, he nurtured the Centre and has left it with an enviable reputation. No praise is adequate to describe the sterling work done by him.

Those of us who succeed him can only hope to maintain the high standards set by him and, in his memory, take the Centre to greater heights. The Centre will always be associated with his name. One project that was close to his heart was the publication of the *Air Power* journal and we hope to ensure its continuation, both in frequency of issue and the quality of its contents. The support of all our readers is solicited.

It is but appropriate that the first article in the current journal describes its launch so many years ago and the role of Air Cmde Jasjit Singh in starting the journal.

Also included in this issue is an article on the likely consequences of Pakistan's slide into *jihad*; and an examination of what India's strategy should be towards the all important aspect of cyber warfare. Tibet will always remain an important subject of study and the article in this issue examines the geo-political aspects. Also, there is an article on the Indian aerospace industry, and an article that studies the impact of the Arctic from an Asian viewpoint.

Happy reading.

LAUNCH OF AIR POWER JOURNAL *(IN RETROSPECT)*

D.C. BAKSHI

The Centre for Air Power Studies (CAPS) was initially housed in a DDA flat. It had limited financial resources, but was powered by the indefatigable zeal of Air Cmde Jasjit Singh. During briefings, Air Cmde Jasjit Singh often

Group Captain **D.C. Bakshi** VSM (Retd) was the Managing Editor of Air Power Journal at the time of its launch in 2004.

expressed his keenness to start a professional journal exclusively for 'air' and 'space'. However, shortage of funds came in the way: we looked for patrons for grants, advertisements and sponsorships. Shri Mukerjee and myself, two of his 'obedient' staff members provided a helping hand, while Air Cmde Jasjit Singh continued to labour hard to fulfill his cherished dream of setting up CAPS. A dedicated professional journal was the corollary of the project which he pursued with the same vigour.

Shri J.R. Nanda, Chief Executive Officer of AVI-OIL, known for his patronage for defence cause (s) came to our rescue when he offered to insert quarterly advertisements in the journal. This would enable us to make an initial breakthrough. I was appointed the first Managing Editor of *Air Power Journal*.

During a brief function at India International Centre, on October 4, 2009, Air Cmde Jasjit Singh, at his wittiest, stated that "it was his crazy dream during the last 30 years to have a journal entirely dedicated to air power. This dream has finally seen its fruition." He further added, "It is probably the only journal of its kind in East/West of Suez".

The release of the *Journal* by Marshal of the Air Force, Arjan Singh, DFC, was of a special significance, since it was dedicated to the legendary hero of the Indian skies, Air Mshl Subroto Mukerjee.

Shri M.K. Rasgotra (former Foreign Secretary) who had chaired the session, cited the dominant role of air power in Kosovo, the two Gulf wars, and in Afghanistan. During these conflicts, air power had played a decisive role and it was proved in ample measure that no war could be won without it.

Shri Inder Malhotra, a profound scholar of politico-military affairs, gave interesting insights from a wide canvas of 30 years of media coverage. Air Chief Mshl S. Krishnaswamy, the then Chief of the Air Staff, had graced the occasion. The distinguished members of the audience who applauded the launch of the *Journal* included Lt. Gen. A.M. Vohra (Retd), Adm Hiranandani (Retd), Air Mshl Vinod Patney (Retd) and Brig Gurmeet Kanwal.

It was on this occasion that Marshal of the Air Force Arjan Singh, DFC, briefly touched upon the subject of "non-participation" (in an offensive

role) of the Indian Air Force (IAF) during the 1962 India-China War. He exhorted the Centre to undertake critical 'stock-taking' of such episodes for benefit in the future. Citing the centuries old *mantra* of gaining an edge against the enemy, the Marshal advised, "One should not only know one's own strengths and weaknesses but those of the enemy as well." Academic inputs by scholars and strategists through *Air Power Journal* were expected to provide sound back-ups.

Former Chief of the Air Staff Air Chief Mshl O.P. Mehra, the patron of CAPS, was of the firm opinion that the R&D sector needed strengthening; he strongly recommended setting-up an Aeronautical Commission to deal with the entire gamut of the aviation sector.

On October 4, 2013, *Air Power Journal* enters the 10th year of its publication. May this enduring legacy of Air Cmde Jasjit Singh continue for years!!

PAKISTAN'S IDEOLOGICAL SLIDE INTO *JIHAD*: CONSEQUENCES AND PROSPECTS

SHALINI CHAWLA

Pakistan has been in existence for more than six decades but the state has not been able to define its identity till date. Pakistan has been a nation of contradictions; it has shared an ambiguous relationship with Islam, tried to embrace Western notions of modernity, and, at the same time, tried retaining the orthodox Islamic identity, has an overpowering and ambitious army which has ruled the nation for more than 30 years directly, and nearly an equal period with a civilian façade, but has still struggled periodically to go back to the democratic order controlled by the fractured political leadership and has suffered a deep national identity crisis. Lack of identity has encouraged the rise of ethnicity and pluralism within the Pakistani society. Born as a result of the demand for a separate Muslim homeland, it eventually stood as the saviour of Islam and, in the process, the military led state has adopted policies based on religion which have had severe repercussions for the state. Religion has been used in Pakistan for a range of issues from nation-building to strategic security.

Pakistan has shared a varying relationship with Islam and presently is experiencing Islamist extremism in the most violent form. It has become the breeding ground for terrorism and the extremist elements

Dr **Shalini Chawla** is a Senior Fellow at the Centre for Air Power Studies, New Delhi.

Religion has been used in Pakistan for a range of issues from nation-building to strategic security.

within Pakistan are on a much stronger footing than ever before, posing a threat to the country's very existence. Pakistan's involvement in the war on terror post 9/11, has further facilitated the blossoming of the terrorist network, not only on the frontier boundaries of Pakistan, but also in the heart of the state where the extremist elements have managed to penetrate even the Army Headquarters (HQ), the most secure place in Pakistan, and various air force and naval bases. The liberal thinking finds survival extremely challenging which is exemplified by the assassinations of Punjab Governor Salman Taseer, who tried to oppose the blasphemy law, and *Asia Times* journalist Salman Shahzad, who tried to disclose the links between the terrorists and the military. But one has to ask the question: did Pakistan fall prey to extremism just as the result of its involvement in the war on terror? The answer is clearly 'no'. Pakistan today, is actually facing the consequences of its own policies which it has believed in, and pursued, for the last five decades. Pakistan's reliance on terrorism as a foreign policy tool is, indeed, responsible for its drift into extremism. This paper attempts to study Pakistan's journey towards the present state of extremism, which the Pakistani leadership is unable to control, posing the most alarming challenge to the stability of the country.

BACKGROUND

Pakistan was born as the result of the demand for a separate homeland for the Muslims of India. The All India Muslim League, led by Mohammad Ali Jinnah strongly argued that Muslims had a special identity which would not be able to survive in a Hindu dominated society, thus, a separate homeland for Muslims was the only solution. But Jinnah's dream was quite different from what Pakistan actually transformed into. There was a lack of consensus over Pakistan's ideological and territorial contours, as Ayesha Jalal has rightly pointed out:

> Jinnah's resort to religion was not an ideology to which he was ever committed or even a device to use against rival communities; it was simply a way of giving a semblance of unity and solidarity to his divided Muslim constituents. Jinnah needed a demand that was specifically ambiguous and imprecise to command general support, something specifically Muslim, though unspecific in every other respect. [1]

Pakistan hardly became a beneficiary of a committed and visionary leadership. The state was driven differently by different regimes following different objectives.

Jinnah in his famous speech before the Constituent Assembly on August 11, 1947 outlined his secular vision:

> You are free; you are free to go to your temples, you are free to go to your mosques or to any other place of worship in this state of Pakistan. You may belong to any religion or caste or creed—that has nothing to do with the business of the state….We are starting with this fundamental principle that we are all citizens and equal citizens of one state…In the course of time, Hindus would cease to be Hindus and Muslims would cease to be Muslims, not in the religious sense, because that is the personal faith of each individual, but in the political sense as citizens of the state".[2]

Jinnah's dream was a secular state where the Muslim culture and social norms could be promoted. Jinnah's vision was the outcome of a different set of circumstances where, on the post-colonial movement, he visualised an arrangement for the Indian Muslims who could be free in an independent state. The Muslim League was looking for a Muslim homeland and the thought at the time of conceptualisation of Pakistan, if at all considered, was liberal Islam. But, Pakistan, over the decades, completely drifted away from Jinnah's spirit. It never inherited a uniformed vision and there were contesting ideas, thus, the birth of the nation itself suffered from lack of

1. Ayesha Jalal, *The State of Martial Rule* (Cambridge: Cambridge University Press, 1990), p. 16.
2. *Quaid-i-Azam Mohammad Ali Jinnah's Speeches as Governor-General of Pakistan1947-48* (Karachi: Government of Pakistan, 1964).

consensus and clarity on the issue of Islam. In the coming years, Pakistan hardly became a beneficiary of a committed and visionary leadership. The state was driven differently by different regimes following different objectives. Jinnah passed away on October 11, 1948, and this was indeed a deadly blow to the spirit of Pakistan, and hardly anyone would disagree that his death altered the course of history.

Many of Pakistan's political elites were uncertain about the role of Islam in defining the nation's constitutional foundations. [3] It took the policy makers close to a decade to formalise the Constitution of Pakistan which dissolved Jinnah's spirit of secular Islam. There was clear lack of consensus on the meaning of Islam. Farzana Shaikh puts it very aptly:

> While Jinnah's political successors, plagued by uncertainty about the public role of religion, were content to acknowledge Islam as a fundamental component of the country's identity, religious parties pressed for Islam to be embodied in an Islamic state — although they were too notoriously vague about what that entailed. [4]

This confusion about the interpretation of Islam had severe political, social, economic, educational and even military ramifications. The persistent confusion and lack of consensus gave the political and military leadership enough space to exploit the factor of religion to serve their own interests.

After independence, the most daunting task for the Pakistani leadership was to secure Pakistan from internal and external threats. Internally, Pakistan was fragmented and the two wings, West Pakistan and East Pakistan, which differed ethnically, culturally, and economically, were separated by thousand of miles of Indian territory. Pakistan faced not only the issue of East Pakistan, but also experienced insurgency in Balochistan in the 1940s itself. The Balochis were resistant to the idea of being part of Pakistan and, thus, their incorporation into the federal government has consistently remained a challenge. The Frontier Province also was opposed to the idea of

3. Farzana Shaikh, *Making Sense of Pakistan* (London: Foundation Books, 2009), p. 5.
4. Ibid., p. 5.

being a part of the Pakistani state. Along with these internal vulnerabilities was the perceived threat from India, which the Pakistanis suspected had hegemonic ambitions, and had been unfair in providing Pakistan with its due share of resources inherited from British India. Hostility against India was the leading factor which obviously exaggerated with Pakistan's internal struggles.

THE BEGINNING OF THE IDEOLOGICAL DRIFT AND PAKISTAN'S WAR FOR KASHMIR

The factor of religion became one of the most critical in Pakistan's strategic security.

The need to control Jammu and Kashmir (J&K) and incorporate it into Pakistan was felt very strongly in Pakistan even since the British declaration of India's partition. Kashmir was not only considered indispensable for Pakistan but what was more important for the Pakistani leadership was that it should not be a part of the Indian territory. The prime reasons for Pakistan's quest for J&K were economic and strategic factors. The first was that Pakistan felt that with J&K state as an integral part of India, Pakistan's security would be jeopardised. The major fear was that India would establish its military forces anywhere within a few miles of the 200-km-long vital road and rail route between Lahore and Rawalpindi. Geographically, most of West Punjab's prominent cities lie close to J&K's western border. Considering that Punjabi elites dominated Pakistan's decision-making, this factor of vulnerability weighed heavily on their minds. The second factor was economic and psychological. Kashmir going to India could seriously impact Pakistan's economy which was based mainly on canal irrigated agriculture. West Punjab particularly depended for its agriculture upon the rivers flowing from Jammu and Kashmir. Given the security and economic concerns, Kashmir for Pakistan was seen as a necessity and not just desirability. But this in no way denies that the issue of religion too was important for the Pakistanis in shaping their attitude towards Kashmir. Pakistan's demand for Kashmir was also due to the frustration of the political leaders who felt cheated with a "moth-eaten" Pakistan which

came into their share. Thus, the desire to expand the boundaries and have a Muslim majority state added to the geo-economic concerns in Pakistan.

Pakistan launched the first war for Kashmir in 1947-48 in the name of a 'tribal revolt'. The Pakistan Army, with the consent of the political leadership, invoked the tribesmen and the retired and serving army officers in the name of *jihad*, to raid and seize Kashmir. Islam was leveraged in the very beginning to respond to the Indian threat. The government in Pakistan called on religious scholars to issue supportive *fatwas* (religious decrees).[5] The importance of the 1947-48 aggression was that it laid the basic guidelines for the future aggression by Pakistan. This was the beginning of the use of religion to forward the state polices and also conduct covert operations backed by full-fledged support by the military.

Internally, Jinnah's dream of a pluralistic society was being challenged and in the early 1950s, there were street protests calling for a declaration that the Ahmedis were non-Muslims.[6] The protests were orchestrated in part to destabilise the ruling polity, and the resignation of Pakistan's first Foreign Minister, Sir Zafarullah Khan, an Ahmadi, was demanded.[7] In 1974, Ahmadis were officially declared non-Muslims through a constitutional amendment. On similar lines, in 1965, during the first indirect presidential elections held under Ayub Khan, opposition was raised against Fatima Jinnah, the sister of Mohammad Ali Jinnah for contesting for power, and a *fatwa* was issued declaring that Islam did not allow a female head of state.[8] Thus, religion became an important factor for the political groups to lead in the power struggle. Unequal rights on the basis of sect and gender became prevalent.

On the external front, the Pakistan Army's covert activities expanded in Jammu and Kashmir after the 1962 India-China War. A close study of the covert activities indicates that the factor of religion started to gain momentum in the 1960s. Pakistan's covert activities in Kashmir were now

5. Ziad Haider, "Ideological Adrift", in Maleeha Lodhi, ed., *Pakistan Beyond the Crisis State* (New Delhi: Rupa Publications, 2011), p. 116.
6. Ahmedis are followers of an alleged 19th century messiah called Mirza Ghulam Ahmed.
7. Haider, n. 5, p. 116.
8. Ibid., p. 117.

gradually moving towards using religion as a driving force to gain support for the disintegration of India.

Pakistan's military and political leadership were more and more convinced about the indispensability of covert warfare in their religiously driven strategies.

Another development in the late 1950s and in the 1960s was Pakistan's entry into a Cold War alliance with the United States. Pakistan entered into military agreements with the US and started to receive massive military aid. The US alliance provided the Pakistanis with high technology weaponry for their army, air force and navy. This added to their aggressive instincts to acquire Kashmir. The military establishment and rule was further strengthened in Pakistan with the US assistance and it gave its military great confidence to carry on its covert war in Kashmir.

In the 1950s, Pakistan's covert operations in Kashmir Valley did not yield results and were adding to frustration and impatience in the country, even leading to the military officers' Rawalpindi conspiracy against the civilian government. In 1964, Pakistan developed a strategy that came to be known as Operations Gibraltar and Grand Slam, which were landmarks in the history of both the nations. By this time, the initial reasons for annexing Kashmir had ceased to exist: the first factor of insecurity, due to the presence of the Indian Army on the western border, was solved as a result of the ceasefire agreement in 1949. The second factor, regarding the waters of rivers which originated from Kashmir was also solved with the Indus Water Treaty signed in 1960 through the good offices of the World Bank, during Ayub Khan's regime.

Operation Gibraltar was a covert operation but achieved little success as Pakistani preparations were not in place and it did not get the expected support from the Kashmiris. Soon after the launching of Operation Gibraltar, on August 10, a body called the Revolutionary Council was formed in Kashmir, calling on the people to join hands in the revolt against the illegitimate occupants of the Valley – India. Pakistan's failure in 1965 to achieve its objectives increased its reliance on religion to achieve its

Islam lost meaning as a unifying factor, as the socio-economic factor had a significant contribution in increasing alienation in the Eastern wing.

objectives in Kashmir. In the late 1960s, a new set of *jihadis* emerged, deriving their inspiration from left wing anti-imperialist struggles. Pakistan's military and political leadership were more and more convinced about the indispensability of covert warfare in their religiously driven strategies towards Jammu and Kashmir. This new outfit was named 'Al Fatah' and it received clear instructions from Pakistan to launch intense attacks on government offices, banks, etc in Jammu and Kashmir. The outfit believed in using more aggressive means as compared to its earlier counterpart to attain its objective of creating unrest and terror in the Valley. The defeat of its aggression in 1965 only added to Pakistan's tilt toward Islamic ideology.

1971: DISMEMBERMENT OF PAKISTAN

In the late 1950s and early 1960s, Pakistan witnessed the rising image of the military in the eyes of the people. Gen Ayub's era, in fact, marked the beginning of military control in the political and civil system of Pakistan. This was important as it eventually led to the splitting up of Pakistan. Ayub's successor Gen Yahya Khan, talked about the Islamic identity of Pakistan and kept defence at the top of its agenda. Yahya Khan, utilised the intelligence agencies to motivate the Islamic parties to work against the two major political parties, the Awami League and the Pakistan's People's Party (PPP). These parties were accused of being unIslamic. The military regime had close ties with the Jamaat-e-Islami and also encouraged the mushrooming of other Islamic groups. [9]

In the 1960s, the military's role expanded and also, political and ethnic tensions increased. The two wings of Pakistan, West and East, were undoubtedly very different. The only common factors between the two wings were *Islam* and *fear of India.* The central leadership could have utilised this for the country's integration and to build goodwill between

9. Ibid., p. 118.

the two parts. But the political parties and leadership struggled with their own weaknesses, failed to rise above provincialism, and exploited religion for power politics.[10] Islam lost meaning as a unifying factor, as the socio-economic factor had a significant contribution in increasing alienation in the Eastern wing.

Shortly after partition, Mountbatten had predicted that East Pakistan would break away from Pakistan within a quarter of a century.[11] The Bengalis may have been Muslims but they had a distinct identity of their own—they had a different culture and language which they cherished and respected. Unfortunately, the West Pakistanis never valued or respected this identity of East Pakistan and what was more painful for the East was the discriminating attitude of the Punjabis who considered themselves a superior class. The tensions in the Eastern wing resulted in an insurgency and Pakistan's third war with India. Like the previous wars in 1947-48 and 1965, religion was used as a factor of motivation. During the war, Lt. Gen. Tikka Khan, drawing from Sir Mohammed Iqbal, exhorted the troops: "Allah, exalts the *mujahid* whether he lives or dies. He is a *ghazi* (crusader) if he lives, and a *shaheed* (martyr) if he dies. The *mujahid* seeks Allah's grace. He does not covet wealth and property."[12]

Even Yahya Khan, the Commander-in-Chief and President of Pakistan, boosted the soldiers by saying that that they (Pakistan Army) were fighting the anti-Islamic *Kaffir* army and were upholding the highest traditions of *Mujahideen* – soldiers of Islam.[13]

What was most critical was the evolution of Pakistan's grand strategy after the 1971 War. The grand strategy incorporated two important objectives which decided the future course of action for the Pakistani leadership.

First, to expand territory eastward (take Kashmir). This implied a rise in covert activities in J&K and added emphasis on radical Islam in the name

10. Safdar Mehmood, *Pakistan Divided* (New Delhi: Alpha Bravo, 1983), p. 5.
11. Larry Collins and Dominique Lapierre, *Freedom at Midnight* (London: Harper Collins, 1997), p.159.
12. Quoted in unpublished manuscript, p.217, as cited in Stephen P. Cohen, *The Pakistan Army 1998 Edition* (Karachi: Oxford University Press, 1998), p. 87.
13. Ibid.

of *jihad*. Thus, terrorism was to be adopted as a foreign policy tool.

Second, to expand control westward (to gain leverage in Kabul). This implied creating strategic depth in Afghanistan and also facilitating a Pakistan friendly governance.

GLOBAL RISE OF ISLAMIC IDEOLOGY IN THE 1970s AND 1980s

The 1970s and 1980s witnessed the reemergence of Islam as a potent global force, starting with the spread of the Saudi Wahhabi ideology. The Iranian revolution had shattered the secular basis of nationalist thinking and expectations of modernisation and development theories. The revolution drew attention to the significant changes that were taking place in many Muslim countries across the globe in the 1970s. Ironically, the revival of the Islamic ideology was most prominent in the societies which were modern or in the process of modernisation, possessing a well-trained, Western oriented, secular elite, for example, countries like Egypt, Lebanon, Tunisia, Turkey and Algeria.

In Egypt and Malaysia, the resurgence of Islam was manifested in people's lives, the conventional religious beliefs and also the state politics. Religion came much more into practice and was reflected in the form of daily prayers, fasting and the way people dressed. Spiritualism was emphasised with the revitalisation of an Islamic ideology. Muslim rulers put stress on Islamic identity to gain legitimacy, and Islamic organisations and symbols assumed paramount importance for the state.

Bhutto's turning towards Islam has to be studied in the context of the developments worldwide. He turned towards Islam to counter his Islamic critics and also to strengthen ties with the oil-rich nations of the Arabian Gulf. Thus, Islam in the 1970s and 1980s was used as a source of protest and opposition and also to legitimise seizure of power. Ironically, it was the same Islamic ideology which was used by Zia to overthrow Bhutto.

BHUTTO'S ISLAMIC SOCIALISM

The idea of an Islamic Pakistan was pronounced by Bhutto and then subsequently nurtured and developed by Zia, who used religion aggressively in controlling

the state. Bhutto took forward the idea of *Islamic Socialism* and thus, enforced Islam as a major factor in statecraft. Stephen Cohen points out, "If the Pakistan movement and the first twenty-five years of the history of Pakistan can be characterized as a struggle to turn Indian Muslims into Pakistanis, the years since 1972 have been an extension of the process; a struggle to turn Pakistanis into good Muslims."[14] Bhutto's Islamic socialism was considered insincere and it was seen more to establish the non-Indian identity of Pakistan.[15] Zia put the state at the service of Islam and took steps to inculcate the Islamic practices within the state by banning alcohol and gambling, and declaring Friday as a non-working day. In 1976, Bhutto had appointed Zia-ul-Haq as the new Army Chief and allocated him the responsibility to Islamise the Pakistan Army. It was during this period that "*Jihad*" was included in the motto for the Pakistan Army apart from "*Iman*" and "*Taqwa*".

THE QURANIC CONCEPT OF WAR

Bhutto's active plan for the Islamisation of Pakistan has been supported by the interpretations of the teachings of the Holy Quran. Although Jinnah believed that Pakistan would be able to grow into a big power because of it being a Muslim state, there had been no serious strategy that the nation followed based on Islam. Eventually, in Pakistan, the Quran has been interpreted to develop Pakistan's doctrine and strategy of war through terrorism.

The most comprehensive and precise study on war doctrine and strategy in the context of the Holy Quran has been by Brig S.K. Malik in his book, *The Quranic Concept of War*. Brig Malik interprets that "the Holy Quran has given a comprehensive treatment to its concept of war" and "determines all aspects of the use of 'force' in inter-state relations."[16] Brig Malik regards the Quranic philosophy of war as supreme, which provides directions for the initiation, planning and control of war. According to his interpretation, the very "initiation of war is for the Cause of God" and *jihad* is the "most glorious word in the vocabulary of Islam".

14. Cohen, n. 12, p. 89.
15. See, Stephen Cohen, *The Idea of Pakistan* (New York: Oxford University Press, 2005), p.170.
16. Brig S.K. Malik, *The Quranic Concept of War* (New Delhi: Himalayan Books, 1986), p. 1.

Gen Zia systematically reinforced the *Islamisation of Pakistan* which was propagated by his predecessor.

Terror, according to the author and a majority of the Pakistani military officers is central to the war strategy. Use of terror as an instrument to impose your will and decisions on the enemy has been legitimised citing examples from the Holy Quran and arriving at the conclusion that "when God wishes to impose His will upon his enemies, He chooses to do so by casting terror in their hearts".[17]

The Islamic concept as derived from the Holy Quran by Brig Malik relies on the use of terror in the preparation stages of the war in order to assure victory and achieve direct results.[18] Thus, terror has been legitimised in the Islamic ideology which has till today shaped the military strategy of Pakistan. Brig Malik asserts that "terror struck into the hearts of the enemies is not only a means, it is the end in itself."[19] It is emphasised that *fear* has to be an important part of the preparation for war and it determines that "the test of utmost preparation lies in our capability to instill terror into the hearts of the enemies"[20]

The Quranic interpretation of the conduct of modern war legitimises *jihad* and the use of terror. One of the most effective modes of generating terror is through *covert warfare*, thus, creating physical and mental unrest and fear in the enemy territory. Covert warfare, as practised by Pakistan, includes different tactics like guerrilla warfare, inciting insurgencies and destruction of buildings, all of which attempt to work towards generating terror and insecurity in the minds of Indians and, thus, aim to weaken their physical and mental capabilities.

GEN ZIA'S PURSUIT OF ISLAMISATION

Gen Zia systematically reinforced the *Islamisation of Pakistan* which was propagated by his predecessor, Zulfikar Ali Bhutto. Zia's vision came out very clearly in his words: "Pakistan, which was created in the name

17. Ibid., p. 57.
18. Ibid.
19. Ibid., p. 59.
20. Ibid., p. 144.

of Islam, will continue to survive only if it sticks to Islam. That is why I consider the introduction of the Islamic system as an essential prerequisite for the country."[21]

Zia introduced "Islamic Reforms" in various aspects of Pakistani society and economy. A number of banking and commercial practices based on Islam were introduced, a dress code in accordance with Islamic norms was stressed, new women's universities were proposed and strict regulations were imposed on the sale and consumption of alcoholic beverages.[22] During Gen Zia's regime, Islamic practices were made mandatory in day-to-day life by the state. The Pakistan Army in this period developed close links with the various Islamists groups, and religion was increasingly used in strategic thinking. Zia, in the process of reinforcing the Islamisation of Pakistan and introducing Islamic reforms, allowed the Tablighi Jama'at (an Islamic missionary society) to operate freely within the army. Zia was also the first Army Chief and the first politician in Pakistan to participate in the Tablighis' annual convention at Raiwind.[23]

Zia was entrusted with the task of Islamisation of the Pakistan Army when he took over as the Army Chief. Bhutto saw Zia as the right man to take the Pakistani military to the next stage of its evolution as the guarantor of an anti-India, Islamic ideology.[24] Even as a Corps Commander, Zia had distributed books written by the Jamaat-e-Islami's founder, Maulana Sayyid Abdul Ala Maududi, as rewards for the officers who proved their calibre in various fields in his garrison. Gen Zia ul-Haq's early steps to Islamise the army are identified by Lt Gen Jalan Dad Khan as Deputy Martial Law Administrator and Corps Commander:

> A devout Muslim, it was a matter of faith with [Zia ul – Haq] to propagate Islam wherever he could. Immediately after his appointment as COAS [Chief of the Army Staff], the motto he gave the troops was *Eman* (Faith),

21. "Gen Zia ul-Haq's Address to the Nation on July 5, 1977", quoted in Hasan Askari Rizvi, *The Military and Politics in Pakistan 1947-1986* (Lahore: Progressive Publishers, 1986), pp 289-93
22. Cohen, n. 12, p. 91.
23. Cohen, n. 15, p. 113.
24. Husain Haqqani, *Pakistan: Between Mosque and Military (*Lahore: Vanguard Books, 2005), p. 112.

The education system was deeply influenced and Islamiat and Pakistan studies became compulsory for the B.A, Engineering, Medical, Commerce and Law students.

Taqwa (abstinence), *Jehad Fi Sabeelillah* (war in the way of or for the sake of God). He urged all ranks of the army during his visits to troops as well as in written instructions, to offer their prayers, preferably led by the commanders themselves at various levels. Religious education was included in the training program and mosques and prayer halls were organized in all army units.[25]

Zia, in his first speech as Chief Martial Law Administrator, described himself as a "Soldier of Islam" and declared his commitment to building a new political, economic and social order based on religion.[26] Adherence to the Islamic practices emerged as a major criterion for selection in the Pakistan Army. According to Zia, a soldier had to be a true Muslim before he took on the responsibility of defending the Islamic Republic. In the armed forces, the status of religious teachers was raised to the level of commissioned officers. This became a major attraction for the qualified individuals from the universities and religious institutions.

During Zia's regime, the observance of Islamic practices increased as compared to earlier political or military regimes in the country. The state was now being run on the values interpreted on the basis of religion. The number of mosques in the country increased. The education system was deeply influenced and Islamiat and Pakistan studies became compulsory for the B.A, Engineering, Medical, Commerce and Law students.

The Islamist parties and especially groups like the Tablighi Jamaat, linked to the Deobandi tradition, got greater access to the military officials. Zia encouraged the Islamist parties to counter the political forces. The Islamist parties received favourable treatment from the ruling militia, and members of the Jamaat-e-Islami were offered senior positions in the important ministries. The judicial system of the state was Islamised and a Shariat Council consisting of *Ulema* was established to look into constitutional

25. Lt Gen. Jalan Dad Khan, *Pakistan Leadership Challenges* (Karachi: Oxford University Press, 1999), p.158; Haqqani, Ibid., p. 113.
26. Haqqani, n. 24, p. 127.

and legal matters pertaining to the state, which were to be conducted in accordance with the Islamic beliefs.

It was during this process of Islamisation that the Afghan War came into the picture and altered the total dynamics of Pakistan's political, military and strategic policies.

THE AFGHAN WAR IN THE 1980s

Following the Soviet invasion of Afghanistan, Pakistan became the frontline for the United States in the fight against Communism. Pakistan had already been a party to the destabilisation of Afghanistan which increased with the Soviet intervention and the reaction to it by the US, with Pakistan as its frontline state. Pakistan's threat perception from India consistently engaged the military, and the political leadership in Pakistan, worrying about the eastern border and turmoil in Afghanistan, made its western borders also insecure. Gen Arif outlined the three options available to Pakistan at the time of the Soviet invasion: "Firstly, she could accept the *fait accompli* as she lacked the capacity to challenge the Soviet Union. Secondly, she could provide open and full support to the Afghan freedom struggle, despite the risks involved. And, thirdly, she could give overt political, diplomatic, and humanitarian support to the refugees, with covert assistance to the Mujahideen".[27] Pakistan surely was not in a position to face the Soviet Union alone and was tempted by the American assistance which would serve its diplomatic, economic and defence interests. Pakistan opted for the third option outlined by Gen Arif and entered into a second term alliance with the United States. The status of US ally gave the Pakistan military an opportunity to fulfill its dreams for military modernisation. This major strategic development placed Pakistan in a position where it could demand the latest military weapons. Pakistan received an enormous amount of military aid from the US. It also received unlimited funds from Saudi Arabia and the Gulf countries to finance the US weaponry, which, Pakistan opted to procure in the 1980s.

27. Ibid., p. 314.

Pakistan offered its territory to the Americans and Zia's military regime undertook the responsibility of training the Mujahideen to carry out covert operations to fight the Soviets. The operations directed by the CIA (Central Intelligence Agency) comprised one of the largest operations planned by the US and shaped a relationship between the CIA and the Pakistani intelligence agency ISI (Inter-Services Intelligence), as the two worked in coordination for about a decade.

Pakistan's alliance with the US in the 1980s led to the development of the following factors.

Religion Became a Major Driving Force

The US' war in Afghanistan led to structural and organisational development of the factor of *religion in war*. The soldiers for war were being trained to fight in a "holy war" in the name of God. The declaration of *jihad* in Afghanistan led to the legitimised structural development of the institutions preparing young fighters. It is reported that over a period of time, over 80,000 volunteers were being trained for the war; they came not only from Pakistan and Afghanistan but also other Muslim countries like Sudan, Bangladesh, Algeria and Turkey. It was the combination of courage, specifically amongst the Afghan fighters and their strong religious belief that made the Mujahideen formidable warriors.[28] The belief was strengthened that the Mujahideen were fighting a holy war against the unbelievers – the *Kafirs*, and "once the *jihad* was declared by their religious leaders, it was the duty of all men to fight, to save their faith, to defend their honour, to protect their independence and to guard their land and families".[29] The battle cry for the Mujahideen was (and is till date) "*Allah o Akbar*" – God is Great, which they shout as they are attacking an enemy camp, base or personnel.[30] Thus, the fighting for religion proliferated.

28. Brig Mohammad Yousaf and Maj Mark Adkin, *The Bear Trap* (Lahore: Jang Publishers, 1992) p. 32.
29. Ibid., p. 33.
30. Ibid.

Pakistan: Training Ground for the Guerrilla Fighters

Ever since the creation of Pakistan, the Pashtuns or the Balochis have been motivated by the creation of an independent state advocated by the Pashtun regimes in Kabul. This worried the leadership in Pakistan about the vulnerability of Pakistan and, thus, the possibility of ethnic unrest.

Following the Soviet presence in Afghanistan, in December 1979, Lt Gen Akhtar Abdul Rahman, the Director General of the ISI convinced Gen Zia that Pakistan had the capacity to defeat the Soviets in a large-scale guerrilla war. The military leadership agreed to support the guerrilla warfare with arms, ammunition, money, intelligence, training and operational advice. Gen Akhtar, also suggested to Zia that Pakistan should offer the border areas of the North-West Frontier Province (NWFP) and Balochistan as a sanctuary for both the refugees and guerrillas. The base was essential for the covert forces as without a secure, cross-border base, no such campaign could succeed.[31]

Pakistan offered its territory as a secure base for the Mujahideen guerrilla fighters and became the base for these fighters, providing them with supplies of arms and ammunition apart from food and shelter, training and intelligence.[32] Brig Mohammad Yousaf and Maj Mark Adkin have observed: "The border areas of Pakistan had grown into a vast, sprawling administrative base for the *Jihad*. The Mujahideen came there for arms, they came to rest, they came to settle…."[33] Since the US assistance to the Mujahideen started as a covert affair, the ISI Directorate became the channel for not only ensuring the secrecy of the operation but also to provide expert advice and train the Mujahideen in guerrilla tactics.

In this process, Zia cultivated a venomous strain of Islamic ideology in Pakistan. The ISI, in partnership with the right wing Islamic parties like the Jamaat-e-Islami and Jamiat-e-Ulema-e-Islam, recruited millions of Afghan refugees in Pakistan and students from the *madrassas*, to join the fight in Afghanistan and be the holy fighters. In this process, these Islamic parties

31. Ibid., p. 25.
32. Ibid., p. 49.
33. Ibid.

developed an extensive network in Pakistan and also became much more influential.[34]

Along with this *jihadi* culture what was also encouraged in Pakistan was sectarianism which resulted in the killing of thousands. On the external front, the Islamic revolution in Iran in 1979 played a crucial role and the Khomeini regime began exporting its revolutionary message across the Muslim world. Pakistan, invariably, became a battle ground for the transplanted war between Iran and Saudi Arabia, which worked towards restricting the spread of Iranian Shia influence.[35] Balochistan became the hub of hundreds of *madrassas* which were basically established to limit the Shia influence in Pakistan. On one side, were the Iranian-backed Tehrik-i-Nifaz-i-Fiqh-i-Jafaria and on the other side, were Sunni extremist groups within Pakistan like the Sipah-e-Sahaba, who demanded that Shias (who comprised 15-20 per cent of the Pakistani population) should be declared non-Muslims like the Ahmadis.[36] The Islamisation process during Zia's regime gave a totally different dimension to *jihad* and encouraged a violent *jihadi* culture and sectarianism in Pakistan.

Non-Accountability of the US Weapons: Tools for Jihad

In the 1980s, the US intelligence services followed a strategy of supplying enormous amounts of arms and ammunition to the Mujahideen leaders and commanders in the field. The weapons pipeline was under the control of the ISI which actually was responsible in deciding the recipient and the quantity of weapons. The ISI retained the majority of the weapons and equipment (reportedly 60 per cent) for its own covert war against India. The weaponry supplied during the Afghan War remained in the region after the war ended. The intelligence agencies faced the problem of concealing this responsibility of distributing the arms and the US did not want to be projected as providing direct military aid to the *jihadis*. It has been reported that the "US intelligences services set up bank accounts in Switzerland into which the US and the Saudi governments directed their contributions to the

34. Haider, n 5, p. 122.
35. Ibid., p. 123.
36. Ibid.

Afghan resistance, which were then used to pay for weapons from a variety of sources. Wealthy individual Saudis and the Iranian government also contributed to the Mujahideen." [37] The Dubai-based Pakistani managed BCCI (Bank of Credit and Commerce International) and Pakistan's own Mehran Bank where profits from narcotics trade were also recycled, stand out in this regard. Initially, the supply of US weapons was a trickle and the weapons supplied for the Mujahideen were mostly outdated but as the fighting intensified, the type of weapon supply improved. Reportedly, Washington provided over two billion dollars of covert assistance to the Afghan War.[38]

Pakistan developed significant financial interest in the drug trade and this assisted in the development of the drug economy in Afghanistan and Pakistan.

Development of the Narcotics Trade

Another important development during this period was the narcotics trade which flourished with the CIA's assistance to fund the covert operations. The opium production went up from 200 metric tonnes in 1980 to 1,200 metric tonnes in 1989.[39] Initially, in the 1980s, the narcotics trafficking network was used to support the US-Pak strategy of arming and supplying the Afghan Mujahideen. Later, the military in Pakistan developed significant financial interest in the drug trade and this assisted in the development of the drug economy in Afghanistan and Pakistan. The drug money was also believed to have been used by the military to support Pakistan's active nuclear programme which was initiated by Bhutto in the early 1970s. Thus, the narcotics trade was initially developed to generate funds for the war against the Soviets but it became one of the major resources for the military to fund its weapon modernisation plans and covert operations in India, not only in Kashmir but also in Punjab.

37. "India: Arms and Abuses in Indian Punjab and Kashmir", September 1994, Vol.6, No.10, at http://www.hrw.org/campaigns/kashmir/1994/index.htm
38. Haqqani n. 24, p. 318.
39. T. Raghvan, "The Narcotics Trade in South-West Asia: Geography and Production", *Security Research Review*, at http://www.bharat-rakshak.com/SRR/Volume14/raghvan.html

RISE IN TERRORISM IN THE 1980s AND 1990s

In Kashmir, in the 1980s, religious resurgence, coupled with increasing alienation of the youth for diverse reasons, started to increase, and Pakistan's strategy of covert war through terrorism began to concretise. What was happening in Afghanistan and also happening simultaneously in Khalistan (with Pakistan's active assistance), had a direct impact in the Valley. Thus, in the mid-1980s, the disturbances in Kashmir were growing, with an unusual amount of Jamaat activity, processions and resentment against the Hindus, and the communal divide had started to be a major disturbing factor. Pakistan continued its covert war and the year 1984 witnessed substantive escalation of violent acts in J&K. In the late 1980s and 1990s, Pakistan became much more active in sponsoring terrorism in J&K. The ISI encouraged young Kashmiris to come to Pakistan for training. The ISI initially indoctrinated and trained the secular groups in Kashmir and eventually shifted to training of groups linked to Pakistan's own Islamic parties. [40]

The weapons used by the terrorists had undergone a change as Pakistan had acquired modern arms in the 1980s to equip the covert fighters in Afghanistan. On one side, Pakistan had equipment for the Afghan Mujahideen which could be easily smuggled into Kashmir, and, on the other, Pakistan also acquired modern weapon systems, including the F-16s from the US during this period and, thus, felt stronger and more confident to carry out its covert strategy in Kashmir. But the most important factor for the escalation of the covert war in Punjab and Jammu and Kashmir was the acquisition of nuclear weapons by Pakistan which it perceived as a security guarantee against a robust Indian military response.

PAKISTAN'S NUCLEAR WEAPONS: SHIELD AGAINST TERRORISM

Pakistan accelerated its nuclear programme in the 1980s under Zia. The military regime in Pakistan exploited the India "threat" with the acquisition of nuclear capability to gain domestic legitimacy. It was under Zia's rule that Pakistan became a nuclear state and defined a coherent nuclear strategy. By 1987, it was

40. Ahmed Rashid, *Descent into Chaos* (London: Penguin Group, 2008), p. 111.

believed that Pakistan could carry out a full nuclear explosion. By 1992, Pakistan declared officially that it possessed the cores of nuclear weapons, and in 1998, Pakistan's nuclear tests followed India's new posture of a nuclear state.

Pakistan became more vocal about the possession of nuclear weapons in the late 1980s and in the 1990s, in order to create the impression that any radical move from the Indian side might be retaliated with the ***Islamic bomb.***

The acquisition of nuclear capability enhanced Pakistan's capability to wage and escalate the covert war in Kashmir as nuclear weapons were believed to deter India from responding with conventional military retaliation. Policy-makers in Pakistan seem to be convinced that they will be able to carry on, or rather accelerate, their activities in Kashmir by holding out the threat of use of nuclear weapons, if required, and this would control India's strategic moves in the Valley. This thought process seems to have grown with Pakistan's "first use policy". Pakistan claimed that it had the capability of a nuclear bomb in 1987, and it is noteworthy, that during the late 1980s, the activities in the Valley also witnessed a shift. The terrorist acts increased significantly in numbers and were planned in a more organised manner, making the job of the Indian security forces more difficult.

Pakistan became more vocal about the possession of nuclear weapons in the late 1980s and in the 1990s, in order to create the impression that any radical move from the Indian side might be retaliated with the *Islamic bomb.* Pakistan's strategy has been to use the nuclear card for aggressive militancy in Kashmir and, thus, the Pakistan military now had the nuclear umbrella to shield it from an Indian military response. *Jihad* now had the protection of the nuclear bomb for Pakistan. There is a clear correlation between the progress in acquisition of nuclear weapons and the launch of the covert war during the last 25 years.

1990s: POLITICAL TUG OF WAR

After Zia's death, Pakistan faced innumerable challenges. The nation had been under the military rule for a long period and, thus, getting back to

democracy was a challenge: the economic downslide had started to show up, the *jihadi* culture took firm roots in the country, the alliance with the US had just ended, and Pakistan stood isolated internationally. The democratic regimes between 1988 and 1999 were unstable and changed frequently, especially if the agenda of the elected governments challenged the power and functioning of the army. During this period, there were four elections and both Benazir Bhutto and Nawaz Sharif returned to power twice. There were four caretaker governments in between as neither of the elected governments could complete its term.

The ISI became an important centre of power on account of its role in the Afghan War and its involvement with the Americans. Although the fundamentalist and Islamists appeared to have lost in the elections, their influence continued to grow, especially among the intelligence agencies, military officers and the emerging middle class in Pakistan. The ISI also managed to create and sustain the differences between the political parties which hampered the evolution of a mature democratic set-up in Pakistan and contributed to the frequent changes on the political front. The intelligence encouraged and utilised the Islamist parties to counter the political groups which went against the military's interests.

On the external front, there were two developments in this decade. Both these developments were a continuation of Pakistan's existing policies. The leadership in Pakistan intensified terrorist activities on the Indian soil through their proxies and anti-India terrorist organisations became much more active in the Valley and other parts of India. The ISI was now a fully trained and equipped organisation with a ready infrastructure for *jihad* which was now fully diverted towards India to continue Pakistan's strategy to 'bleed India through a thousand cuts'. By 2002, Pakistan became home for more than two dozen militant groups operating in the neighbourhood and pursuing their own agenda, which was considered by the state to be in its favour. The largest among them were the Lashkar-e-Tayyeba (LeT), Jaish-e-Mohammed (JeM), Harkat-ul-Mujahideen (HuM) and Harkat-ul-Jihad-al-Islami (HuJI). All of these organisations shared similar sources and pursued similar goals. They had the state's patronage and funds have never been a

problem. The state's patronage, in fact, helped the *jihadi* organisations to raise public funds.

On the western front, Pakistan was keen to create its strategic depth and not to have a hostile government. The Pakistan Army and ISI, along with the political leadership, came together to support a new class of warriors – the Taliban. In 1994, Afghanistan saw the outbreak of the Taliban, which was composed of the younger generation of Pakistani-Afghans. The Taliban were mainly the Afghans who grew up in the Pakistani refugee camps and were products of *madrassas* which were encouraged during Zia's time and funded by the Saudi money. Maulana-Fazl-ul-Rahman, leader of the Jamiat-e-Ulema-e-Islam-Fazl-ul (JUI-F) supported the Taliban, and being a close ally of Benazir, he played a critical role in facilitating communications between Pakistan and the Taliban.[41] The Pakistani leadership extended full-fledged support to the Taliban and added to their strength from Pakistani *madrassas*. The Taliban began to take over one province after another in Afghanistan and brought the whole of Afghanistan under their control in less than five years. [42]

MUSHARRAF'S COUP AND US LED WAR ON TERROR POST 9/11

The military under the leadership of Gen Musharraf assumed control of the state in 1999 and, even though the coup was condemned by most world leaders, it was supported by a majority of the Pakistani populace. Pakistan once again witnessed a major strategic development and entered into a third alliance with the US post 9/11. Once again, Pakistan arrived at a critical crossroads. Musharraf attempted to project a path of moderation and publicly announced on January 12, 2002, that Pakistani territory would not be used for *(jihadi)* terrorism. In 2004, he announced his plea for *Enlightened Moderation* which could provide an answer to Pakistan's identity and its relationship with Islam. Defining the Enlightened Moderation, he said:

41. Hassan Abbas, *Pakistan's Drift Into Extremism: Allah, the Army and America's War on Terror*, (New York: M.E. Sharpe, 2005), p. 154.
42. Ibid., p.155.

> The strategy of enlightened moderation …….. involves a win-win situation for the whole of the world as well as for the Muslim countries. This is a two-pronged strategy. One prong is to be delivered by the Muslim world itself by shunning militancy and extremism and adopting the path of socioeconomic uplift to achieve its own emancipation. The other prong is meant to be delivered by the West, and the United States in particular, to determinedly resolve with justice all political disputes in which Muslims are engaged and also assist in the socioeconomic betterment of the deprived Muslim world……..The time has come to re-think our position. What we need is a rennaissance…... We have to concentrate on human resource development, and the best way for that is through poverty alleviation, greater education, better health and assured social justice….. We have to adopt the path of moderation, a conciliatory approach, a pacific approach, in order to cleanse ourselves of the charge that Islam is a religion of militancy and is averse to modernization, democracy and secularism.[43]

Although Musharraf talked about the moderate, secular path which included rejection of extremism, the actual strategies which the military pursued were certainly not in sync with the announced enlightened moderation. It was more to appease the West and project an image of Pakistan as a moderate Islamic nation which believed in countering extremism and was focussed on socio-economic development.

The military regime came under immense pressure by the Bush Administration to act against the terrorist organisations and Musharraf issued orders to ban some of the key militant outfits and also for registering of the *madrassas*. These efforts failed to provide results and the popular consensus has been that the military's flawed approach towards the war on terror has been responsible for the rising extremism and flourishing insurgency on Pakistan's frontier borders, NWFP (now Khyber Pakhtunkhwa – KPK) and the Federally Administered Tribal Areas (FATA). These have been troublesome regions even in the most peaceful times and are now

43. Speech by Gen Musharraf, "OIC Challenge and Response: Enlightened Moderation", June 1, 2004, at http://presidentmusharraf.wordpress.com/2005/01/18/musharraf-oic-enlightened-moderation/

engaged in a full-blooded insurgency. Pakistan, for the first time, is facing terrorist attacks within its own territories. The military has a history of waging insurgencies (in the name of *jihad*) since the time of its creation in 1947, but, post 9/11, it has been compelled to take on a reverse role of counter-insurgency. The military has been flagrantly discriminate in dealing with various terrorist groups and has not given up *jihadi* terrorism as its state policy.

The military has been flagrantly discriminate in dealing with various terrorist groups and has not given up *jihadi* terrorism as its state policy.

A study by Ashley Tellis identifies four different terrorist groups implicated in this regard: domestic sectarian groups, anti-Indian terrorist groups, the Taliban and Al Qaeda.[44]

The first set includes the domestic sectarian groups like the Sunni Sipah-e-Sahaba and its offshoot, the Lashkar-e-Jhangvi, and the Shia Tehrik-e-Jafaria and its offshoot, the Sipah-e-Muhammad. These groups have been engaged in violent sectarian activities within Pakistan. Although these groups were initially supported and encouraged by the military, they became a major challenge for the military leadership, posing a serious threat to the domestic order. The global war on terror provided an opportunity to the military leadership to crack down on these elements. The state leadership was selective in suppressing these organisations and the target groups were the ones whose objectives fell out of sync with the military's perception of national interests: those engaged in the *jihadi* violence within the state rather than in support of the military's external ambitions vis-à-vis India and Afghanistan.[45]

The second set of terrorist groups includes the organisations working in coordination with the Pakistan Army and the ISI against India, such as LeT, JeM and HuM. These are the terrorists groups which the Pakistan Army has trained, encouraged and financed to carry out the covert war in Jammu and Kashmir and the rest of India since the 1980s. These groups are an extension of Pakistan's military strategy to continue sub-conventional

44. Ashley J. Tellis, "Pakistan and the War on Terror: Conflicted Goals, Compromised Performance" (Washington DC: Carnegie Endowment, 2008), p.4.
45. Ibid.

warfare through various means and, thus, received different treatment from Gen Musharraf, as compared to the sectarian groups. These groups are viewed as working to legitimise the struggle for self-determination for the Kashmiri people and, thus, have been excluded from the military's campaign against violence and extremism.[46] These groups have been active not only in Jammu and Kashmir but also in other parts of India, creating occasions to spark a war or to precipitate action from India.

The third group of the extremist elements comprises the Taliban, who were forced to leave Kabul after the initial success of Operation Enduring Freedom.[47] The Taliban, after their defeat by the Northern Alliance, reverted to their villages in the southern and eastern Afghan provinces, as well as along the border areas on the western side of the Durand Line separating Afghanistan from Pakistan.[48] A significant number of the Taliban leaders, along with the Pakistani Pashtuns, being the prime targets in the global war on terror, took refuge in the FATA. Most of the Taliban fighters were originally mobilised by the ISI from the Gilzai confederation of Pashtuns who dominated southeastern Afghanistan and from other Pashtun tribes belonging to FATA, and thus, their going back to a relatively secure place, their original homeland, was natural after the Pakistan military decided to join the US in the aggressive military operation against the Taliban.[49] The Taliban has made Pakistan's tribal belt the base for training camps and for conducting action plans in Afghanistan and the Pakistani territory. The Taliban leadership has manoeuvred an independent administrative set-up in FATA and the locals are in no position to oppose them.

From the beginning in 2008, there have been reports of the Taliban extending their conservative extremist norms to the civilians in the region, controlling even their day-to-day lives. Pakistan's former Interior Minister, Aftab Khan Sherpao, whose ancestral village is in the foothills of the tribal region, very categorically stated that there is a serious risk of "total

46. Ibid., p. 5.
47. Ibid., p. 6
48. Ibid.
49. Ibid.

Talibanization" in the NWFP.[50] It is tough to believe that the Taliban is able to regenerate to this extent without the support of the Pakistan military and the intelligence units which have allowed them to flourish and operate in cities like Karachi within Pakistan. Because the Pakistani leadership was so deeply involved in the making of the Taliban, it has undeniably avoided the killing or capturing of the senior Taliban leadership in southern Afghanistan or in the FATA. The Taliban has enjoyed leverage from the Pakistan Army and has expanded the *jihadi* terrorists network within Pakistan, resulting in massive suicide bombings and revolts.

The fourth group, Al Qaeda, which also found sanctuary in FATA, received a much more aggressive and firm response from the military.[51] Although Al Qaeda commands some sympathy within the Pakistani society, the 9/11 terrorist attacks in the US were conclusively attributed to this terrorist outfit, and the US embarked on a worldwide campaign against it. Pakistan too extended support to the US by conducting various law enforcement and internal security operations targeting the terrorist financing, and apprehending and rendering terrorist targets for prosecution abroad.[52] The massive military operation resulted in the arrest of around 700 terrorists from Al Qaeda and other extremist organisations. Although the aggressive military operations led to the arrest of many Al Qaeda operatives, the top leader, Osama bin Laden, was not touched (till May 2011). The operations forced the militants to disperse further into Pakistan areas, as the Khyber Pakhtunkhwa areas, while considered secure for the Taliban, became unsafe for these operatives. Also, the cities in Pakistan provided them with a more advanced mode of communication in order to connect them to the extremist network.[53]

In May 2011, Osama bin Laden was killed in an operation carried out by the US Navy SEALs from the US Special Operations Command. Bin Laden has been living for years in a military compound in Abbottabad,

50. Ibid.
51. See, Zafar Abbas, "Pakistan Army Confronts Al Qaeda", *BBC News*, January 8, 2004, at http://news.bbc.co.uk/2/hi/south_asia/3378395.stm
52. Ibid.
53. Tellis, n. 44, p. 10.

Pakistan, where he was holed up in a two-storey house just 100 yards from a Pakistani Military Academy. Abbottabad, is located just 50 km from the capital, Islamabad, and is home to three Pakistan Army regiments, and thousands of military personnel. The area is relatively affluent, with several retired military men residing there. Although Gen Kayani has repeatedly claimed that he was unaware of Osama's location, it is tough to believe that bin Laden was residing in the army compound without the knowledge of the Pakistan military and intelligence officials. President Obama's chief counter-terrorism adviser, John Brennan, said it was "inconceivable that Osama bin Laden did not have a support system in the country that allowed him to remain there for an extended period of time".[54] The end of bin Laden has marked a major shift in the Pakistan-US relationship. The level of trust between the two allies has been deteriorating, bringing the relationship between the two nations to the lowest level.

After almost a decade of blatant military operations, the Americans appear increasingly frustrated with the results of the operations. Not only have the numbers of the extremist acts escalated, but the terrorists attacks are also much more intense, better planned and persist with deadly regularity, making it difficult for the American intelligence to detect. Increasing drone attacks by the US and North Atantic Treaty Organisation (NATO) forces have increased anti-US sentiments in Pakistan tremendously.

TALIBAN INSURGENCY : EMERGENCE OF THE TTP

The Taliban insurgency began as early as 2003 when the Al Qaeda and Afghan Taliban fighters were flushed out of Afghanistan by the US armed forces. In 2007, the Tehrik-e-Taliban Pakistan (TTP) emerged as an entity in the context of a series of military operations (that took place post 9/11): Pakistani military operations in FATA as well as US Unmanned Aerial Vehicle (UAV) strikes in FATA. Until then, most of the component groups of the TTP were loosely organised, with ties to the Afghan Taliban. The TTP started to professionally organise itself when Abdullah Mehsud of the Afghan Taliban returned to Waziristan from the Guantanamo Bay camp. He

54. "Inconceivable that Osama had no Support System in Pakistan: US", *The Hindu* May 3, 2011.

blew himself up in Pishin, Balochistan, during a siege by Pakistani forces in 2006.[55] After Abdullah Mehsud's death, Baitullah Mehsud, a leading member of the Afghan Taliban, organised all the groups operating in FATA who professed similar ideologies and knit them into one of the most dangerous terrorist/insurgent groups called the TTP.[56]

The organisation consists of a number of militant groups (around 20 of them) and is rooted in the tribal belt of Pakistan. The TTP's creation in December 2007 marked a new development arising out of the realisation among the local and foreign militants that a central command was required in order to attain their objectives, and Baitullah Mehsud provided them the unifying force. The main objectives of the TTP are: (i) foreign troops must leave Afghanistan; (ii) Pakistan must end its cooperation with the US and NATO forces; and (iii) the *Sharia* must replace the existing legal system. The TTP has adopted a strictly anti-state and specifically anti-military agenda and has been conveying its message by consistently attacking the government/military offices. In other words, the TTP has organised itself as a true insurgency, ideologically as well as organisationally.

The TTP draws its ideological guidance from Al Qaeda, and also provides safe havens to the Al Qaeda allies in FATA. Given the mutual cooperation between the two organisations, it would not be wrong to state that the TTP is a force multiplier for Al Qaeda.[57] The TTP has launched numerous attacks against US, NATO and Pakistani targets. The organisation regards the Pakistani state as an enemy of Islam for siding with the US. It has adopted an anti-state posture and has claimed responsibility for most of the terrorist attacks, including the assassination of Benazir Bhutto. The organisation is growing in influence among the young and unemployed youth and is using the *Sharia* to promote its political and ideological agenda.

55. Imtiaz Gul, *The Al Qaeda Connection: the Taliban and Terror in Pakistan's Tribal Areas* (New Delhi: Penguin Books, 2009), p. 51.
56. TTP was the revival of an older organisation of the same name founded in 1998 in Orakzai Agency.
57. "Tehrik-e-Taliban Is a Terror Group", *VOANEWS.com Policy*, July 9, 2010, at http://www.voanews.com/policy/editorials/Tehrik-e-Taliban-Is-A-Terror-Group-102393269.html

CONCLUSION

Presently, Pakistan is facing a broad landscape of militancy. A variety of terrorist groups with varying agendas operate from Pakistan and share a varied relationship with the state. Some of these organisation like the TTP regard the state as an enemy of Islam for joining hands with the West and killing their own people. On the other side are the deadly groups like the Jamaat-ud-Dawa, which are flourishing in the heart of Pakistan and are under the state patronage. For the first time, militancy has managed to penetrate the interiors of Punjab and Sindh, and the Army General Headquarters (GHQ) became one of the terror targets in the recent past. In fact, the bases of all the three forces have been attacked — the air force bases have been frequent targets. The impact of the Afghan War has allowed Al Qaeda, the Haqqani network and the Taliban inside Pakistan where they have been expanding their influence. The Pakistan military and the ISI have nurtured some of the terrorist organisations which it categorically grades as "strategic assets" and is clearly not willing to act against them. These so-called "friendly"[58] groups as Ayesha Siddiqua Agha terms them, include: the Good Taliban, Lashkar-e-Tayyeba (LeT), Jamaat-ud-Dawa (JuD), and Jaish-e-Mohammad (JeM). The Haqqani network which has strongholds in the bordering Afghan districts of Paktia and Khost and is involved in anti-US and anti-NATO operations, has enjoyed state patronage for long.[59] The military has desisted from acting against these groups and has been "selective and partial" in its counter-terrorism approach, which has been the root cause for the lack of success in the war on terror.

The frontiers borders – NWFP and KPK—have become the breeding ground for terrorism and the region presents a conglomeration of various insurgents and terrorists groups to the Pakistani military and NATO forces. Al Qaeda, Haqqani and the Taliban have established their sanctuaries in these area. Insurgency in Balochistan,, which became active in 2004, has aggravated much more after the killing of Akbar Bugti in 2007. The Balochis have always suffered a deep sense of alienation from the state and resisted it

58. Ayesha Siddiqua Agha, "Pakistan's Counterterrorism Strategy: Separating Friends from Enemies", *The Washington Quarterly*, Winter 2011, pp.149-162.
59. Ibid.

regularly, which the leadership has tried to curb with brute military force in the past, starting in the 1940s. Added to this deadly mix of extremists is the TTP. The TTP has posed a real danger to the state and, in a way, is an extension of Sunni Deobandi militancy. It has absorbed members of radical Sunni organisations, and this has further exaggerated the problem of Shia-Sunni violence not only in the tribal belt but also in other parts of Pakistan.

The impact of the Afghan War has allowed Al Qaeda, the Haqqani network and the Taliban inside Pakistan where they have been expanding their influence.

Islam has remained extremely critical for Pakistan in its domestic and foreign policies. But the interpretation of Islam has varied under different regimes. Jinnah's vision was that of a secular nation where Muslim culture and norms could be protected and practised freely by the Muslims. Obviously, his vision was shaped under a different set of circumstances, and, eventually, as one can see, the state adopted a very different interpretation of Islam, completely deviating from Jinnah's spirit. Religion under Zia found its most extremist expression and Pakistan's ideological posture was reshaped. The underlying problem is that the state has not been able to define its relationship with Islam till date. The Pakistani leadership has allowed itself to become entangled in contradictions, where it talks about enlightened moderation on one side, and simultaneously, patronises the terrorist outfits which brainwash the young Pakistani minds to join hands in fighting a holy war in the neighbourhood. Pakistan is facing a deadly *jihadi* consequence of its own long stated policies based on terrorism, threatening the very survival of the state. The leadership in Pakistan now needs to seriously reconsider its strategic calculus and refrain from using terrorism legitimised by religion as a foreign policy tool.

INDIA'S CYBER WARFARE STRATEGY IN NEXT DECADE

M.K. SHARMA

Attack is the secret of defense; defense is the planning of an attack.
— Sun Tzu, *The Art of War*

INTRODUCTION

The world is witnessing a remarkable shift in the locus of global power with the relative decline of the United States of America and the dramatic rise of China. It is estimated that the rise of India and China will alter the nature of the global system and the global landscape in the coming two decades. During this great geo-political transition period, there is an urgent need to revaluate our theories, paradigms, assumptions and strategies in the light of technological, economic, political and military developments in the region. The heavy dependence of government organisations, business, economic activities and military affairs on Information and Communication Technology (ICT) necessitates incorporation of cyber technology into our strategic calculations. Cyber power is exerting itself as a key lever in the development and execution of national policy, including counter-terrorism, economic growth, and diplomatic affairs. The US–China power competition in the region places extraordinary demands on India to enhance its power and influence primarily for the defence of its own sovereignty, territorial integrity and promotion of the global good while it builds up its economy

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

Cyber power is exerting itself as a key lever in the development and execution of national policy, including counter-terrorism, economic growth, and diplomatic affairs.

and long-term prosperity, ironing out domestic inequities. Towards this, cyber power has the ability to create synergy with other elements and instruments of power and integrate them in a way that improves them all. For the next decade or so, cyber power can also be leveraged as an instrument of foreign policy to offset India's inadequate hard power, taking advantage of the expertise and human resource in the domain of ICT. Therefore, it is imperative to craft a cyber strategy that enables the exploitation of the capabilities that cyber space offers, while simultaneously protecting and defending against the vulnerabilities it presents.

This paper seeks answers to why the cyber weapon cannot be deployed and used like another kinetic weapon without the support of an apt strategy. And why (or why not) India should pursue cyber warfare more aggressively and, consequently, the paper explores how cyber offence, defence and deterrence options relate to form the national cyber warfare strategy.

UNDERSTANDING THE NEED

Strategy is defined as "the art and science of developing and employing instruments of national power in a synchronised and integrated fashion to achieve theatre, national and/or multinational objectives"[1]. However, when we approach a particular operational domain, the strategy is to be grounded in that realm; accordingly, cyber strategy means development and employment of strategic capability to operate in cyber space, integrated and coordinated with the other operational domains (land, sea, air and outer space), to achieve or support the achievement of objectives across the elements of national power, in support of the national security strategy.[2] Therefore, the key challenge to a national

1. Joint Publication (JP) 1–02, *DOD Dictionary of Military and Associated Terms* (Washington, DC: The Joint Staff, August 31, 2005).
2. Daniel T. Kuehl, *Cyber Power And National Security* (New Delhi: Vij Books, 2009), ch. 2, p 40.

cyber strategy would be to clearly demonstrate how it will integrate with, and support, other domain specific strategies and, consequently, the national security strategy to achieve their critical and interrelated objectives.

Cyber strategy means development and employment of strategic capability to operate in cyber space, integrated and coordinated with the other operational domains (land, sea, air and outer space).

Let us ask ourselves some basic questions as a starting point to arrive at a cyber strategy: is the advent of cyber warfare a good thing, or does it place India at a disadvantage? Do we envision the use of cyber war weapons only in response to the use of such weapons against us or are cyber war weapons something that we will employ routinely in both large and small conflicts? Do we see cyber space like other domains (like sea, air space or outer space) in which we must be militarily dominant and in which we will engage an opponent while simultaneously conducting operations in other domains? Should we be hacking into other nations' networks in peace-time? If so, should there be any constraints on what we would do in peace-time? What do we do if we find that another nation has hacked into our networks in peace-time? What if it left behind logic bombs in our infrastructure networks? Do we intend to use cyber weapons primarily or initially against military targets only, and if so, how do we define military targets?[3]

Further, some more important questions that the cyber warfare strategy should enquire into are: what is the importance of avoiding collateral damage with our cyber weapons? How might avoiding it limit our use of the weapons? What level of command authority should authorise the use of cyber weapons, select the weapons and approve the targets? Also, how do we signal our intentions with regard to cyber weapons in peace-time and in crises? Are there ways that we can use our possession of cyber weapons to deter an opponent? And, finally, if an opponent is successful in launching a widespread, disabling attack on our military or on our

3. Richard A. Clark and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About it* (Echo, April 2010), ch. 5. pp. 152-154.

economic infrastructure, how does that affect our military and political strategies?

In order to arrive at any useful cyber strategy based on the principles of war, it would be prudent to note that we are analysing a 'virtual world' with all its unique characteristics.

LOOKING THROUGH THE PRISM OF 'PRINCIPLES OF WAR'

Historically, military intellectuals have developed a set of principles of war to support the planning and execution of operations. These principles have evolved over hundreds of years through the writings of key military analysts.[4] India's principles of war are Selection and Maintenance of the Aim, Offensive Action, Maintenance of Morale, Security, Surprise, Concentration of Force, Economy of Effort, Flexibility, Cooperation, and Sustainability, as inherited from the UK.[5] These principles are based on the work of Maj Gen J.F.C. Fuller. Although there are country specific variations in the elements of these principles, the list revolves around unity of command, objective, offensive, mass, manoeuvre, economy of force, security, surprise and simplicity. In order to arrive at any useful cyber strategy based on the principles of war, it would be prudent to note that we are analysing a 'virtual world' with all its unique characteristics. Further, to evaluate the effectiveness of that strategy, we need to evaluate the ways and means available to the nation-state. Therefore, how this process can be applied to cyber warfare needs further illustration.

When we consider cyber warfare, do we see it happening only in the virtual battlefield or as being enmeshed into the physical battlefield too? While some of the principles of war don't easily transfer into the virtual battlefield, they can be force multipliers in the physical battlefield.[6] When

4. Carl Von Clausewitz, *On War*, ed. and trans, Michael Howard and Peter Paret (Princton University Press, 1975).
5. Air Vice Mshl Arjun Subramaniam AVSM, *Basic Doctrine of the Indian Air Force 2012*, ch. 3 pp. 13-16. http://merln.ndu.edu/whitepapers/India_Doctrine_Air-Force_ENG_2012.pdf
6. Janson Andress and Steve Winterfeld, "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioner" in *What is Cyber Warfare* (Syngress,2011), ch. 1, p. 6.

deciding on a cyber warfare strategy, it would not be prudent to throw away our time-tested doctrines and tactics—rather, we should be able to modify them, based on the new realities brought in by the ICT. While keeping selection and maintenance of aim paramount with a plan that produces surprise is still the key to success, we need to ponder on whether offensive action is still the best way to achieve victory in the realm of cyber warfare or is there a requirement of reassessment of the appropriate principles of contemporary warfare?

In fact, there is already a debate on about having a revised set of modernised principles of warfare as appropriate for 21st century operations. Charles Dunlap has updated the list to include Perceived Worthiness, Informed Insight, Strategic Anchoring, Durability, Engagement Dominance, Unity of Effort, Adaptability and Culminating Power.[7] Table 1 shows the interrelation and linkage of the modernised principles to the classical principles of war.

Table 1

Modernised Principles	**Relationship to Traditional Principles**
Perceived worthiness	Moral: what makes it worthwhile to risk one's life in combat?
Informed insight	Sense making, cognition, surprise.
Strategic anchoring	Concentration on, and prominence of, offensive.
Durability	Incorporates security into plan; depend on logistics.
Engagement dominance	Incorporates and simplifies manoeuvre; imposes/ opposes surprise.
Unity of effort	Draws on unity of command; reinterprets economy of force, mass, manoeuvre.
Adaptability	Presupposes flexibility but does not mandate simplicity.
Culminating power	Power needed to attain satisfactory closure at a given level of conflict.

Source: Charles J. Dunlop, "Neo-Strategicon: Modernized Principles of War for the 21st Century", *Military Review,* March – April 2006.

7. Charles J. Dunlap, " Neo-Strategicon: Modernized Principles of War for the 21st Century," ***Military Review,*** March-April 2006.

It may be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are "acceptable" and those that will trigger a major escalation in the intensity of cyber activity.

NEW REALITIES AND ROLE TRANSFORMATION OF MILITARIES

The changed techno-political realities present some fresh challenges to any responsible military leader or diplomat. Firstly, because the past experiences tell us that there is a very fine line between prudent preparation to defend our own assets and provocative military activities that tend to increase the probability of conflict. Secondly, unlike earlier days, the measures of the ultimate success of a military are not only by how well it defeats the enemy but also by how well it is able to provide protection to the growing economy and support the rest of the nation. Therefore, how we ingrain our responses to these demands while forming a cyber strategy would not be as simple as plainly deploying and using the newly discovered cyber weapons. Krepinevech's comments on the issue are quite thought provoking:

> It may, therefore, be difficult for the leadership of one cyber power to determine when, in the mind of its enemy, it has crossed the line between cyber operations that are "acceptable" and those that will trigger a major escalation in the intensity of cyber activity that could lead to catastrophic attacks.

Furthermore, there is always a time lag between the discovery of a new weapon and development of the strategy that would guide its employment and deployment. India became nuclear weapon capable in 1974 with the Pokhran-I test, however, the draft doctrine of credible minimum deterrence came into being only in August 1999.[8] In the absence of a strategy for the employment of a new type of weapon, we run the risk of accidental wars as was seen in the case of the nuclear weapons era. For the first decade or so,

8. http://en.wikipedia.org/wiki/India_and_weapons_of_mass_destruction

post Hiroshima, neither the US nor the erstwhile USSR had a comprehensive strategy for employing (or not employing) nuclear weapons. This resulted in the two superpowers coming to the brink of nuclear war several times, including during the Cuban missile crisis in October 1962.[9] The point driven home is that while there are obvious differences in the nature of cyber war and nuclear war, some experiences highlighting the necessity of a comprehensive strategy are worth contemplating as we develop a strategy for this new type of weapons.

PECULIARITIES OF CYBER DOMAIN

In the domain of kinetic war, one examines the vulnerabilities of the adversary's plans and military hardware, including tanks, airplanes, ships, missiles and other types of vulnerabilities such as the turning radius of a fighter aircraft or the acoustic blind spot of a submarine. Accordingly, specific tactics are developed to exploit these vulnerabilities, and, in some cases, specific weapons are built against them. Also, it is considered less likely for adversaries to be using the same systems as ours, and, thus, vulnerabilities in our opponent's systems are normally different from those of our own. In other words, hardening our own systems against vulnerabilities usually does not impact our ability to exploit the vulnerabilities of an adversary. But in the case of cyber warfare, this equation does not hold good, primarily because the entire cyber domain is built on the foundation of hardware with common processing architectures connected by a standardised system for exchanging data packets across the globe. Added to this basic commonality is the virtual monopoly in operating systems and popular software by Microsoft. As a consequence, at the top level, we share many common cyber vulnerabilities with our adversaries and allies alike. This presents a strategy dilemma for India when developing and using cyber offensive weapons and, at the same time, also trying to strengthen the cyber defences, both of which have become prominent policy concerns.

9. http://www.cbc.ca/news/interactives/tl-cuban-missile-crisis/index.html

STRATEGIC OPTIONS: THE OFFENCE–DEFENCE DYNAMICS

From the offensive perspective, the traditional policy choice would be to classify any vulnerabilities (in hardware, software, or systems) to enable development of exploits and eventually offensive cyber capabilities and also to keep them out of the hands of other states and cyber criminals. This is the traditional choice that governments make when it comes to conducting offensive military campaigns in any domain. Although it can be successfully accomplished in the traditional domains of warfare, in the cyber domain, this choice falsely assumes that only governments are involved in defence and offence. While this is a reasonable assumption in the case of land, sea, or air operations, in the cyber domain, the equations are different for various reasons as given below.

Blurring of Attack Surface

The 'attack surface' is very loosely defined and spread across the military, public and private infrastructure. Vulnerabilities exist in many more places than just operating systems and in many more objects than just traditional desktop and laptop computers. Virtually everything that runs computer software is vulnerable; the newly discovered categories including Programmable Logic Controllers (PLCs) that control the industrial process, Industrial Control Systems (ICS), Supervisory Control And Data Acquisition (SCADA) systems and mobile phone operating systems are receiving increased attention of both the 'black hat' and 'white hat' hacker communities.

Offence–Defence Catch Twenty-Two

There is another hurdle in building already costly cyber defences from our own offensive cyber warriors while planning and executing a covert cyber offensive to permit plausible deniability. This, more often than not, implies that knowledge about such cyber operations would not be shared by organisations and departments even within the same government, making its own systems vulnerable to the same exploits. For instance, a security researcher discovered several new critical ICS vulnerabilities, which he

planned to unveil at a cyber security conference. However, the vulnerabilities he discovered were so serious that he was persuaded by the US Department of Homeland Security and Siemens to forego his talk.[10] Thus, strategies aimed at improving a nation's cyber offensive capabilities would hinder the ability to improve its own cyber defence and result in counter-productive efforts: inter-departmental blame game, and duplication of resources.

For the Indian armed forces and National Technical Research Organisation (NTRO), there would be constant trade-offs between revealing a vulnerability to Computer Emergency Readiness Team (CERT)/ vendors/ industry/ the public so that they can be fixed, and keeping the vulnerability classified so that it can be potentially used offensively by them. This culture leads government agencies to hire experts (similar to cyber criminals) who would dig out the vulnerabilities and develop exploits for cyber offensive operations rather than informing the public or the vendors. This may result in a situation where government agencies and cyber criminals are using the same exploits on our systems at the same time. At an annual hacking contest sponsored by Google in March 2012, a well-known cyber security firm refused to divulge vulnerabilities and exploits that it had discovered in Google's Chrome web browser because it was worth more to it to divulge such information only to its customers, which consist of North Atlantic Treaty Organisation (NATO) governments and NATO partners.[11]

The Cost-Benefit Analysis

The costs of offence, when measured against the combined costs of defence and consequence management reveal some unique trade-offs. On the one hand, attackers seeking to cause damage that will generate strategic effect will require a substantial monetary investment in intelligence, targeting, and testing, and the weapon's shelf-life will be short. On the other, defenders still face formidable costs in protecting infrastructure and conducting

10. Chris Blask, "Network Security: The Threats You Don't See", Infosec Island, June 22, 2011, <www.infosecisland.com/blogview/14682-Network-Security-The-Threats-You-Dont-See.html>.
11. Andy Greenberg, "Meet The Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)", *Forbes*, March 21, 2012, <www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-whosell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/>.

consequence management across inter-agency boundaries. Therefore, while it is true that offence is still dominant on one side of the equation, the operational value of weapons is also complicated by their relatively short shelf-lives and some of the uncertainties involved in whether or not they achieve the desired effects on the target.

Investments in cyber defence have a diminishing marginal return per rupee spent on security. Extrapolating from this, the larger the attack surface, the less cost-effective defence is in preventing harmful effects. The diminishing returns on investment in defence relative to offence are especially conspicuous when considering the disparity between "hacking" and "patching" in complexity, cost, and time required. For example, a sophisticated network defence software contains between 5 million and 10 million lines of code, whereas an average attack malware contains an average of 170 lines of code. Also protection of critical government networks typically requires standard government competition and contracting, which can take years before solutions are initiated, whereas designing an attack can be accomplished in weeks.[12] While network defence against sophisticated attackers requires advanced work by highly specialised firms, network attack is literally a cottage industry. This, therefore, calls for the examination of cyber warfare with the same intensity with which nuclear warfare was examined during the Cold War.

Cyber Warfare Strategy Conundrums

The governments that are seeking to both strengthen their own national cyber defences and develop offensive cyber techniques and weapons that can be used against adversaries are faced with a conundrum arising from the unique nature of the cyber domain. Pursuing the usual offence–defence equations in this regard is likely to have an impact outside of the military domain because the same software and hardware is being used across military, commercial and civilian applications. Furthermore, it is very likely that any useful exploits that the armed forces or NTRO discover in

12. David C. Gompert, Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint* (US: National Defense University, 2011), p. 132.

developing offensive cyber weapons could also be used against their own systems or other government and private institutions, posing a strategy dilemma of either favouring cyber offence or cyber defence.

To understand the development and deployment of cyber weapons, and create the choice between cyber offence and defence, some lessons from the case analyses of the first public demonstration of a cyber weapon, the 'Stuxnet', would serve a good purpose.

CHARACTERISTICS OF A MODERN CYBER WEAPON

The Stuxnet Case Analysis

Originally detected by security researchers in June 2009, the Stuxnet malware was used to target the Iranian nuclear enrichment facility at Natanz. The Stuxnet attacks consisted of multiple versions of a complex Microsoft Windows malware discovered up to mid-2010 with the main target being the centrifuges used at Natanz for enriching uranium. To affect the centrifuges, Stuxnet needed to infect computers known as Industrial Control Systems (ICS) used to programme and control the Programmable Logic Controller (PLC) devices which, in turn, controlled the frequency converter drives that ran the centrifuges.[13] This meant that Stuxnet first needed to exploit vulnerabilities in the host operating system to infect the overall machine, exploit vulnerabilities in the application software for the PLCs, exploit vulnerabilities in the PLCs themselves, and, finally, command the frequency converters in a way that damaged the centrifuges.[14]

Failure of 'Air Gap' Panacea

The first major hurdle in executing the attack was that the ICS computers that Stuxnet needed to infect were not connected directly to the internet. Like the Indian Air Force's (IAF's) Air Force Net (AFNET), the Indian

13. "W32.Stuxnet Dossier", Symantec, ver. 1.4, 2011, <http://securityresponse.symantec.com/en/id/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>.
14. "Enumerating Stuxnet's Exploits", Langner Communications, June 7, 2011, <www.langner.com/en/2011/06/07/enumerating-stuxnet%E2%80%99s-exploits/>.

Navy's Navy Enterprise Wide Network(NEWN)[15] and the Indian Army's Army Wide Area Network (AWAN), the Iranians had also implemented a common security protocol called "air gapping" (i.e. physical, electrical and electromagnetic isolation) to insulate them from other systems and, in particular, the internet. However, operators still needed a way to update the software on these computers as we update our 'stand-alone' Personal Computers (PCs) and transfer data to and from them. This was done using USB flash drives, which should not have been done. Therefore, the Stuxnet was designed accordingly and was unleashed in three different waves against five different organisations with a presence in Iran.[16] Over a period of time, Stuxnet spread within and between networks until finally it reached the ICS computers, where the payload executed.

Drawing a parallel with the incident, the IAF, Indian Army and Indian Navy operate their computer networks as 'air gapped' from each other and from the internet to ensure network security, however, they have an operational necessity to access and transfer data across multiple networks to achieve their mission. This need, in many cases, puts pressure on combatants to bypass the security features and Standard Operating Procedures (SOPs), thus, promoting the use of devices such as flash drives/ CDs/DVDs between the networks. The IAF has very stringent SOPs for transfer of data between the AFNET and internet; however, incidents of violations keep getting reported.

Advantage Zero Day Exploits

Another observation highlighting the vulnerability of Microsoft Windows monoculture is that Stuxnet took advantage of four zero-day exploits[17] in Windows to infiltrate its targets. The first version of Stuxnet, discovered in June 2009, took advantage of a remote code execution vulnerability in

15. http://articles.janes.com/articles/Janes-Military-Communications/Navy-Enterprise-Wide-Network-NEWN-India.html
16. Ibid., p. 9.
17. Zero-day exploits (actual software that uses a security hole to carry out an attack) are used or shared by attackers before the developer of the target software knows about the vulnerability. http://en.wikipedia.org/wiki/Zero-day_attack

the Windows Print Spooler Service.[18] This vulnerability had been previously disclosed by the security magazine *Hakin*[19] in April 2009, but was not patched by Microsoft until September 2010.[20] Also, a new version of Stuxnet, discovered in March 2010, exploited a previously unknown remote code execution vulnerability in the way Windows handles shortcut or link files.[21] Microsoft issued a security advisory for this vulnerability in July 2010 and a patch to fix it in August 2010.[22] The security firm Symantec privately disclosed two other privilege escalation vulnerabilities to Microsoft as a result of Symantec's analysis of Stuxnet.[23] Probably, Stuxnet's team had discovered these vulnerabilities in Windows and the other parts of the system in the process of development or they had a library of publicly unknown exploits to choose from. Whatever be the case, the more important point is that these vulnerabilities were kept secret and not disclosed to Microsoft. This brings us to the point that the compartmentalisation of cyber offence teams from cyber defence teams is very likely to happen and this would leave many millions of computers owned by governments, companies and private citizens around the world vulnerable to the same exploits, as happened in this case.

Compartmentalisation of cyber offence teams from cyber defence teams is very likely to happen and this would leave many millions of computers owned by governments, companies and private citizens around the world vulnerable.

Minimising Collateral Damage

Another aspect of cyber weapons is their newly acquired ability to restrict collateral damage. Unlike many other types of malware or worm, Stuxnet

18. Ibid., p. 4.
19. Ibid., p. 4.
20. See "Microsoft Security Bulletin MS10-061 - Critical", Microsoft, September 14, 2010, <www.microsoft.com/technet/security/Bulletin/MS10-061.mspx>.
21. "W32.Stuxnet Dossier", n. 13, p. 4.
22. "Microsoft Security Bulletin MS10-046 - Critical", Microsoft, August 2, 2010, <www.microsoft.com/technet/security/bulletin/MS10-046.mspx>.
23. "Updated W32.Stuxnet Dossier is Available", Symantec, updated February 14, 2011, <www.symantec.com/connect/blogs/updated-w32stuxnet-dossier-available>.

took considerable steps to limit its spread as it only spread via USB flash drives and within a Local Area Network (LAN), and each infected device was limited to infecting three others.[24] Stuxnet also contained a code for "self-destruct", and on June 24, 2012, it did so.[25] This indicates the short life span of cyber weapons when compared with kinetic weapons. On the other hand, despite its non-proliferating design, the Stuxnet had infected over 100,000 hosts in 155 countries as of September 2010, highlighting the inherent property of ICT to spread unhindered,[26] albeit the spread occurred because of the still unpatched vulnerabilities in Windows and the widespread carelessness in the use of USB flash drives.

Surgical Strike Capability

Although Stuxnet infected many systems, there is no evidence that it disrupted or damaged any systems outside of Iran. The final analysis of the Stuxnet code has shown that its payload was designed to execute only against specific ICS computers used for the Iranian centrifuges at Natanz. This kind of precision was not seen in earlier versions of cyber weapons. The assigned target for Stuxnet was the Windows machine that was running the Step 7 software used to control the PLC manufactured by Siemens Corporation. To make it more precise, the PLC needed to be a Siemens model 6ES7-315-2 controlling at least 33 frequency converter drives, manufactured by Fararo Paya in Tehran or by Vacon in Finland, running between 807 and 1,210 Hz.[27] This surely requires substantial intelligence gathering, reconnaissance and targeting effort and that is not possible without strong funding support to such operations.

Propagation Dynamics

The reverse engineering effort required to reproduce the cyber weapons is minimal. Once the weapon is released and becomes public, it is possible for

24. "W32.Stuxnet Dossier", n. 13, p. 10.
25. http://news.antiwar.com/2012/06/25/stuxnet-attack-over-as-worm-self-destructs/
26. "W32.Stuxnet Dossier", n. 13, p. 5.
27. Ibid., and Dale G. Peterson, "Langner's Stuxnet Deep Dive S4 Video", *Digital Bond*, January 31, 2012, <www.digitalbond.com/2012/01/31/langners-stuxnet-deep-dive-s4-video/>.

anyone with the tools and motivation to discover how it worked. And, as usually is the case, it takes months to years to patch the vulnerabilities it used, so the hackers take advantage to perpetrate organised crime during this time lag. For instance, Microsoft reported a massive spike in the number of malware infection attempts using the same shortcut/link exploit used by Stuxnet by the end of July 2011.[28] These attempts were especially prevalent in Brazil and the United States, which was not so earlier. Presently, there are other malwares in the wild, known as Duqu and Flame, which bear a striking resemblance to Stuxnet, leading some security researchers to believe they are from the same developers or were built by reusing key parts of Stuxnet.[29] While the *Wall Street Journal* believes that Stuxnet was developed by the Central Intelligence Agency (CIA), with the help of the Department of Energy and Israeli hackers,[30]there are all indications that these have been created by a nation-state.[31]

WHY INDIA SHOULD PURSUE 'OFFENSIVE CYBER WARFARE'

Besides what the Stuxnet analysis shows, there is enough evidence suggesting the lethality of cyber weapons of mass disruption across the globe. In 1997, a teenager shut down air and ground communication at a US airport in Massachusetts, and in 2000, the Russian government announced that hackers had succeeded in taking control of the world's largest natural gas pipeline network, Gazprom, by using a type of Trojan. In 2000, Vitek Boden took control of a sewage pumping station in Australia. He remotely triggered the release of a million litres of sewage into public waterways.[32] Computers and manuals seized in Al Qaeda training camps contained large

28. Holly Stewart, "Stuxnet, Malicious .LNKs, ... and Then There was Sality", Microsoft Makware Protection Centre, July 30, 2010, <http://blogs.technet.com/b/mmpc/archive/2010/07/30/stuxnet-malicious-lnks-andthen-there-was-sality.aspx>.
29. "W32.Duqu", Symantec, ver. 1.4, November 23, 2011, <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf>.
30. http://online.wsj.com/article/SB10001424052702304821304577440703810436564.html?mod=googlenews_wsj
31. Dr Hamadoun Toure, head of the UN telecommunications agency, told the BBC. *Huffington Post* UK | By Michael Rundle Posted: 07/06/2012 17:04 Updated: 07/06/2012 17:26.
32. Garry Barker, "Cyber Terrorism a Mouse-Click Away" *The Age*, July 8, 2002. http://www.theage.com.au/articles/2002/07/07/1025667089019.html

Offensive cyber warfare as a means of strategic balancing is based on the basic premise that cyber warfare is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance.

amounts of SCADA[33] information related to dams and critical infrastructure. In 2003, the Slammer Worm took a US nuclear power plant's safety monitoring system offline, and the Blaster Worm was connected with a massive blackout in the eastern US.[34] Of late, the world also witnessed the rising level of sophistication, lethality and precision in the modern cyber weapons in the form of Stuxnet[35], Duqu[36], Flame, etc.

The reason why India should pursue offensive cyber warfare as a means of strategic balancing is based on the basic premise that cyber warfare is capable of causing massive damage with little funding, it is difficult to detect and defend against, it provides a high level of deniability, and it eliminates the problem of geographical distance. An offensive approach to cyber warfare is a favourable option considering India's prowess (though not fully oriented towards warfare!) in this domain. By developing offensive capability, India would be able to mitigate if not neutralise the asymmetries of China's Anti-Satellite (ASAT) capability, or its Electro-Magnetic Pulse (EMP) capability. While India, China and Pakistan are nuclear weapon states, the human rights and environmental concerns have relegated these weapons to the role of deterrent, resulting in the emergence of limited warfare. By using cyber warfare, India could achieve the same asymmetric destructive power, while bypassing the drawbacks.

33. SCADA stands for Supervisory Control and Data Acquisition. It generally refers to an industrial control system: a computer system monitoring and controlling a process. The process can be industrial, infrastructure or facility-based as Industrial processes, infrastructure processes or facility processes. http://en.wikipedia.org/wiki/SCADA
34. David Maynor, and Robert Graham. "SCADA Security and Terrorism: We're Not Crying Wolf," *X force, Internet Security Systems*, 2006 http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.
35. http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml
36. http://www.crysys.hu/publications/files/bencsathPBF11duqu.pdf

Offensive Cyber Warfare to Counter China's ASAT

ASAT is being considered as an emerging threat to space-based assets. India's technology and capability gap on this account could be bridged by leveraging cyber warfare capabilities till such time it acquires such capabilities. **Cyber warfare enables effecting far more devastating attacks on satellites by knocking out the corresponding relay stations on earth.** India's focus should be to on neutralising the uplinks and downlinks of the space-based systems of adversaries through diverse forms of cyber attack including the simple Denial of Services (DoS) attack. This would give India the advantages of deniability and low cost. It would also remove distance from the equation, allowing multiple targets to be taken out simultaneously, regardless of location, and it would remove international condemnation and/or involvement.

On the other hand, the use of kinetic kill weaponry, such as China's direct ascent ASAT to disrupt space-based assets has many disadvantages. Firstly, while India's Indian Regional Navigational Satellite System (IRNSS[37]) that would provide surveillance, tactical communication and precision navigation makes it a desirable target, the attack surface would not be limited to a single satellite; rather, it would be a constellation of seven satellites. When one is destroyed, others can be manoeuvred to fill holes in the net. Secondly, at any given time, not all of these satellites are within striking range. This means a sky clearing operation would take a significant amount of time, thereby revealing Beijing's intentions. Thirdly, it would risk retaliation and international pressure, putting China at a disadvantage and, finally, there is no guarantee that such an attempt would be successful, as each launch requires precise targeting, and China's ASAT has only been tested once.

Cyber Offensive as an Alternative to Nukes

Going purely on the capability basis, India could destroy a vast majority of China's electronics, including computers, cars, phones, and the power

37. http://en.wikipedia.org/wiki/IRNSS-1'the IRNSS-1 expected to be launched on board PSLV-HP by May/June 2013'

grid, using an EMP burst through high altitude nuclear explosions with as few as three nuclear bombs, like any other nuclear armed state could, and against Pakistan the effort required would be much less. In fact, it is now public that the US, China, France, and Russia all are using an EMP burst as a surprise first strike in war-games, as reported by numerous sources.[38] However, such brute-force tactics would cause international outrage as an EMP burst violates an international treaty, it damages the environment, and it indiscriminately disrupts everything in its blast radius. Alternatively, shutting down China's power grid, production lines, water utilities, chemical plants, telecommunications, and transportation routes is possible through cyber attack, and it would provide the benefit of deniability also.

Offensive Cyber Warfare for Technology Leapfrog

ICT is a key enabler for the developed countries; for emerging nations like India, it offers a great possibility to leapfrog many competitors, and for those still in the agricultural age, it offers the ability to conduct asymmetric operations.[39] Espionage and technology transfer prosper in cyber warfare, where being physically present is not required, and attribution becomes increasingly difficult. Although it does not fall strictly in line with India's non-coercive and rather submissive approach to security strategy, cyber warfare allows acquisition of foreign military knowledge, to quickly catch up and begin working at a comparable level, rather than investing large amounts of time and effort to acquire this knowledge independently. While India has been subjected to large scale and complex espionage operations, involving exfiltration of thousands of classified and sensitive government

38 Hearing on "China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities" Tuesday, May 20, 2008, Room 562, Dirksen Senate Office Building First Street and Constitution Avenue, NE Washington, DC 20510. http://www.uscc.gov/hearings/2008hearings/agenda/08_05_20agenda.pdf; Liang Qiao and Xiangsui Wang. *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999). http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf; Bartlett, Roscoe. "Nuclear Electromagnetic Pulse", *US Congressional Record*, June 9, 2005. http://cryptome.org/bartlett-060905.txt www.icnnd.org/research/New_Weapons_Technology.pdf

39. Jason Andress and Stev Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Elsevier Inc, 2011), ch 1, p. 9.

documents[40], **it is about time to extrapolate Chanakya's idea of having a great deal of emphasis on spies, grouped into a separate organisation directly reporting to the king,**[41] **in the cyber domain.**

As an empirical observation of international politics, the nation-states with a proven history of cyber espionage do not necessarily attract sanctions or get subjected to international pressures as long as they are able to propel their economy and enhance the interdependence of the world economy. The case in point is China, where in spite of evidence of mass exfiltration of Research and Development (R&D) data, political intelligence and intellectual property from the EU, US and India by online espionage activities, Europe still supplies technology to China, and the EU has a regular dialogue with China.[42]

Offensive Cyber Warfare for Power Projection

India currently lacks the cyber power projection to protect its National Critical Information Infrastructure (NCII) from disruption. Online technology transfer and the further development of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) are crucial to extend this power projection. Online Psychological Operations (PSYOPS) and media warfare would also enhance India's soft power.

Offensive Cyber Warfare to get Military and Financial Edge

In 1991, having faced the balance of payment crisis, India opened the doors to the new neo-liberal policies, including opening for international trade and investment, deregulation, initiation of privatisation, tax reforms, and inflation-controlling measures. Since then, it has seen a sustainable economic growth. Economic growth is critical to military development;

40. Wing Cdr M.K. Sharma,*Cyber Warfare: The Power of the Unseen* (New Delhi: KW Publishers, 2011) ch. 6, pp.192-199.
41. Wing Cdr (Dr) R. Venkataraman Ph.D, *India's Higher Defence: Organisation and Management* (New Delhi: KW Publishers), ch. 1, p. 15.
42. Pieter D. Wezman and Matieu Gilles Duchatel, " CAPS-SIPRI Roundtable Discussion", Centre for Air Power Studies, New Delhi, March 20, 2013.

The information revolution has given more power to individuals and increased globalisation through the interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types.

economic growth creates a greater energy demand, which, in turn, creates a greater military demand, thus, the two form a positive feedback loop,[43] of which India should take full advantage.

The information revolution has given more power to individuals and increased globalisation through the interconnectedness of economies, rapid dissemination of news, and improved access to communication and information of all types. To compete on a global level without the use of these technologies would place India at a significant military and economic disadvantage. For this reason, the benefits of economies becoming electronically reliant outweigh the risks involved, and it is imperative for any growing economy to embrace this technology. Therefore, to benefit from the positive feedback loop of economic growth and military development, India must be able to guard its assets against cyber attacks. Further, it is impossible for a nation to develop a defence against cyber warfare without simultaneously learning how to execute attacks itself.

IN THE DEFENCE OF 'CYBER DEFENCE'

The main objective of our national security policy is the defence of the sovereignty and integrity of India. Thus, we develop/procure weapons primarily to safeguard the nation and not for extending our hegemony over various domains such as land, sea, air space and cyber space. While this seems quite logical, there are those who would profess that the best form of defence is offence. They believe that the capability of destroying the enemy by an preemptive attack would outweigh the requirement for a defensive strategy. This approach has proved to be dangerous and costly to

43 John G. Ikenberry,. "The Rise of China and the Future of the West", *Foreign Affairs* , January/ February 2008. http://www.foreignaffairs.org/20080101faessay87102-p0/gjohn-ikenberry/ the-rise-of-china-and-the-future-of-the-west.html.

many nations in the history of warfare. In the 1950s, the US Air Force Gen Curtis LeMay as Commander of the Strategic Air Command convinced RAND Corporation analysts that his bombers would not be destroyed on the ground by a Soviet attack because "we are going first". Another strategic fallout of the same argument was when the Bush Administration justified post 9/11 that it would be too expensive to defend the US against a terrorist attack at home so "we need to go out to the source"[44]. Hence, the global war on terror that burdened the US with two wars over a decade, over US$ 2.4 trillion and, of course, the loss of more than 5,000 American lives.

The capability of destroying the enemy by an preemptive attack would outweigh the requirement for a defensive strategy.

In the cyber domain, there are a few compelling factors for India that make a strong case for a defensive strategy, at least for the coming decade. Firstly, India's gaping vulnerabilities because of the growing dependence of its National Critical Infrastructure (NCI) on ICT with no comprehensive national cyber defences. This needs to be seen in the light of recent incidents of Chinese exfiltration of sensitive government data and the possibility of them helping Pakistan to provide highly capable hackers in the future. Secondly, the comparative importance of defences could be argued on the premise that even if our cyber offensive capability is able to disrupt/ degrade/ manipulate / corrupt the enemy Air Defence (AD) network/ banks/financial institutions, etc but our NCI is under attack [say the Bombay Stock Exchange / National Stock Exchange (BSE/NSE) is put down or the data therein is manipulated or the banking system is degraded for weeks together], the cost of such loss of faith of the populace in the system and the inconvenience would have a far more grave effect on democratic India than it would have on, say, the Chinese government for a similar attack on them. Thirdly, increased vulnerabilities to cyber attack lead to self-deterrence and, thus, likely reluctance to use even our superior conventional weapons in a conflict situation. Fourthly, **with our undefended NCI under attack, we**

44. Clark and Knake, n. 3, ch. 5,.p. 158.

would be forced to escalate in a cyber conflict very quickly. We would need to be more aggressive in knocking down enemy information systems to prevent further damage to our NCI. Fifthly, unlike a conventional offensive, in the cyber domain, you cannot destroy all the enemy's offensive capability, as the cyber weapons may already be in Indian cyber space and just need a trigger. Finally, lack of cyber defences could widen the already existing strategic power imbalance between India and China.

For example, if China is able to demonstrate that it can exploit the vulnerabilities of India's NCI, implying the possibility of greater damage, it would increase the credibility of China not only in the India-China military calculus but also in the US-China military, economic and political balance. Ironically, in such a scenario, a higher level of cyber attack capability is not likely to improve the imbalance in favour of India. Therefore, to reduce the risk of any nation threatening to use cyber weapons against it in a crisis, India must have credible cyber defences. Having assured defence, India should be able to deter its adversaries on the basis of offensive cyber warfare capabilities so developed based on broad-based technical Intelligence, Surveillance, Reconnaissance (ISR) and precise targeting of the potential adversary's NCI 'attack surface' spread over both civil and military cyber space.

Cooperation and Coordination Compulsion

Increased cooperation and coordination among and within nation-states—amongst the armed forces, private industry and academia—forms a significant element of cyber defence. Today, the private sector represents a significant part of the NCI attack surface which is required to be protected. Many computer systems of the NCI widely use commercial software applications and architectures, thus, making the protection of NCI partly reliant on discovering and fixing of vulnerabilities in commercial software.

Academics already play a significant role in the cyber security world, but efforts by researchers are often hindered by corporations and governments

because they are seen as a threat and not an asset.[45] This would need to change, and the cyber community would need to adopt a favourable attitude towards any research and experimentation that leads to a better understanding of cyber vulnerabilities and weaknesses in security architectures. The public is often overlooked but plays a potentially significant role in cyber defence. The many millions of personal computers are potential weapons that can be compromised by an attacker and turned into weapons, for example, as part of a botnet running a denial of service attack. Compromised personal computers, mobile devices or online accounts of government officials and corporate executives could provide critical information that leads to the compromise of protected systems. Friends and relatives on social networks are also potential avenues of attack, potentially more likely to succeed because of their trusting nature.

Thus, policies aimed at improving a nation's cyber defence would necessarily need to increase the amount of information-sharing among governments, industry, academia and potentially even the public, and make major changes in the current classification policy for cyber vulnerabilities and attacks. Governments, industry and academia would need to share information about the latest attacks, malware signatures and vulnerabilities.[46] Incentive programmes for the responsible disclosure of vulnerabilities, such as those already being run by Google and the Mozilla Foundation for their respective web browsers,[47] could greatly increase the number of people looking for vulnerabilities and the rate at which they are discovered and fixed. However, these approaches would also have an increasingly negative impact on the ability of a state to develop and field offensive cyber capabilities over time, largely through the increased cost

45. Jaikumar Vijayan, "Carrier IQ Drops Legal Threat Against Security Researcher", Computerworld, November 28, 2011, <www.computerworld.com/s/article/9222203/Carrier_IQ_drops_legal_threat_against_security_researcher>.
46. Jason Healey, "Cybersecurity Legislation Should Force U.S. Government to Listen Less and Speak More", *The Atlantic*, March 15, 2012, <www.theatlantic.com/technology/archive/2012/03/cybersecurity-legislationshould-force-us-government-to-listen-less-and-speak-more/254491/>.
47. "Encouraging More Chromium Security Research", The Chromium Blog, January 28, 2010, <http://blog. chromium.org/2010/01/encouraging-more-chromium-security.html>; and "Bug Bounty Program", Mozilla, February 1, 2012, <www.mozilla.org/security/bug-bounty.html>.

of finding new vulnerabilities and developing offensive weapons against them even as they are being patched.

CYBER DETERRENCE: IS IT WORTH IT?

Learning from the previous wars and extrapolating this knowledge to the realm of cyber space, cyber deterrence seems to be the natural good idea like missile deterrence and nuclear deterrence proved to be effective strategy in the past.[48] But, the peculiarity of cyber attacks is that they are enabled not through the generation of force but by the exploitation of the enemy's vulnerabilities. Permanent effects are hard to produce unlike traditional military action through conventional or unconventional means. So is it fair to draw a direct analogy between nuclear deterrence or traditional military deterrence and cyber deterrence wherein we may not know exactly who did it? Or what is the assessment of collateral damage due to interdependence on target infrastructure? Or how much are we prepared to absorb of a retaliatory cyber attack?

Another difference in the notion of deterrence in cyber space is that something that works today may not work tomorrow (indeed, precisely because it did work today). Thus, deterrence and war-fighting tenets established in other media do not necessarily translate reliably into cyber space. Such tenets must be rethought.

Cyber Deterrence: The Attraction

The attraction of cyber deterrence is that, if it works, it can reduce the cost of defending systems. Instead of having to put money into making systems more secure, the defender inhibits the attacker's efforts by threatening retaliation against successful attacks.[49] So if an attacker can be persuaded to reduce its efforts in the face of punishment, the money thus saved by the defender that would have been spent on the security (to achieve the same level of assurance) is worth considering.

48. During the Cold War, the nuclear stand-off between the US and Soviet Union never went out of control. This provides the historical basis for believing that cyber deterrence should work.
49. Martin C. Libicky, *Cyber Deterrence and Cyberwar* (RAND Project Air Force,2009), ch.3, p. 42.

As with any other type of deterrence, the aim of cyber deterrence would be to reduce the risk of cyber attacks to an acceptable level and at an acceptable cost. And if this aim could be achieved through cyber security measures alone, then why build cyber deterrence systems at an additional cost? The problem with cyber security is that there is nothing like total security and near total security too may be achieved at prohibitive costs. For instance, the expenditure of US organisations on information security easily measures in tens of billions of dollars a year yet security breaches occur daily.[50] This is why the US President's budget request allots more than $13 billion to cyber programmes, nearly 16 percent of a federal Information Technology (IT) budget totalling about $82 billion.[51]Therefore, cyber deterrence becomes an absolute necessity.

Cyber Deterrence for Buying Time

India seeks to maintain domestic and regional stability while developing its economic, military, technologic, scientific, and soft power. It also seeks a balance between military and economic development, believing they are mutually dependent. At this juncture, while India tries to equitably match its military power with China, it could buy time by keeping a low profile and depending on cyber reconnaissance. Cataloguing adversary weaknesses not only provides an asymmetric advantage in the event of a conflict, it also acts as a deterrent while India catches up with its military modernisation drive.

Cyber Posturing: A Potent Foreign Policy Instrument

For India, cyber posturing could be a potent foreign policy instrument. **Unlike conventional military deterrence, in cyber space, the acquired offensive capabilities do not necessarily have to reside in military organisations**. India's prowess in IT and IT Enabled Services (ITES)

50. Dawn S. Onley, "Army Urged to Step Up IT Security Focus," *Government Computer News*, vol. 1, no. 1, September 2, 2004.
51. http://www.washingtonpost.com/business/on-it/obamas-budget-proposal-would-increase-spending-on-cybersecurity/2013/04/14/218e71d6-a2b8-11e2-be47-b44febada3a8_story.html

Cyber warfare strategy would include India's take on employing cyber offensive, building up cyber defences and conveying cyber deterrence power to the adversaries.

could be leveraged to build cyber deterrence capabilities to gain asymmetric advantage against militarily mightier potential adversaries. Here, the concept of employing week-end cyber warriors on cyber warfare projects is worth considering.

STRATEGY OPTIONS FOR INDIA

Cyber warfare strategy would include India's take on employing cyber offensive, building up cyber defences and conveying cyber deterrence power to the adversaries. This would be supported by a cyber security strategy to enable cyber capability building that remains at the core of the issue. Towards this, cyber security strategies proposed to be adopted during the Twelfth Five-Year Plan include:

- Enhancing the understanding with respect to factors such as dynamically changing threat landscape, technical complexity of cyber space and availability of skilled resources in the area of cyber security,
- Focus on proactive and collaborative actions in public-private partnership.
- Enhancing awareness and upgrading the skills, capabilities and infrastructure.
- Improving interaction and engagement with various key stakeholders.
- Carrying out periodic cyber security mock drills to assess the preparedness of critical sector organisations to resist cyber attacks and improve the security posture.
- Supporting and facilitating basic research, technology demonstration, proof of concept and testbed projects in thrust areas of cyber security through sponsored projects at recognised R&D institutions.

Six focus areas have been identified for implementation of the cyber security activities. These are: Enabling Legal Framework, Security Policy, Compliance and Assurance, Security R&D, Security Incident – Early Warning and Response, Security Awareness, Skill Development and Training and

Collaboration.[52]

Pursue Cyber Research to Create Cyber Resource

If there could be any single approach that could be called the 'silver bullet' to deal with cyber warfare, it would be to create cyber resources. There is no point in crafting a strategy without having resources in that domain. Cyber research is the key to creating resources in all cyber sub-domains such as cyber power, cyber space, cyber strategy, institutional issues, cyber assessment and cyber policy.

- *Cyber power research* needs to, firstly, adequately assess the relative worth of cyber assets in the political, economic and social levers of national power. Secondly, at the military level, it is important to not only focus on the benefits of cyber power but also to carry out military risk assessment of relying on cyber space. This would require development of intellectual capability, methodology, tools and data collection. Lastly, the armed forces are required to quantify the future cyber conflict scenario with potential adversaries.
- *Cyber space research* is aimed at identifying and projecting the future technologies that have the potential of substantially altering the performance of the cyber space. Working on such technologies/ architectures would provide technology leadership to India while providing better protection to essential data in cyber space.
- *Cyber strategy research* would deal with challenges posed by various entities/actors that are cyber empowered. This would deal with the vital questions of adopting cyber offence, cyber defence or cyber deterrence approaches. Research is also required to investigate the feasibility of collective development of 'tailored cyber deterrence' say by the BRICS (Brazil, Russia, India, China and South Africa) nations, firstly, to create common understanding and interdependence and, secondly, to communicate such a concept to potential adversaries.

52. N. Sitaram, Distinguished Scientist & Former CC (R&D), DRDO, Twelfth Five-Year Plan (2012 – 17) Information Technology Sector, Government of India Ministry of Communications & Information Technology, Department of Information Technology, p. 4.

Cyber assessment research is needed to upgrade from rudimentary ways of cyber power assessment to developing analytical methods and tools for more objective and realistic assessment of our own and the adversary's cyber power.

- *Institutional issues research* is required to bridge critical gaps in the areas of internet regulation, e-governance, information sharing architecture, and legal issues. The ICT infrastructure must be regarded as an 'ecosystem' in which everything is interconnected. It functions as a whole; it must be defended as a whole.[53]
- *Cyber assessment research* is needed to upgrade from rudimentary ways of cyber power assessment to developing analytical methods and tools for more objective and realistic assessment of our own and the adversary's cyber power. This obviously demands huge intellectual capital to address the issues of cyber infrastructure and cyber strategy.
- *Cyber policy research* would iron out many contentious issues related to major policy, including the legal framework, e-governance and international cooperation on information sharing, etc.

Cyber Reconnaissance: A Strategic Tool

Cyber reconnaissance appears to be the most beneficial tool of cyber warfare. Beyond finding exploitation points in the attack surface of adversaries for future attacks, the commercial sector allows India the opportunity to skip generations of research and development efforts, levelling the playing field in science and technology, and boosting economic and military might. This boundaryless military operation, could provide access to the mind of the enemy on any issue, including how he thinks on human rights issues in relation to soft power, globalisation, international condemnation, and the legal apparatus.

The relative ease with which the Titan Rain attacks were conducted makes the private sector computer networks look like an easy target.[54]

53. Toomas Hendrik Ilves, President of Estonia, "Cyber Security: A View from the Front", *International Herald Tribune*, April 12, 2013.
54. Marcelo Almeida, "Cyberwar: The Beginning" *Rand Corporation Monograph*, July 2006.http://www.rand.org/pubs/monograph_reports/2005/MR580.pdf. http://www.zone-h.org/index.php?option=com_content&task=view&id=13932& Itemid=30&msgid=710.

While the government and defence installations are heavily funded for security, the private sector is not. Many of these systems do not support authentication, encryption, or basic validation protocols; of those that do, most run with security features disabled. The vulnerability of the private sector's computer network, due to a lack of understanding or a lack of incentive, provides India with the opportunity to cripple the adversary's civil information infrastructure.

For instance, Hugo Teso a security consultant at n.run, Germany, demonstrated that one could manipulate the steering of a Boeing jet in auto pilot mode, make oxygen masks drop down and even cause the plane to crash by setting it on a collision course with another plane.[55] Firstly, the Automated Dependent Surveillance Broadcast (ADS-B) which is a surveillance technology used for tracking the aircraft is unencrypted and unauthenticated and has no cyber security. Secondly, the Aircraft Communication Addressing and Reporting System (ACARS) which is used for exchanging messages between the aircraft and stations via radio or satellite also has no security features.

Increase Hardware and Software Market Share

India should seek to gain a market share in the production of ICT software and hardware as a means of increasing its cyber warfare capability. On the infrastructure level, India could seek to increase ownership of submarine cable infrastructure, allowing it further access to cyber reconnaissance or the option of shutting down portions of internet connectivity during times of war.

Build Espionage Backbone

India must also grow in the field of microchips, something that other countries need for defence related electronics. Not necessarily for embedding exploits, but dominance in this field would give India access to critical individuals and information through partnership, come close to sensitive information and hardware when needed and conduct social engineering or Human Intelligence (HUMINT). Fears of international pressures or

55. Sophie Warnes, "Control an Aircraft with an Android Phone", *The Times of India*, April 14, 2013.

sanctions for adopting this approach, as some would believe, may not be well placed. Empirically, for instance, despite ample clear indications of many cyber espionage operations to exfiltrate R&D, design and political sensitive data on a large scale from all over the world, including the EU countries, US and Asian nations, China continues to have improved trade relations and technology transfer agreements with the EU and US. The key here seems to be creation of economic interdependence.

CONCLUSION

As a starting point to deal with the cyber challenges, India should take concurrent steps at the strategic, operational and tactical levels. The strategic level approach must be based on building strong defences ensuring resilience of the National Critical Infrastructure (NCI). At the operational level, we must develop credible cyber offensive capability employed in rigorous in-house experimentation, simulation and exercises that would be deployed against a highly advanced cyber adversary. Lastly, the tactical level actions would look into the mission oriented approach to influence military operations that would integrate the physical, information, social and cognitive domains together to execute Net-Centric Operations (NCO).

In essence, while we develop a national strategy on cyber warfare, we must create cyber resources and procedures simultaneously that would contribute towards achievement of specific national security objectives. Those resources would be technological, organisational and human, employed for cyber offence, cyber defence, cyber deterrence or combinations of these. **Without the creation of cyber resources, the cyber strategy is like having an air strategy without having aeroplanes**. The strategy must be based on partnership given the inseparability of private, government and military cyber space. The armed forces are becoming increasingly dependent on the private sector for development, maintenance and security of national cyber space capabilities. In many ways, we are facing something more like the Cold War where cyber espionage and spending on cyber warfare are the missiles that will determine the outcome of future conflicts.

GEO-POLITICAL PERSPECTIVE: TIBET

RAJ MONGIA

INTRODUCTION

A region in the far reaches of the Himalayas, Tibet looms large in the popular imagination. It is the original home of the Dalai Lama, one of the great spiritual leaders of our time. Tibetan Buddhism inspires millions worldwide with the twin values of wisdom and compassion. The Chinese takeover of the country six decades ago also shows another side of Tibet – that of a passionate symbol of freedom in the face of political oppression. International sympathy has kept the Dalai Lama's appeals for autonomy on the world's political agenda, but in the light of China's political and economic gains, there is fear that Tibet is in danger of being forgotten by the world. As the Dalai Lama grows older and China threatens to intervene in the selection of Tibet's next spiritual leader, many wonder whether there is any hope for the cause of Tibet or will it become a casualty of globalisation .[1]

GEOGRAPHY OF TIBET

The geography of Tibet consists of the high mountains, lakes and rivers lying between Central, East and South Asia. Traditionally, Western (European and American) sources have regarded Tibet as being in Central Asia, though today's maps show a trend toward considering all of modern China, including Tibet, to be part of East Asia. Tibet is often called "the roof

---

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

1. Diane Wolff, *Tibet Unconquered: An Epic Struggle for Freedom* (Palgrave Macmillan, 2010), pp. 1-5.

As the Dalai Lama grows older and China threatens to intervene in the selection of Tibet's next spiritual leader, many wonder whether there is any hope for the cause of Tibet.

of the world," comprising tablelands averaging over 4,950 m above the sea, with peaks at 6,000 to 7,500 m, including Mount Everest, on the border with Nepal.

It is bounded on the north and east by the Central China Plain, on the west by the Kashmir region of India and on the south by Nepal, India and Bhutan. Most of Tibet sits atop a geological structure known as the Tibetan plateau which includes the Himalayas and many of the highest mountain peaks in the world. High mountain peaks include the Changtse, Gurla Mandhata, Jomolhari, Gyachung Kang, Gyala Peri, Mount Kailash, Kawagebo, Khumbutse, Melungtse, Mount Nyainqentanglha Namcha Barwa, Mount Nyainqentanglha, Shishapangma and Yangra . Mountain passes include Cherko la, and North Col. Smaller mountains include Mount Gephel and Gurla Mandhata.[2]

Physically, Tibet may be divided into two parts: the "lake region" in the west and northwest, and the "river region", which spreads out on three sides of the former on the east, south and west. The regional names are useful in contrasting their hydrological structures, and also in contrasting their different cultural uses which is nomadic in the "lake region" and agricultural in the "river region". Despite its large size and mountainous nature, variation of climate across the Tibetan plateau is more steady than abrupt. The "river region" has a sub-tropical highland climate, with moderate summer rainfall averaging around 500 millimetres (20 in) per year, and day-time temperatures ranging from around 7 °C (45 °F) in winter to 24 °C (75 °F) in summer — though the nights are as much as 15°C (25°F) cooler. Rainfall decreases steadily to the west, reaching only 110 millimetres (4.3 in) at Leh on the edge of this region, whilst temperatures in the winter become steadily colder. In the south, the "river region" is bounded by

2. Tsepon Shakabpa, Victor C. Falkenheim and Turrell V. Wylie. "Tibet". *Britannica Online Encyclopedia*. Retrieved March 25, 2013, pp. 5-6.

the Himalayas, and on the north by a broad mountain system. The system at no point narrows to a single range; generally, there are three or four across its breadth. As a whole, the system forms the watershed between rivers flowing to the Indian Ocean – the Indus, Brahmaputra and Salween and their tributaries – and the streams flowing into the undrained salt lakes to the north.[3]

The "river region" is characterised by fertile mountain valleys and includes the Yarlung Tsangpo river (the upper courses of the Brahmaputra) and its major tributary, the Nyang river, the Salween, the Yangtze, the Mekong, and the Yellow river. The Yarlung Tsangpo Canyon, formed by a horseshoe bend in the river where it flows around Namcha Barwa, is the deepest, and possibly longest, canyon in the world. Among the mountains, there are many narrow valleys. The valleys of Lhasa, Shigatse,Gyantse and of the Brahmaputra are free from permafrost, covered with good soil and groves of trees, well irrigated, and richly cultivated. The South Tibet Valley is formed by the Yarlung Zangbo river during its middle reaches, where it travels from west to east. The valley is approximately 1,200 km long and 300 km wide. The valley descends from 4,500 m above sea level to 2,800 m. The mountains on either side of the valley are usually around 5,000 m high. The lakes here include Lake Paiku and Lake Puma Yumco.[4]

The "lake region" extends from the Pangong Tso Lake in Ladakh, Rakshastal Lake, Yamdrok Lake and Mansarovar Lake near the source of the Indus river, to the sources of the Salween, Mekong and Yangtze. Other lakes include Dagze Co, Nam Co, and Pagsum Co. The lake region is an arid and wind-swept desert. This region is called the Chang Tang (Byang sang) or 'Northern Plateau' by the people of Tibet. It is some 1,100 km (700 mi) broad, and covers an area about equal to that of France. Due to the extremely high mountain barriers, it has a very arid alpine climate with annual precipitation of around 100 millimetres (4 in) and it possesses no river outlet. The mountain ranges are spread out, rounded, disconnected, and separated by

3. Yang Qinye and Zheng Du, *Tibetan Geography* (China Intercontinental Press), pp. 30–31.
4. Zheng Du, Zhang Qingsong, Wu Shaohong, *Mountain Geoecology and Sustainable Development of the Tibetan Plateau* (Kluwer, 2000), p. 312.

With the disappearance of independent Tibet and its annexation by China, the strategic setting for India has changed, with far-reaching security implications.

flat valleys of relatively little depth. The country is dotted over with large and small lakes, generally salt or alkaline, and intersected by streams. Due to the presence of discontinuous permafrost over the Chang Tang, the soil is boggy and covered with tussocks of grass, thus, resembling the Siberian tundra. Salt and fresh water lakes are intermingled. The lakes are generally without an outlet, or have only a small effluent. The deposits consist of soda, potash, borax and common salt. The lake region is noted for a vast number of hot springs, which are widely distributed between the Himalayas and 34° N but are most numerous to the west of Tengri Nor (northwest of Lhasa). So intense is the cold in this part of Tibet that these springs are sometimes represented by columns of ice, the nearly boiling water having frozen in the act of ejection.[5]

STRATEGIC IMPORTANCE OF TIBET

The existence of independent Tibet on India's northern borders provided a buffer between the two Asian giants, India and China. With the disappearance of independent Tibet and its annexation by China, the strategic setting for India has changed, with far-reaching security implications. The frontiers which, by and large, were settled with Tibet, were declared disputed all along the 3,440 km by China. Not only India, even Nepal and Bhutan now have borders with China instead of Tibet. China is in possession of 36,846 sq km of Indian territory in Aksai Chin and claims another approximately 93,000 sq km in the central and eastern sectors. India now has to guard two fronts instead of one. The repercussions are an addition to the defence budget and border guarding responsibility. India's defence budget as a consequence has increased by approximately 30 per cent.

5. J. M. Dortch et al, "Catastrophic Partial Drainage of Pangong Tso, Northern India and Tibet", *Geomorphology*, 2010, pp. 3-4.

Around 500,000 Chinese troops and a quarter of China's nuclear arsenal are located in the Tibet Autonomous Region (TAR) and adjoining Tibet's ethnic areas. According to sources, China has constructed missile bases at Kongpo, Nyitri, Powo Tramo, Rudok, Golmud and Nagchuka. Nagchuka seems to have become one of the most important nuclear bases in China. It is reported that there are 7-8 Intercontinental Ballistic Missiles (ICBMs), 60-70 Medium Range Ballistic Missiles (MRBMs) and 15-20 Intermediate Range Ballistic Missiles (IRBMs) located in Tibet.

Tibet provides the ideal site for multiple targeting. There are nearly 15 radar stations and 14 military airfields in the TAR and the adjoining Tibetan ethnic areas. The airfields are kept in a perpetual state of readiness for all types of military and civil aircraft. China has already completed the Golmo-Lhasa railway. The strategic roads have already been upgraded. The rail-road-air infrastructure development, just to support a population of two-three million on the plateau, indicates the objective of creating military capabilities.[6]

China has already gained access to the Indian Ocean with the construction of the Karakoram Highway and projected development of a road from Yunnan through Myanmar. Its access to the Indian Ocean has further improved with the occupation of Tibet. This occupation of Tibet by China has increased China's reach into South Asia with conventional as well as nuclear-tipped missiles. With the missiles deployed in Tibet, all strategic locations in South Asia can be engaged with devastating effects. The airfields in Tibet facilitate mid-air refuelling to mount air attacks on crucial points in South Asia. Engagement of South Asia (particularly India) by China along India's northern borders is a strategic imperative if China is to grow into a regional or global power. China has improved its strategic capability of colluding with Pakistan or with any of India's neighbours against the interests of India. Pakistan's ceding of territory of the Northern Areas (Pakistan Occupied) to China in 1963 is a prominent example in this regard.[7]

6. V.P. Malhotra, *Tibetan Conundrum* (New Delhi: Knowledge World, 2006), pp. 85-88.
7. Ibid., pp. 89-93.

NATURAL RESOURCES

Tibet is rich in mineral resources, particularly strategic materials like uranium, gold, iron, oil, coal and in forests and hydro potential. A scientific investigation has discovered extensive gold fields in the district of Sankora. There are deposits of radium, iron and titanium on the eastern shores of Mansarovar and nearby Rakas Tal, lead near Gebuk on the Manchuan Ho; arsenic and serpentine(a dark green mineral composed of hydrated magnesium silicate taking a high polish and used as decorative material) near Kungri-bingri Pass; and large deposits of borax on the shore of Tseti Tsho (Lake Tseti). The reserves in Tibet and Tibetan ethnic areas are:

- Forty per cent of China's reserves of chromite is in Tibet. Chromite mines are located in Nagchu and Lhoka.
- Tibet contains 14.4 per cent of China's copper reserves. Two of China's copper projects are located at Chamdo and Amdo.
- Tibet has abundant gold reserves, particularly in Amdo (Ngachu, Wulan County, Golok, Markham in Kham and Kandze). Over 1,000 kg of gold is known to have been extracted so far. Ngachu has over 10 tons of alluvial gold and is likely to produce 386 kg of gold annually.
- According to many geologists, Tibet is perhaps the last and the largest oil belt in the continent. The stratum is similar to the oil fields in the Persian Gulf and Karakoram. Tsaidam Basin has oil reserves of 42 billion tons and natural gas reserves of 1,500 billion cubic metres. Natural gas reserves in Tibet and Tibetan ethnic areas alone can sustain China's requirements for seven years. Two hundred million tons of oil has also been found in Chang Tang, in Lhunpula Basin.
- Tibet has large deposits of uranium around the eastern mountainous shores of Koko Nor. Known mines of uranium include Tsaidam Basin, Thewo in Amdo, Yamdrok Tso and Damshung near Lhasa.
- Eighteen million tons of strontium has been discovered in Tsaidam. Strontium is used for nuclear missile cladding.
- Discovery of plutonium in Tsaidam has also been reported.
- Cesium is a rare metal used in military and hi-tech applications, particularly in atomic clocks and as high energy solid fuel. Cesium

deposits worth around $ 6.5 billion have been reported in TAR.

- The most valuable woodland is the Khams district (different from the Khams region), though extensive forest-clad mountains are also found in the Sutlej Valley in the southwest and in the Chumbi Valley in the south. In the late 1950s, some 30 kinds of trees, including those of economic value such as varnish trees, spruce and fir were discovered. The estimated total of forest timber resources in the Khams area alone was placed at more than 100,000,000 cubic metres.

Tibet's stupendous mineral resources were one of the China's primary strategic compulsions to invade and occupy it.

Tibet's stupendous mineral resources were one of the China's primary strategic compulsions to invade and occupy it. Several mining projects were launched in China's Eighth and Ninth Five-Year Plans. Many of the major schemes in the "43 Development Projects" and "62 Development Projects" are directly related to mining in Tibet. These revelations were made by Yi Fatang, the Chinese First Secretary in Tibet in the 1980s. Thereafter, China has not confirmed or refuted the data. It is worthwhile to mention here that the Chinese call Tibet Xizang, meaning Western Treasure House.[8]

WATER RESOURCES

The status of the plateau of Tibet is unique: no other area in the world is a water repository of such size, serving as a lifeline for large parts of a continent. Indeed, the plateau plays a triple role: it is Asia's main fresh water repository, largest water supplier and principal rain maker. But Tibet is rich in more than just water. It also holds other resources of immense strategic value. As elaborated in the preceding paragraphs, it is a treasure trove of minerals, including precious metals and the so-called rare earth elements. With its galloping style of economic growth, China has depleted its own natural resources and is now avariciously draining resources from

8. S.K. Sharma, *History and Geography of Tibet* (Anmol Publications), pp. 98-102.

the Tibetan plateau.[9]

Stretching 2,400 km from east to west and 1,448 km from north to south, this unique water bank is the world's largest plateau. It is also the world's highest plateau, with the average elevation in Tibet so high, more than 4,000 m above the sea level, rightfully earning the sobriquet "The Roof of the World." It is one of the most bio-diverse regions of the world with the rarest medicinal plants, the highest number of living primates on the earth and scores of bird, mammal, amphibian, reptile, fish and plant species not found anywhere else. As a land that includes ecological zones from the Arctic to the sub-tropical, this plateau has a range of landscapes, extending from tundra to tropical jungles, besides boasting of the world's steepest and longest canyons as well as its tallest peak, Mount Everest. It is such a matchless ecological region that a Chinese study has highlighted a "total of 26 altitudinal belts, 12,000 species of vascular plants, 5,000 species of epiphytes, 210 species of mammals and 532 species of birds."[10]

Lowlanders take days to get acclimatised to Tibet's rarefied air, which contains about 40 percent less oxygen than is available at sea level. Environmental hypoxia causes the blood to thicken as the body churns out more red blood cells to offset the low oxygen level, leading to chronic altitude sickness, a condition that in some cases can develop into life-threatening lung, heart or brain complications. By contrast, ethnic Tibetans, with low blood haemoglobin levels, have distinctive genetic features that allow them to breathe easily at very high altitudes. Scientists have identified two genes associated with haemoglobin that play a role in hypoxia adaptation and explain the Tibetans' ability to thrive in such a harsh environment.[11] These genetic differences set the Tibetans apart from their present-day rulers, the Han Chinese.

With its height, the Tibetan plateau literally towers over the rest of Asia. It actually rises up to the middle of the troposphere—the lowest and the

9. Brahma Chellaney, "Water: Asia's New Battleground", Amazon.com, pp. 95-96.
10. Zhang Bai-ping, Chen Xiao-dong, Li Bao-lin and Yao Yong-hui, "Biodiversity and Conservation in the Tibetan Plateau," *Journal of Geographical Science,* 12, no. 2, April 2002, p. 135.
11. Ruiqiang Li, Songgang Li, Lars Bolund, Huanming Yang, Rasmus Nielsen, Jun Wang and Jian Wang, "Sequencing of 50 Human Exomes Reveals, Adaptation to High Altitudes," *Science* 329, no.5987, July 2, 2010, pp. 75-78.

most dense layer of the atmosphere—and helps deflect wind outward in winter and inwards in summer. It influences the Asian climatic, weather and monsoonal patterns, as well as the Northern Hemisphere's atmospheric general circulation, the system of winds that helps transport warm air from the equator, where solar heating is greatest, toward the higher latitudes, giving rise to different climate zones.[12] Due to Tibet's high topography, the jet stream – a torrent of fast flowing air 8 to 11 km above sea level—curves around the mighty Himalayas and the adjacent Karakoram, Kunlun, Hindu-Kush, Pamir and Tian Shan ranges. The plateau's unique features and role, fragile ecosystems and endangered endemic species make it more vulnerable to the effects of global warming than any other region in the world.[13]

Although more than half the world's mountain regions play "an essential or supportive role" for the adjacent lowlands by serving as their "freshwater towers", Tibet is a life giver and water supplier for much of the world's biggest continent, Asia, especially its most heavily populated regions [14]. The abundance of runoff in the mountain areas, principally because of much greater precipitation, makes these regions critical for supplying the earth's land surface with blue water in the form of river runoff, with mountains actually serving as the main source of fresh water in arid zones.[15] However, in comparison with the European Alps—the water tower of Europe—the sources of fresh water originating in the Tibetan plateau support a several times larger population in the lowlands of Asia. Tibetan rivers, indeed, are the lifeblood of the world's two most populous nations—China and India—and the other countries that stretch from Afghanistan to Vietnam

12. Xuefeng Cui, Hans-F. Graf, Baerbel Langmann, Wen Chen and Ronghui Huang, "Hydrological Impacts of Deforestation on the Southeast Tibetan Plateau," *Earth Interactions,* 11, no.15, September 2007, pp. 1-18.
13. Hong Xie, Jiansheng Ye, Xiuming Liu and Chongyi E., "Warming and Drying Trends on the Tibetan Plateau," *Theoretical and Applied Climatology*, September 2009, pp. 45-46.
14. Daniel Viviroli, Hans H. Durr, Bruno Messerli, Michel Meybeck and Rolf Weingartner, "Mountains of the World, Water Towers for Humanity: Typology, mapping and Global Significance," Water Resources Research 43, no.W07447, July 28, 2007, pp. 74-75.
15. Rolf Weingartner, Daniel Viviroli and Greg Greenwood, "Mountain Waters in a Changing World," in Proceedings of the COST Strategic Workshop, *Alpine Space- Man & Environment,* Volume 7, edited by R. Jandl, A. Borsdorf, H. van Miegoet, R. Lackner and R. Psenner (Innsbruck: Innsbruck University Press, 2009).

Tibet is endowed with one of the greatest river systems in the world. Its rivers supply fresh water to 65 per cent of Asia's population and approximately 30 per cent of the world's population.

in a contiguous arc. They include Bangladesh, Myanmar, Bhutan, Cambodia, Laos, Nepal, Pakistan and Thailand. Together, these countries make up 46.3 percent of the global population and contain four-fifths of the people in the larger Asia that extends up to the Bosphorus.[16] Fed by thousands of Himalayan glaciers and mountain springs, the great river systems of Asia flowing down from the Tibetan highland constitute an ecological marvel.

The Tibetan plateau is called the "Third Pole" because it has the largest perennial ice mass on the planet after the Arctic and Antarctica. With its snowfields and glaciers feeding virtually every major river system of Asia—from the Indus (Sengye Khabab to the Tibetans) in the west to the Yellow river (known in Chinese as Huang He) in the east—the plateau holds more fresh water than any place on the earth other than the North and South Poles.

Tibet is endowed with one of the greatest river systems in the world. Its rivers supply fresh water to 65 per cent of Asia's population and approximately 30 per cent of the world's population. Asia is governed by the monsoon patterns of rainfall, bringing rain for only a few months of the year and the perennial flow of its rivers relies upon the constant flux of glaciers on the Tibetan plateau. More than 42,000 sq km of Tibet is covered by permanent snow or ice. The Indian subcontinent is nourished by the perennial flow of major rivers originating from different directions of the Kailash range in western Tibet:

- From the east, the Brahmaputra (Yarlun Tsangpo) flows into India and joins the Ganges in Bangladesh before draining into the Bay of Bengal.
- From the west, flows the Sutlej, passing through Himachal Pradesh and Punjab in India, and joining the Indus river in Pakistan.
- From the north, flows the Sindhu/Indus, passing through Jammu and

16. Based on 2010 estimates of the United Nations' Population Information Network or on the figures in United Nations, World Population Prospects: The 2008 Revision (New York: United Nations Population Division, Department of Economic and Social Affairs, 2009).

Kashmir in India and entering Pakistan before joining the Arabian Sea.

- From the south, flows the Macha Khabab, entering western Nepal as the Karnali before becoming the Gaghara in India to join the holy Ganges.
- Other mighty rivers flowing from Tibet such as the Drichu (Yangze), Machu (Yellow), Gyalmo Ngulchu (Salween) and Zacha (Mekong) sustain the lives of millions in China, Myanmar, Laos, Cambodia, Thailand and Vietnam.

The Brahmaputra or Yarlung Tsangpo, is the largest river on the Tibetan plateau. It runs 2,057 km in Tibet and then makes a U-turn (Great Bend) to enter India in Siang district of Arunachal Pradesh, flows through India and Bangladesh and drains into the Bay of Bengal; 33 percent of its water is collected in catchment areas in Tibet. Its valleys in India and Bangladesh are fertile farmlands with thick forest coverage and crops of tea, rice, jute and rare flora and fauna. The river is crucial to the economy of the entire region. It is reported that China intends to build the world's largest dam with a capacity of 40,000 MW of power. It also plans to pump the water northwards to the arid regions of Xinjiang and Gansu. Since the plan will influence the lives of millions of people in Tibet, India and Bangladesh, a detailed study should be carried out by the lower riparian countries so that the project proceeds according to established international norms. A similar approach should be adopted by the lower riparian countries with regards to other Tibetan rivers, namely, the Karnali, Mekong and Salween flowing into Nepal, Myanmar, Thailand, Laos, Cambodia and Vietnam. The Mekong has 14 dams with ramifications for the lower riparian countries. Tibet is a water powerhouse which can alter the lives of millions in Tibet, South Asia and Southeast Asia.[17]

TIBET AND CHINA: TWO DISTINCT VIEWS

The Chinese Version: Tibet has been part of China since the Yuan dynasty (1271-1368). Centuries ago, Mongol and Manchu Emperors ruled large parts of Asia. During the Tang period (618-907), the Tibetan King Songsten

17. Chellaney, n. 9, pp. 56-57.

Gampo, married Princess Wen Chung. The Princess had a lot of influence in Tibet. During the Yuan dynasty (1271-1368), Tibet was part of the Mongol Empire which was under Yuan rule. At this time, the Yuan government implemented residence registration, levied taxes, and imposed duties in Tibet. China's "White Paper" claims that the Ming dynasty (1368-1644) replaced the Yuan dynasty in China and inherited the right to rule Tibet. During the Manchu rule (1644-1911), the Qing Army entered Tibet on a number of occasions to protect it. Finally, in 1951, China and the Tibetan Local Government signed a 17-point agreement concerning the peaceful liberation of Tibet. During this time, the 14th Dalai Lama supported the liberation and acknowledged that Tibet was a part of China.

The Tibetan Version: Tibet has a recorded history of statehood extending back to 127 BC. From the 7th to the 9th centuries, the Tibetans often dominated the Tang dynasty in battles. Additionally, during the time of this dynasty, the marriage of Princess Wen Chung and King Gampo should be viewed as a strategic move to achieve cooperation and peace between Tibet and China. In 821, after centuries of periodic fighting, China and Tibet signed a treaty wherein boundaries were confirmed and each country promised respect for the other's territorial sovereignty. During the Yuan dynasty (1271-1368), the Mongol leader Genghis Khan conquered most of Eurasia, including China. Thus, instead of China claiming a right to Tibet, Mongolia could assert claims to both China and Tibet. There is no historic evidence to support the assumption that the Ming dynasty (1368-1644) ruled Tibet. In fact, the Qing Emperor, in 1652, not only accepted the fifth Dalai Lama as a leader of an independent state, the Emperor also treated him as Divinity on Earth. During this period, Tibet was known in Chinese as Wu-si Zang or Wu-si Guo (*Guo* means country). During the Manchu rule (1644-1911), the Qing Army was asked by the Tibetans to settle disputes. But this does not support China's right to Tibet. If it did, then the USA should claim Kuwait and Haiti since it assisted these countries. In fact, on a number of occasions, Tibet exercised power over China, suggesting that perhaps Tibet should claim China! At the time of China's invasion in 1949, Tibet possessed

all the attributes of an independent country recognised by international law, including a defined territory, a government, tax system, unique currency, unique postal system and stamps, an army and the ability to carry out international relations. Two years later, the 17-point agreement [Appendix A] was imposed on the Tibetan government by the threat of arms after 40,000 People's Liberation Army (PLA) troops had already seized Tibet's eastern provincial capital Chamdo. The Tibetan delegates were threatened. The seal of the Tibetan government was forged by Beijing. In Tibet, the 14th Dalai Lama could not freely express his disapproval. However, soon after arriving in India, he repudiated this agreement, stating that it was thrust upon the Tibetan government and people by the threat of arms. If Tibet had always been a part of India, why was a 17-point agreement needed? Finally, the Atlas of Chinese History Maps (published by the Chinese Social Science Institue in Beijing depicts Tibet as an independent country that was never part of China.[18]

The claims and arguments of the Chinese and Tibetans are totally in contrast to each other. The Chinese maintain that Tibet has always been a part of China, and due to imperialistic influence and feudal exploitation, had become a living hell where the false notion of independence prevailed. According to China, after Tibet was 'liberated' and merged with the Chinese motherland, it has been ushered into an era of harmony and growth.[11] At the same time, for the Tibetans, before the Chinese invasion, Tibet was a peaceful and religious country, with people living in peace and contentment. However, after the Chinese occupation, the fundamental rights of freedom and independence were snatched away and the Tibetans were turned into prisoners in their own motherland. The Chinese definition of Tibet is very different from that of the Tibetans. For China, only the Tibetan Autonomous Region (TAR) comprises Tibet, but for the Tibetans, 1/4th of the area of China is Tibet.[19]

18. "Tibet and China: Two Distinct Views", http:/www.rangzent.com/history/views.html accessed on March 28, 2013.
19. Sana Hashmi, " Between the Dragon and the Elephant: The Geostrategic Importance of Tibet", *Defence and Security Alert*, vol 3, issue 6, April 2012, pp. 69-71.

For thousands of years, Tibet was the buffer that kept India and China geographically apart and, therefore, at peace.

TIBET IN INDO-CHINA RELATIONS

Tibet is a key factor in India-China relations. It was only after the 1950 Chinese occupation of Tibet that India and China came to share the now disputed common border. In recent years, China's military build-up and infrastructure development in Tibet, as well as reported plans to divert or dam rivers that rise in Tibet and flow into India, have raised India's anxieties. Conversely, China's insecurity about Tibet is an important driver of its approach toward India. India has been unable to assuage China's fears about its possible use of the presence of the Dalai Lama in India and its large Tibetan refugee population of about 120,000 to create trouble for China in Tibet. The presence of the Dalai Lama and a large community of Tibetan refugees in India has kept the "Tibetan question" alive. Given India's open democratic system and long tradition of giving refuge to persecuted peoples, India will find it politically impossible to meet China's expectations on the Tibet question without a significant *quid pro quo*. The breakdown of talks between the Chinese government and representatives of the Dalai Lama does not augur well for the future, and a post-Dalai Lama situation could become much more complicated. Of late, China's aggressive territorial claims on India, the deepening of the China-Pakistan alliance and a shift in China's position on Kashmir has led to a hardening of India's position on Tibet. India is now seeking satisfaction on what it considers to be the core issues relating to India's sovereignty and territorial integrity. India-China relations are unlikely to be on an even keel until this tangled knot is unravelled. [20]

For thousands of years, Tibet was the buffer that kept India and China geographically apart and, therefore, at peace. It has only been for the last six decades or so, after China invaded and occupied Tibet in 1950, that India and China have come to share a common border, and with it, the inherent issues of border security, such as the delineation and demarcation of the

20. Sana Hashmi, " China's Tibet Policy: Implications for India", ***AIR POWER*** Journal, vol. 7, no. 3, MONSOON 2012 (July-September), p. 2.

The independence of India was welcome, but China, as the recognised great power in Asia after World War II, expected India to know its place.

border and the movement of people and flow of trade across it. However, in the absence of any extensive historical experience of relations with each other, each country has a poor understanding of the psyche and system of the other. This was a critical lacuna when the two countries began to interact after India's independence in 1947 and the Communist Revolution in China in 1949. Both were then governed by proud nationalist leaders who were imbued with an exalted sense of the greatness, destiny and mission of their respective nations, but who also had deeply ingrained grievances arising out of the humiliations they had suffered under colonial rule. Given the vanities, egos and different ways of thinking of the leaders of India and China, the likelihood of misperceptions and misunderstandings was built into the situation.[21]

Before the mid-20th century, India-China relations were minimal. There was some overland and seaborne trade, as well as occasional exchanges of pilgrims and scholars. The experience of the Indians and the Chinese of the outside world was completely different. India did not—indeed, could not--keep out foreign influences and ideas. Macedonians, Turks, Afghans, Persians, Mongols and assorted tribes from the Eurasian heartland who invaded India over the centuries made a profound and lasting impact on the country. The old order was not swept away. Rather, a new composite culture and society emerged as, over time, the invaders settled down in the hospitable climes of the plains of India. Here they lived in peace and prospered, eventually becoming indistinguishable from, indeed a part of, the local population. That was not the experience of the Chinese, who remained self-assured that they comprised the "Middle Kingdom" and all others were barbarians. This patronising approach persisted when India and China became independent in the mid-20th century. China's attitude toward India was one of an elder brother or uncle who was well established

21. Rajiv Sikri, "The Tibet Factor in India-China Relations", *Journal of International Affairs*, vol. 64, no. 2, Summer 2011, pp. 3-5.

in the world, giving advice to a younger relative struggling to make his way. The independence of India was welcome, but China, as the recognised great power in Asia after World War II, expected India to know its place. [22]

However, the Chinese also had a complex about India. Instinctively, many Chinese people, including the Communist leaders, understood that India was a very advanced civilisation from which China had borrowed much, including Buddhism. India's spiritual and philosophical traditions were admired. Mao Zedong himself admitted to the Indian Ambassador that, in China, there was "an old belief that if a man lived a good life, he would be reborn in India." Former Chinese Premier Zhou Enlai also acknowledged that China had learned much from India. Yet, the Chinese people were quite ignorant about mid-20th century India, an ideological perspective that led the Chinese Communists to view India with wariness and suspicion as a capitalist and reactionary country whose leaders were too much under British influence. Even the Indian leaders understood that the Chinese regarded them as "tools or stooges of Anglo-American diplomacy or strategy" and that China did not regard India as a friend.[23]

The thinking of independent India's leaders about China was somewhat different. Jawaharlal Nehru, India's first Prime Minister who almost single-handedly guided India's foreign policy both before and after India's independence, harboured a generally benign view of China and its intentions in Tibet, despite being aware of the inimical attitude of China's Communist leaders toward India and toward him personally. As a well-educated, widely travelled politician and intellectual, Nehru had great understanding, sympathy and admiration for China. He harboured romantic, idealistic and somewhat naive notions of India and China as two great Asian civilisations that, as independent nations, would learn from each other's experience, forging a common destiny and promoting world peace in the 20th century. However, during the Chinese civil war, the liberal-minded Nehru's sympathies were clearly with the Nationalists led by

22. L.L. Mehrotra, "India's Tibet Policy: An Appraisal and Options", *Journal of Tibetan Parliamentary and Policy Research Centre* , 2000, pp. 13-14.
23. P.M. Kamath, *India-China Relations: An Agenda for the Asian Century* (Gyan Publishing House, 2011), pp. 66-67.

Chiang Kai-shek rather than with the Communists, something that would have hardly endeared him to China's new Communist leaders. There was mutual admiration, as well as close contacts and correspondence between the two men. Although Chiang Kai-shek, during his visit to India in 1942, could not get the leaders of the Indian Congress Party to support the Allied war effort, the position changed as soon as Britain decided to give India its independence. In July 1947, just six weeks before India gained independence, the United States and India signed an agreement that permitted the United States to continue, even expand, its aerial missions in Tibet in support of Chiang Kai-shek's Kuomintang (KMT) forces against Mao's Red Army.[24]

CHINESE INCURSION AND AFTERMATH

A platoon strength (50 personnel) contingent of China's Army came 19 km inside the Indian territory in Burthe in Daulat Beg Oldi (DBO) sector, which is at an altitude of about 17,000 ft in the Depsang Valley, on the night of April 15, 2013, and established a tented post there.

The Indian side got its first indication of the gradual Chinese build-up in the stand-off area when the troops noticed three vehicles moving between the Chinese tents and their nearest back-up location 25 km away, suggesting replenishment of supplies.

Troops from the Indo-Tibetan Border Police (ITBP) also established a camp approximately 300 m opposite the location. The Ladakh Scouts, an infantry regiment of the Indian Army and specialising in mountain warfare was also moved towards the area where the situation was described as tense. Although small incursions are common across the Line of Actual Control (LAC), the de facto border that runs some 4,000 km across the Himalayas, it is rare for either country to set up camp so deep within disputed territory.[25]

Differing perceptions about the disputed boundary, which is yet to be demarcated, was said to be the root cause of the problem and it was expected to be resolved amicably.

24. Amardeep Athwal, *China-India Relations: Contemporary Dynamics* (Routeledge, 2008), pp. 133-134.
25. Maj Gen R.K. Arora (Retd), "The 21-Day Faceoff", *Indian Military Review*, May 2013, pp. 4-5.

Daulat Beg Oldi (DBO), located in northernmost Ladakh, is a historic camp site, located on an ancient trade route connecting Ladakh to Yarkand in Xinjiang, China. It lies at the easternmost point of the Karakoram range in a cold desert region in the far north of India, just 8 km south of the Chinese border and 9 km northwest of the Aksai Chin LAC between China and India. A landing strip was established at DBO during the 1962 War. At 5,100 m, the strip is one of the world's highest.

Though the stand-off was resolved 21 days later with both the Chinese and Indian sides returning to their original positions behind the LAC, the exact motive of the Chinese incursion remains intriguing to many.

The Chinese grand strategy resembles their national game, Wei qi, which is different from the US and Western premise of grand strategy based on the game of chess. In chess, there are 16 identified pieces of known capabilities, with each side on a playing board with 64 squares. The contest is for total victory, through checkmate. Translated into military strategy, chess identifies the adversary's centre of gravity and seeks a decisive point to eliminate the opponent through a series of head-on clashes. Both the intent and capabilities of each side are on the table.

Wei qi, on the other hand, has an expansive playing board with 361 squares. Each player is given a total of 180 stones of equal capabilities. Unlike chess, where a game starts with all the pieces fully displayed on the board, Wei qi starts with an empty board. The players take turns placing stones at a point on the board, building up positions of strength while working to encircle and capture the opponent's stones. Multiple contests take place simultaneously in different portions of the board. At the end of the game, the board is filled with interlocked areas of strength. The margin of advantage at each point is small; only a Wei qi expert can assess victory through a multitude of contests.

In military terms, Wei qi is about strategic encirclement and demands enormous patience and single-mindedness of purpose through strategic flexibility to achieve objectives.

This strategic thinking is in consonance with Sun Tzu's famous treatise on *The Art of War*, where premium on victory is through psychological

advantage and by avoidance of direct conflict.[26]

"Deception is an integral element of the Chinese strategic culture". At the same time, the importance of being more conversant with the Chinese thought process for improving Indo–China relations cannot be undermined. The relevance and urgency of taking a holistic view needs no further emphasis, especially in the light of the recent friction between India and China over differences in interpretation of the border, resulting, recently, in a 19-km incursion in the Daulat Beg Oldi sector of the Depsang Valley in Ladakh.

Another pet Chinese ploy is to constrict their 'win-set' or range of acceptable solutions, so that the other party has to walk the extra mile in order to accommodate the former's inflated demands.

The sense of *déjà vu* should not be lost given that there have been over 550 instances of Chinese transgressions into the Indian territory since January 2010 alone, including one in July 2012 in the same Chumar area of Ladakh. This had ensued in a similar face-off, after Chinese helicopters destroyed Indian bunkers and tents, but it did not escalate.

Before the oft-asked question about 'how to deal with China' can be answered, it must be noted that there is a discernible and recurring pattern in the manner in which China conducts its foreign relations with India and other small neighbours.[27]

CHINESE GAMBIT

Factoring in the element of 'deception' — not exactly a vice in statecraft — could help us put into perspective some of China's actions. For one, it could explain why Chinese Defence Minister Liang Guanglie, during his visit to India in September 2012, insisted that the People's Liberation Army (PLA) had "never deployed a single soldier" in Pakistan Occupied Kashmir (PoK), even as India's military intelligence had picked up credible reports of about 735 Chinese nationals working at the site of the Neelum–Jhelum

26. Pravin Sawhney and Ghazala Wahab, "China's Age of Wei Qi", *Force*, May 2013, pp. 4-6.
27. "China Needles India in Eastern Ladakh", *The Times of India* (New Delhi), September 19, 2012.

China had consistently conducted a series of live ground and air drills in the Tibetan Autonomous Region in 2012.

hydroelectric project, near the Line of Control (LoC) in Jammu and Kashmir (J&K) and the presence of Chinese soldiers in PoK to provide security to development projects.

Another pet Chinese ploy is to constrict their 'win-set' or range of acceptable solutions, so that the other party has to walk the extra mile in order to accommodate the former's inflated demands. By doing so, the first party gives the illusion of 'having compromised' but has conceded very little. A case in point would be the recent Chinese incursions in the disputed[28] western sector of the border where they demanded a *quid pro quo* pulling down of structures from the Indian side.

Yet another art that the scions of Sun Tzu know only too well is "masking offence as defence". The Chinese advanced their indignation at the increase in India's infrastructure outlay along the border as a reason for the recent setting up of tents in the western sector of the Indo-China border. However, before India gets apologetic about it, it should recount the numerous instances of China's own infrastructure programmes along the border, including the repaving of the Xinjiang–Tibetan highway in July 2012, which runs through the disputed Aksai Chin area. Besides, China had consistently conducted a series of live ground and air drills in the Tibetan Autonomous Region in 2012, as a response to which India merely registered "its concern". China also announced an 11.2 per cent hike in its defence budget in March 2012 and recently omitted a reference to its no-first-use strategic nuclear weapons doctrine in the latest government White Paper released in April 2013.[29]

China has, in the past, also antagonised India on a number of occasions by issuing stapled visas for people from Arunachal Pradesh, which it

28. Vinay Kumar, "Chinese Providing Security to PoK Projects: Army Chief", *The Hindu* (New Delhi), September 20, 2012.
29. Jane Perlez, "Continuing Buildup, China Boosts Military Spending More Than 11 Percent", *The New York Times*, March 4, 2012, http://www.nytimes.com/2012/03/05/world/asia/china-boosts-military-spend, accessed on May 13, 2013.

incidentally terms as "South Tibet"; condemning official state visits to the same; and depicting disputed areas as part of Chinese territory. India may have put up a strong front in the light of the latest border incursions but has probably not given out the right messages in terms of signalling its resolve and intent in dealing with issues of 'concern' to it.[30]

China, on the other hand, in tandem with its diplomatic 'doublespeak', makes extremely effective use of 'speech acts', including a combination of coercion and sometimes reassurance, as part of its diplomatic manoeuvres. China articulates in very strong terms any perceived or actual infringement of its territory. For instance, in April 2012, China objected vociferously to India's OVL collaborating with Vietnam for exploration of oil in a sector of the South China Sea which China claimed as part of its territory. Not only did China send a strongly-worded message that it "will not stand any joint cooperation in [its] claimed maritime areas" but also chided India for pointing out that the South China Sea was the "property of the world". India eventually moved out of the oil block in the South China Sea in April 2012.[31]

Asked why China was objecting to India's exploration projects in the South China Sea when China was similarly involved in carrying out infrastructure projects in PoK, the top Chinese official in-charge of India affairs said both issues are "totally different" and further professed that Chinese involvement in PoK projects and development of the Gwadar port was "without prejudice" to any dispute between India and Pakistan.[32] Not only this, but when China, a few months after crying foul at Vietnam, put up the very same disputed oil block of the South China Sea for global bidding, India went ahead and accepted the invitation, much to Vietnam's consternation. Apparently, this was to 'prove' that Indian presence in the

30. Arvind Gupta, "China's Defence White Paper 2013: Lessons for India", *IDSA Comment*, April 25, 2013, http://www.idsa.in/idsacomments/ChinasDefenceWhitePaper2013LessonsforInd, accessed on May 13, 2013.
31. Ananth Krishnan, "Krishna's Comments on South China Sea a Mistake: Chinese Paper", *The Hindu*, April 7, 2012.
32. Ananth Krishnan, "China's PoK Rail Link Plan Gains Traction", *The Hindu* (New Delhi), September 1, 2012.

South China Sea was "purely an economic activity",[33] which brings back the question of why India is in a constant bid to refrain from 'offending' China.

FUTURE: THE ROAD AHEAD

Tibet is not of much strategic importance as far as the world at large is concerned. It is a high altitude, landlocked region and is not comparable with a strategic powerhouse like the Middle East or the Central Asian Republics. The USA and European countries will not take any initiative which may ruffle China. The issue of Hong Kong stands resolved and Tibet can, in no way be equated with the geo-political importance of Taiwan, the island off the South China Sea and a US facilitator to keep China engaged, as also to enhance its interests in the Asia-Pacific region. It also does not fall under the family of "One China, Two Systems." China is under no compulsion to compromise in this case. Tibet, however, is of paramount strategic significance to China and South Asia, India in particular.[34]

History cannot be undone. The Dalai Lamas carried out their temporal authority with foreign support and there was 'off and on' Chinese influence in Tibet which was exploited by China. The invasion of Tibet in 1950 was justified based on historical trivia like the tribute paid by the Tibet to the Chinese Emperor, ignoring concrete evidence of Tibet's historical independence. The four requirements of statehood in international law are population, territory, a government exercising effective control over that population and territory, and the capacity to enter into relations with other states independently. Tibet met all the parameters of being a nation-state.[35]

Tibet is a theocratic Buddhist state with non-violence and compassion as its core value system. The Dalai Lama epitomises non-violence the world over and was awarded the Nobel Peace Prize in 1989. On the other hand, China occupied Tibet by employing military power and concluded the 17-point agreement under threat of further military action. China is a

33. Ananth Krishnan, "Protest Over China's China Sea Oil Tender", *The Hindu* (New Delhi), June 28, 2012.
34. David Shambaugh, *China Goes Global: The Partial Power* (Oxford University Press, 2013), pp. 22-23.
35. Dawa Norbu, "Chinese Strategic Thinking on Tibet and Himlayan Region", *Strategic Analysis (IDSA Journal),* July 1988, pp. 371- 372.

powerful country and cannot be evicted from Tibet militarily unless there are serious internal disturbances in China itself.[36]

The Dalai Lama's course of action is severely restricted by his being the spiritual head of the Buddhist Tibet, with non-violence and compassion as its core value system. The Dalai Lama is the most precious jewel of the Tibetan people. It appears prudent for him to escape and serve the Tibetan people rather than be abducted and leave Tibet without a leader. On the other hand, in his absence, the Chinese have changed the face of Tibet from one which was conservative, religious, traditionalist, ritualistic and non-materialistic to one with declining religious values and traditions and increasingly materialistic.[37]

The demographic ratio between the Tibetans and Han(Chinese) is changing in favour of the latter. The Hans generally do not follow any religion. Although the Dalai Lama is held in the highest esteem by the Tibetans and also by the Chinese people, his role and relevance will decline, thus, facilitating the objectives of Chinese. The Chinese are determined to retain Tibet in order to engage the South Asian countries. After the signing of the 17-point agreement, Tibet became an integral part of China with a promise of near complete internal autonomy. The promise was not kept. The Chinese also sought to impose their systems which ran counter to the Tibetan way of life and religion. The widespread riots which started in 1956, culminated in the respective policies and the escape of the Dalai Lama to India in 1959.[38]

The ultimate goal of the Tibetan freedom movement would be to make the people of Tibet pursue their traditional way of life in Tibet. The fundamental characteristics of Tibet as a nation have been peace, compassion, non-violence, spirituality and democracy. Political freedom is only a means and not the end. The youth contends that the Tibetan struggle would be neither a political movement nor an anti-Chinese one. The Dalai Lama, his

36. *Collected Statements of His Holiness The Dalai Lama on Devolution of Power to the Elected Leaders of Central Tibetan Administration* (DIIR Publication, 2011), pp. 1-2.
37. "Why Teach and Learn Tibet?" Tibet Education Network, www.globalsourcenetwork.org/TibetWhyTeach.htm, accessed on March 28, 2013.
38. "The Dalai Lama: What He means for Tibetans Today", Roundtable before the Congressional Executive Commission on China, one hundred twelfth session, July 2011, pp. 2-3.

government and the Tibetans would endeavour to undo the obliteration of their country by peaceful means, according to the Buddhist traditions. But like any other youth, the Tibetan youth is getting restless and is convinced that non-violent means are being seen as Tibetan weakness and may not lead to any tangible results. The Tibetan youth may well adopt the Indian model, a combination of non-violent and violent means. The Dalai Lama would continue to hold his spiritual and temporal position but the more assertive part of the movement could be without his sanctions. The Dalai Lama continues to pursue peaceful means and the path of compassion, but the Tibetan community, which even though it has displayed enough patience, will have to create compelling circumstances for China before the damage done to Tibet becomes irreversible.

APPENDIX A

The Agreement of the Central People's Government and the Local Government of Tibet on Measures for the Peaceful Liberation of Tibet

Following is the agreement between the Central People's Government and the Local Government of Tibet on Measures for the Peaceful Liberation of Tibet:-

1. The Tibetan people shall unite and drive out imperialist aggressive forces from Tibet. The Tibetan people shall return to the family of the motherland, the People's Republic of China.
2. The local government of Tibet shall actively assist the People's Liberation Army to enter Tibet and consolidate the national defence.
3. In accordance with the policy towards nationalities laid down in the *Common Programme of the Chinese Political Consultative Conference*, the Tibetan people have the right to exercise national regional autonomy under the unified leadership of the Central People's Government.
4. The central authorities will not alter the existing political system in Tibet. The central authorities also will not alter the established status, functions and powers of the Dalai Lama. Officials of various ranks will hold office as usual.

5. The established status, functions and powers of the Bainqen Erdini shall be maintained.
6. By the established status, functions and powers of the Dalai Lama and of Bainqen Erdini are meant the status, functions and powers of 13th Dalai Lama and the 9th Bainqen when they were in friendly and amicable relations with each other.
7. The policy of freedom of religious belief laid down in the *Common Programme of the Chinese Political Consultative Conference* shall be carried out. The religious beliefs, customs and habits of the Tibetan people shall be respected and lama monasteries shall be protected. The central authorities will not effect a change in the income of the monasteries.
8. Tibetan troops shall be recognized by stages into the People's Liberation Army and become a part of the national defence forces of the People's Republic of China.
9. The spoken and written language and school education of the Tibetan nationality shall be developed step by step in accordance with the actual conditions in Tibet.
10. Tibetan agriculture, livestock raising, industry and commerce shall be improved step by step and the people's livelihood shall be improved step by step in accordance with the actual conditions in Tibet.
11. In matters related to various reforms in Tibet there will be no compulsion on the part of the central authorities. The Local Government of Tibet should carry out reforms of its own accord and demands for reform raised by the people shall be settled by means of consultation with the leading personnel of Tibet.
12. In so far as former pro-imperialist and pro-Kuomingtang officials resolutely sever relations with imperialism and the Kuomingtang and do not engage in sabotage or resistance, they may continue to hold office irrespective of their past.
13. The People's Liberation Army entering Tibet shall abide by all the above-mentioned policies and shall also be fair in all buying and selling and shall not arbitrarily take a single needle and thread from the people.

14. The Central People's Government shall conduct the centralised handling of all external affairs of Tibet and there will be peaceful coexistence with neighbouring countries and the establishment and development of fair commercial and trading relations with them on the basis of equality, mutual benefit for territory and sovereignty.
15. In order to ensure the implementation of this agreement, the Central People's Government shall set up a military and administrative committee and a military area headquarters in Tibet and apart from the personnel sent there by the Central People's Government shall absorb as many local Tibetan personnel as possible to take part in the work.
16. Funds needed by the military and administrative committee the military area headquarters and the People's Liberation Army entering Tibet shall be provided by the Central People's Government. The Local Government of Tibet will assist the People's Liberation Army in the purchase and transport of food, fodder and other daily necessities.
17. This agreement shall come into force immediately after signature and seals are affixed to it.

Signed in Beijing on the 23rd of May 1951.

Chinese Representatives: Li Weihan, Zhang Jingwu, Zhang Guohua and Sun Zhiyuan.

Tibeten Representatives: Ngabo Nggawang Jigme, Khame Sonam Wangdu, Lhawutara Thupten Tenther, Thupten Lekmon and Sampho Tenzin Dhundup.

ENERGISING AEROSPACE INDUSTRY: A NATIONAL SECURITY IMPERATIVE

NISHANT GUPTA

> *[I]t was surprising that whereas every country wanted to produce her own war material, in India, even very senior officials and Ministers wanted to remain dependent on foreign countries and governments for military hardware and would not take any initiative for local production. These people did not understand that a country must not remain forever dependent on another country for her military requirements as, in the event of a war breaking out, that country could stop supplies, putting the receiving country in dire difficulties when her need would be the most acute.*[1]
>
> — Jawahar Lal Nehru

A recent statement of Raksha Mantri, Shri A.K. Anthony, putting emphasis on a greater need for indigenisation of the defence industry, has renewed focus on this long-standing issue of indigenisation being pursued since independence, though with not so encouraging results. There can be no denial of the fact that technology is, indeed, a critical component of national security. Essentials like doctrine, strategy training, and morale, undoubtedly, enhance the effectiveness of national security (and that of the Air Force); but the primary pillar of strength of any air force is its technological vitality. An aspiring nation with limited resources and huge

Wing Commander **Nishant Gupta** is a Research Fellow at Centre for Air Power Studies, New Delhi.

1. B. N. Mullik, *My Years with Nehru: 1948-1964* (New Delhi: Allied Publishers, 1972), p. 130.

India is expected to invest US $ 100 billion in defence and out of this expenditure, about 15-20 per cent is expected to be spent on military aircraft.

economic and social commitments, has no option but to innovate and strengthen its own Research and Development (R&D) since no nation would share its cutting edge technology; and, secondly, commercially available overseas technology has its own problems, termed as the *"triple-trap":* the technologies developed abroad may not be suitable to us; the suitable technologies may be denied; and the technologies available may be unaffordable.[2]

Alongside, trends in national defence as well as the civil aviation sector project humongous growth in the coming decades. In the next five years, India is expected to invest US $ 100 billion in defence and out of this expenditure, about 15-20 per cent is expected to be spent on military aircraft. As per Air Mashl R.K. Sharma, Deputy Chief of the Air Staff, the Indian Air Force (IAF) alone is likely to spend about ₹ 2 lakh crore on procurements during the 12th and 13th Plans.[3] In addition, Boeing expects a demand of between 900 to 1,000 commercial aircraft in the next 20 years, worth US $ 100 billion approximately.[4] Hence, the size of the cake would be really large, and the opportunities unprecedented.

These inputs invoke several questions. What should be the national approach to comprehensively meet the military aerospace requirements? What is the dynamics of indigenisation and how far have we succeeded in this pursuit? What milestones have been crossed and why are we still appearing to be far away from any semblance of a credible indigenous defence design, development and production system? Can the IAF play a constructive role and energise the process of indigenisation? This paper is an attempt to explore answers to such questions; the scope of this paper is largely limited to the military aviation, which is critical for the IAF that is

2. Dr V. Siddhartha, "The Triple Trap, Dual-Use and Single Reform" in Satish Kumar, ed., *India's National Security: Annual Review 2011* (Delhi: Routledge, 2012), pp. 444-445.
3. Air Mshl R.K. Sharma DCAS addressed the 7th Aerospace Industry Conference jointly organised by the IAF, Centre for Air Power Studies and CII at India Habitat Centre on September 20-21, 2012.
4. Confederation of Indian Industries website www.cii.in/Sectors.aspx?enc=prvePUj2bdMtgTmvPwvisYH+5EnGjyGXO9hLECvTuNtzD8aRMyMz, accessed on November 20, 2012.

facing severe weapon system constraints in terms of fighter, transport as well as trainer aircraft. Against an approved force level of 39 and a half combat squadrons, presently, the IAF is meeting the national security and defence requirements with just about 28 combat squadrons. The rationale behind the authorised combat strength is another debate which is kept out of the purview of this paper as the focus is entirely on the process and dynamics of indigenisation.

As the colonial powers trod the path of industrialisation, they deliberately deindustrialised India and used it as a major source of raw material for their industry, as well as a market for their industrial products.

HISTORICAL PERSPECTIVE

Before coming to the Indian aerospace industry *per se*, it will be appropriate to touch upon some historical facts about industrialisation in India. In the 18th century, India had an impressive and large manufacturing base. In 1750, India was producing roughly 24 percent of the world's manufacturing output and China was the only nation ahead of India, with a production of about 31 percent of the world's manufacturing output. That is, more than half of the world's goods were produced by India and China; while Britain's share was barely 2 percent. However, as the colonial powers trod the path of industrialisation, they deliberately deindustrialised India and used it as a major source of raw material for their industry, as well as a market for their industrial products. Thus, by the time India became independent, the equation had totally reversed — Britain's global share scaled up to 24 per cent while India's share dropped down to less than 2 percent.[5]

India entered the aviation era in such an unfavourable background. Nonetheless, Hindustan Aircraft Private Limited, the first aircraft industry in India, was set up in 1940 as a private joint venture between an Indian entrepreneur, Walchand Hirachand, and William Douglas Pawley, an American entrepreneur who had established China's first aircraft factory. The Maharaja of Mysore strongly supported the cause in terms of 50 percent

5. M.J. Akbar, "Indian Armed Forces and Strategic Environment," *USI Journal*, April-June 2012 (Delhi: USI of India, 2012) p. 182.

investment in the shares of the new company and land in Bangalore (now Bengaluru). Soon, the licence produced Harlow PC-5 trainer was flying and designing of fighter aircraft was on its way. However, to meet the post Pearl Harbour expanding requirements of the Allied forces in the Asia-Pacific region, the company was soon taken over by the British government in New Delhi and was leased to the United States Army Air Force (USAAF) for overhaul and repair. As a result, aircraft design and development, which is the bedrock of the aircraft industry, suffered a harsh setback in its infancy.[6]

POST INDEPENDENCE

The 1948 Blackett Report largely laid the foundation of defence of independent India. Dr P.M.S. Blackett, a Nobel Prize-winning British physicist, examined how science could contribute to Indian defence and emphasised on development of an industrial and technological base, to give India a self-supporting defence identity at the earliest. His recommendations like India must limit its ambitions and pursue a policy of non-alignment to escape an unnecessary arms race, and military spending shall not exceed 2 percent of the Gross Domestic Product (GDP), continue to be the cornerstones of Indian national policy.[7] However, his military perceptions about weapon systems were debatable. Chris Smith has brought out that most of his advice was against the grain of military professionals. (Is the nation still appearing to be following this tradition of not giving due cognisance to the demands, requirements and opinions of the military professionals?)

Nevertheless, being a scientist, the following advice of Blackett in respect of defence science and organisation was indeed valuable and insightful. [8]

- No executive responsibilities to be given to the Scientific Adviser to the Defence Minister, though he would have the right to be consulted on the research programmes and on appointment of the scientific staff.
- Indian defence science to follow the organisational pattern of the British

6. Jasjit Singh, *Indian Aircraft Industry* (New Delhi: KW Publishers, 2011), pp.30-31.
7. Sunil Dasgupta and Stephen P. Cohen, "Is India Ending its Strategic Restraint Doctrine?", *The Washington Quarterly Journal*, Spring 2011, pp. 163-177. Blackett also argued against nuclear and chemical weapons, but geo-strategic compulsions made India opt for the strategic nuclear weapon.
8. Singh, n. 6, pp. 84-87.

Admiralty (and not of the British Army or the Air Force). As per this framework, R&D establishments work under the Services' control and usually have a Service officer as Director. The Director of Scientific Research assumes mainly an advisory role.

The former recommendation does not seem to have convinced the policy-makers as yet. Till date, the chief of the Defence Research and Development Organisation (DRDO) exercises executive as well as advisory powers. Despite being the Director General DRDO, he is the Scientific Adviser to the Raksha Mantri as well as the Secretary, Department of Defence R&D. Regarding the latter recommendation with respect to following the pattern of the British Admiralty, out of the three Services, only the Indian Navy inherited and continued to follow this concept. The Indian Navy established the Directorate of Warship Designs and associated institutions like Weapons and Electronic System Engineering Establishment (WESEE) and Controller of Warship Constructions, as an integral component of the Naval Headquarters. As a result, the Navy has reaped significant benefits, and today, it is a prime stakeholder in warship design, development and production. On the other hand, despite a long journey of over eight decades, the IAF has largely remained detached from the process of design, development and production. In the present set-up, the role of the IAF appears to be limited to defining the Air Staff Requirement (ASR) during the inception stage, and thereafter it comes into the picture in the final phase when the new weapon system is offered to the IAF for trials. The IAF plays hardly any significant role in the system development process. I will come back to this aspect a little later.

At the national level, India aspired for *self-reliance* in defence equipment through a three-pronged strategy: **direct purchase; licensed production; and indigenous design and production.** Fundamentally, there are three broad avenues for any technology procurement: purchase (buy); indigenous development (build); and espionage (steal). Various combinations of these three primary avenues lead to another three broad options – reverse engineering (combining buy/steal and build); co-production (combining

buy and build), and co-development (combining buy and build, with an emphasis on build). There are costs, benefits, and trade-offs inherent in each approach. The quest for 'strategic autonomy' through the policy of 'non-alignment' definitely impacted India's pursuit for progress in science and technology, including defence technology. Unlike Pakistan, which got humongous support from the US as an ally, Indian attempts to get access to leading technology have been repeatedly scuttled.

LICENSED PRODUCTION VIS-A-VIS INDIGENOUS DESIGN AND DEVELOPMENT

India embarked on the journey of establishing its military aircraft industry with reconstruction and overhaul of war-time residual aircraft like the B-24 Liberators, Tiger Moths and Harvards. Alongside, Hindustan Aeronautics Limited (HAL) commenced licensed production of the flying trainer Percival P.40 Prentice T3 aircraft and also established the Aircraft Design and Development Department at Kanpur. The Hindustan Trainer No.2 (HT-2) Basic Trainer was the first aircraft to be designed, developed and manufactured in India in the early 1950s and this successful aircraft continued to be with the IAF training schools till 1981 when another indigenously designed and developed trainer, the HPT-32, started replacing it.[9] The HPT-32 was recently grounded, in 2009, due to serious accidents in basic flying training. The first jet aircraft designed, developed and manufactured by HAL, the HJT-16 Kiran, the intermediate jet trainer, has also been serving the IAF for a long time.

The HF-24 Marut (a multi-role combat aircraft) was the first combat aircraft indigenously designed by HAL. It was developed in collaboration with a team of German designers led by Dr Kurt Tank but the fundamental principle of designing an aircraft around a proven engine was violated and, subsequently, the government failed to materialise a suitable agreement for an appropriate engine. Though the Marut had its own share of problems, it was 30-40 per cent superior to the Ajeet in various aspects and its accident rate was also approximately one-eighth of that of the Gnat/Ajeet.[10]

9. Pushpindar Singh, *Diamonds in the Sky: Sixty Years of HAL 1940-2000* (New Delhi: HAL, 2001) p. 38.
10. Singh, n. 6, p. 159.

Table 1: Procurement Mode of IAF Aircraft Inventory[11]

	Direct Purchase	Licensed Production	Design and Development
Trainer	Iskara Pilatus PC-7Mk II	DH-82 Tiger Moth(150)[12] Ajeet Hawk AJT	HT-2 HPT-32 Kiran HJT-16
Helicopter	Mi-4, Mi-8, Mi-17, Mi-25, Mi-26 Bell Model 147 G Sikorsky S 55 C	Cheetah (SA 315 BLA MA) Chetak (Alouette-III)	Dhruv (ALH) Saras
Transport	DHC-3 Otter, DHC-4 Caribou, TU-124, Super Constellation, Packet C-119, Vickers Viscount, Super Aero-45, AN-12, An-32, IL-14,IL-76, IL-78, AWACS, C-130 J Super Hercules, Boeing 737, EMB135 Legacy, C-17 Globemaster,	Avro HS-748 Do-228	Krishak HAOP-27
Fighter	Mystere, Hunter, Canberra, SU-7, Ouragon, Mirage2000, MiG-23, MiG-25, MiG-29, SU-30	MiG-21, , Jaguar, MiG-27, SU-30 MKI, Ajeet, Gnat, Vampire	Marut HF-24 LCA

Through licensed production, HAL has produced a variety of aircraft in significant numbers. The IAF had entered the jet age with the de Havilland Vampire — the first jet fighter produced under licence in India. All the aircraft produced under licence in India—862 MiG-21s between 1967 and 1987;[13]over 400 Cheetahs and Chetaks; and 90 Ajeets—speak volumes

11. Ajay Singh, "Quest for Self-Reliance" in Jasjit Singh, ed., *India's Defence Spending: Assessing Future Needs*, Second Edition (New Delhi: KW Publishers, 2001), p. 134 and Vijay Seth, *The Flying Machines: Indian Air Force 1933-1999* (New Delhi: Sethi Communications, 2000) pp. 10-11.
12. Chris Smith, India's Ad Hoc Arsenal: Direction or Drift in Defence Policy (New York: Oxford University Press and SIPRI, 1994 reprinted in 2008) p. 159.
13. Singh, n. 6, pp. 183-184.

The Aeronautics Committee headed by C. Subramaniam rightly opined way back in 1968 that licensed production was inhibiting indigenous development and it would completely extinguish development.

about the professional ability of HAL. Since 1983-84, HAL has also been manufacturing the Dornier transport aircraft, and for the past five years, this aircraft has not been imported.[14] HAL is also manufacturing under licence the Su-30 MKI, MiG-27 M and Hawk advanced jet trainer. But the quantum of production has been inadequate and the IAF had to resort to purchase of a significant number of various types of aircraft from Russia, North America and West Europe.

The next logical step forward should have been indigenisation through initiation of design and development of sub-systems and components and then graduating to complete weapon development in an incremental manner. But, unfortunately, the strengths of licensed production have not been harnessed to develop incremental expertise in design and development – a critical pillar for achieving self-reliance. The Aeronautics Committee headed by C. Subramaniam rightly opined way back in 1968 that licensed production was inhibiting indigenous development and it would completely extinguish development.

Let us have a closer look at the DRDO, the flag bearer of defence research and development in India. In indigenisation of weapons production, DRDO has not moved beyond the 30 per cent mark it had reached in 1995.[15] And it is yet to produce a single aerospace system for the IAF that could alter the strategic balance in the subcontinent.[16] Nevertheless, there have been spurts of success, though separated with long gaps. The Marut (1964), Ajeet (1978), Light Combat Aircraft (LCA) (2001) and Advanced Light Helicopter (ALH) are a few significant breakthroughs in design and development which can be talked about. A huge gap of nearly thirty years between design and

14. Defence Minister Shri A.K. Antony in a written reply to Shri P.R. Natarajan in the Lok Sabha on December 4, 2012. accessed at http://pib.nic.in/newsite/erelease.aspx?relid=13232, the official website of the Press Bureau of India on January 7, 2013.
15. Yatish Yadav and Nardeep Singh Dahiya, "The Secret World of DRDO," *The Indian Express*, September 2, 2012
16. Dasgupta and Cohen, n. 7, pp. 163-177.

development of successive fighter aircraft (Marut and LCA) or even between basic trainer aircraft (HT-2 and HPT-32) are inexplicable. The gap is even larger for the intermediate stage trainer since, after the Kiran aircraft, the design process has not fructified yet.[17] Dr Shyam Chetty, Director National Aerospace Laboratories (NAL) under the Council of Scientific and Industrial Research (CSIR) brought out during one of his public addresses that these long breaks have led to yawning gaps in the skill sets, especially at the middle level, and core competencies in R&D are hardly available.[18]

To meet this challenge, for the LCA programme, the nation preferred creation of a new organisation rather than strengthening the existing set-up of HAL. Thus, the Aeronautical Development Agency (ADA) was established under DRDO as an ad-hoc institution by pooling resources mainly from various HAL Divisions. The LCA was originally meant to be a much simple aircraft — a replacement for the MiG-21. But its specifications were scaled up far beyond the design capabilities of ADA. The project was launched three decades ago in 1983 and the first test flight was flown in 2001. In January 2011, the Indian Air Force formally granted initial operational clearance to the country's first indigenously manufactured light combat aircraft. In the meantime, NAL was established under the CSIR which was under the Ministry of Science and Technology, for designing aircraft like the Hansa trainer and Saras light transport aircraft.

OPPORTUNITIES MISSED

There are several instances of missing an opportunity of promoting and strengthening design and development. For example, in the 1960s, William Edward Petter, design leader of Midge – an air superiority fighter being developed by Folland for a North Atlantic Treaty Organisation (NATO) requirement — had agreed to offer his services to the Government of India for the development of the Gnat and had also proposed to establish a design bureau in India for the development of more advanced versions of the Gnat. But the proposal was not accepted probably because the HF-24 design and

17. Singh, n. 11, p. 133.
18. Shyam Chetty addressed the seminar entitled "Competitiveness in Indian Aerospace and Defence Sector" at India Habitat Centre, New Delhi, on December 8, 2012.

development was already approved and a poor nation could not afford the luxury of two concurrent programmes to design and develop jet fighters.[19] However, it is interesting to note that India contracted for the Gnat since it was four times cheaper than the Ouragon (Toofani) and was recommended to Nehru by Mountbatten (though it was not approved for selection as a NATO fighter). In the 1965 War, the Gnat proved itself and gave a sterling performance, earning fame as a "*Sabre slayer*".[20]

India exhibits a propensity for initiating new programmes and letting existing ones decay,[21] and the aircraft industry is no different. Multiple agencies have tried various combinations from time to time, but the nation failed to adopt a good strategy for further promoting the successful experiments. There are various instances of half-hearted efforts, a variety of experimentation, premature termination of design and development projects and changing track mid-course without achieving success or learning from the failures. As mentioned above, in addition to HAL, ADA and NAL have been created under different departments and ministries. Even the Directorate General of Civil Aviation (DGCA), a regulatory authority for civil aviation, unsuccessfully tried to design a trainer aircraft along with the Indian Institutes of Technology (IITs).

There are several examples of abandoning of progressive projects. The Hindustan Turbo Trainer HTT-34, a modified aircraft with a turboprop engine, designed and tested by HAL and the IAF in the 1980s was also not inducted.[22] In 1983, HAC-33, another project for indigenously designed aircraft was abandoned in favour of licensed production of the Dornier 228. The Gas Turbine Research Establishment (GTRE) had developed an afterburner (reheat) for the Bristol Orpheus 703 engine and successfully demonstrated its design performance of 20 percent increase in thrust on the testbed. But instead of redesigning the fuselage for fitting the same, a short-cut was attempted by fitting the afterburner after the end of the

19. Singh, n. 9, p. 47.
20. Mullik, n. 1, pp. 125-131.
21. Deepak Pental, "Our Scientific Experiment", *The Indian Express* (New Delhi), January 18, 2013, editorial page.
22. Singh, n. 6, p. 116.

fuselage. Obviously, the experiment failed as the added drag nullified the extra thrust generated by the indigenously developed reheat system; and the HF-24 programme was prematurely closed rather than capitalising on the progress made and furthering the development. In the early 1980s, the IAF prematurely retired the HF-24 fleet of 141 serviceable aircraft.[23] The proposal for HAL manufacturing 108 HTT basic trainers was also rejected by the Ministry of Defence (MoD) in late 2012 since HAL trainers were costing significantly more than the PC-7 Mark II being purchased from Pilatus.[24] Largely, it appears that India is weak on turning its research into profitable application. The problem lies in the deep-rooted bureaucracy, importance to hierarchy over passion for knowledge, ritualism over scientific temperament, and acceptance of mediocrity. Suitable structural changes to address these cultural deficits are essential.[25] These issues must be debated and discussed and viable solutions must be explored on priority. Just creating more institutions and abandoning the existing ones without addressing pertinent issues would not fructify into success. Failure in realisation of the dream of *self-reliance* in military weapons has resulted in substantial dependence on foreign support.

INDO-SOVIET MILITARY RELATIONSHIP

Military equipment transfer has been a strong pillar of the Indo-Soviet relationship since the 1960s. Although Soviet arms sales to India started in the 1950s, supply of the MiG-21 was the first significant high-end combat equipment, which fructified due to heightening tension between India and China as well as between Beijing and Moscow.[26] To counter the US supply of arms to Pakistan and China's increased military level engagement with Islamabad, the Indo-Soviet military relationship continued to deepen during the Cold War. By the time the Soviet Union broke up, it was fulfilling nearly 80 per cent of India's defence needs. But the changing realities called

23. Ibid., pp. 170-173.
24. Ajai Shukla "IAF to Order 37 More Pilatus Trainers Worth Rs 1,250 Cr Pilatus Could Eventually Supply 183 Basic Trainers," *Business Standard* (New Delhi), February 4, 2013,
25. Pental, n. 21.
26. The Soviet Union had refused to sell the MiG-21 to China.

for reorientation and adjustment in the Indo-Soviet relationship. The two decade-old Indo-Soviet Treaty of Peace Friendship and Cooperation of 1971 was amended — the word *'peace'* was dropped from the title as was the famous Article IX, the kernel of the old arrangement. [27]

The collapse of the erstwhile USSR resulted in its inability to sustain its elaborate aerospace and defence industry. The well established aerospace industry as well as the huge pool of trained engineers and scientists, with vast knowledge and experience, were suddenly facing an existential crisis and were exploring overseas economic opportunities for their survival. This was a strategic opportunity for India to boost its aerospace industry and several efforts were made.[28]

The Long-Term Integrated Military Technical Cooperation Agreement of 1994 renewed the defence cooperation and paved the way for joint development of technologies and systems. The agreement provisioned for even exporting jointly developed products. Under this agreement, a broad spectrum was covered, which included significantly strategic projects like development and production of the cruise missile, the Brahmos, purchase and production of the SU-30, development of avionics for the Indian LCA, advanced air defence missiles, upgradation of old MiG aircraft, joint development of military and civilian transport aircraft and multiple-launch rocket systems, etc.[29] The contract includes licensed manufacture of over 200 Sukhoi 30 MKI air dominance fighters, development and licensed manufacture of a similar number of Fifth Generation Fighter Aircraft (FGFA) estimated at $25 billion, development of the medium tactical military transport aircraft to replace the fleet of 100 AN-32 aircraft and procurement of 80 new MI17 1V helicopters (which is underway and the first squadron has been inducted at Air Force Station Phalodi in Rajasthan), to be followed by an order of 59 additional machines.[30]

27. C. Raja Mohan, *Crossing the Rubicon: The Shaping of India's New Foreign Policy* (New Delhi: Viking, 2003), ch. 5, pp.125-126.
28. Though it is understandable that it was not easy to make strategic moves whilst both the nations were undergoing a crisis and there were several barriers. And business with a disintegrating Russia was not as simple as a bilateral agreement with the erstwhile USSR.
29. Raja Mohan, n. 27, pp. 128-129.
30. Air Mshl B.K.Pandey, "US Aerospace Industry and India," *Indian Defence Review*, vol. 26.1 January-March 2011.

Despite the huge opportunity that presented itself, the nation failed to take effective advantage of the situation towards its quest for self-reliance. Notwithstanding a long and healthy relationship with the Soviet Union and the transition from a buyer-seller relationship to joint development of technologies and systems, the nation has failed to harness this strategic opportunity for developing the research, design and development capacity of the national aerospace industry. It seems the leadership entirely missed a vital point that in the long run, appropriate financial and intellectual investments in research and development of the aerospace industry would not only energise the industry but the nation would also reap phenomenal economic benefits as well. And both are essential for the overall national development and security of an aspiring global power.

India is still struggling to be counted as an accomplished science and technology nation, and the aircraft industry is no different.

THE WAY AHEAD

At the time of independence, amongst all the nations that got freedom from colonial powers in the 20th century, India exhibited most progressive leadership in critical fields, including science and technology. However, despite a visionary start and a passionate approach towards science and technology, India is still struggling to be counted as an accomplished science and technology nation, and the aircraft industry is no different.

Strengthening Defence Public Sector Undertakings (DPSUs), DRDO, HAL, Ordnance Factory Boards (OFBs), promoting Foreign Direct Investment (FDI) and private sector involvement, establishing joint ventures, boosting the Public–Private Partnership (PPP) model, establishing Aerospace Innovation Parks, integrated Special Aerospace Economic Zones (SAEZs) and Aviation Technology Parks (ATPs), and harnessing offsets are crucial for energising the indigenous aerospace industry. But most important is to establish a **National Aeronautics Commission (**like the Atomic Energy Commission and Space Commission) and formulate a comprehensive and

futuristic National Aerospace Industry Policy. The commission will also help in synergising knowledge, experience and infrastructure available with various agencies including the IAF, ISRO, HAL, NAL, DRDO, ADA, ADE, GTRE, IISc, IITs.

At the same time, the expanding aerospace industry would require strengthening of the ecosystem across the industry. The certification agencies — the **Centre for Military Airworthiness and Certification (CEMILAC)** for defence aircraft and **DGCA** for the civil aircraft — would deal with the increased workload, necessitating beefing up and overall strengthening. For stringent quality control, Quality Assurance (QA) organisations — Directorate General of Aeronautical Quality Assurance (DGAQA) and DGCA, responsible for the defence and non-defence sector respectively – are to be scaled up and made accountable.

Role of IAF in Energising Aerospace Industry: The long journey of the IAF is studded with attempts to make a dent in the field of R&D and industry. In fact, the IAF has made a few landmark accomplishments. In the 1960s, the IAF took an unprecedented lead and manufactured the **Avro HS-748** — the first transport aircraft in India — at Kanpur under an IAF organisation, the Aircraft Manufacturing Depot (AMD). The efficiency of the project can be adjudged from the fact that in November 1961, the licensed manufactured medium transport aircraft was test flown barely two months after the first British produced aircraft was flown. However, the winning combination was disturbed: AMD was taken away from the IAF in 1964 and later merged with HAL. Was the IAF leadership not keen to take on the responsibility of producing equipment or were there other reasons for this decision? Whatever may have been the reason, but this great opportunity to assume a greater role in design, development and production was missed. Nevertheless, in 1969, the IAF created a Directorate for Projects at Air Headquarters (HQ) and there are several feathers in its cap for the successful execution of development and integration projects. In the early 1980s, the IAF integrated the navigation attack and weapon aiming system for the Jaguar called the DARIN, and made Indian Jaguars far superior to those of the Royal Air Force (RAF) and French Air Force. Additionally, the Radar

and Communication Projects Office (RCPO), INAS Integration Organisation (ITO), Low Level Radar Networking Group (LRNG) also had a high component of design and development and these were executed well.[31] Despite the phenomenal success of such projects, the IAF leadership has not been able to adequately prioritise in-house design and development capabilities though many retired IAF officers, including retired Air Marshals have advocate the same in their writings and dispositions at seminars.

The inability of the research body to involve the armed forces in developmental projects from the start has also been identified as a major area of concern.

At the same time, some analysts believe that the IAF's quest for the world's best weapon systems has been self-damaging. There are opinions that had the IAF not scaled up the LCA ASRs—initially, the LCA was planned to be a replacement of the MiG-21s with slight upgradation – probably ADA would have been able to develop and deliver the aircraft much earlier; and the present scenario of the IAF still awaiting induction could have been avoided. The modest indigenous defence industry has largely failed to produce high end technology systems as per the IAF requirement, even after phenomenal time and cost overruns. Hence, the IAF is finding itself in a severe weapon system deficit which may jeopardise national security. This has also been disastrous for the national aircraft industry as well, since in the quest of producing cutting edge technology products, the DPSUs have failed to produce anything worthwhile or viable. The P. Rama Rao Committee of 2008, which was formed to revamp DRDO, concluded that DRDO's tendency to overestimate its capabilities is the major cause for delays and failures of indigenous defence products. The inability of the research body to involve the armed forces in developmental projects from the start has also been identified as a major area of concern.[32] As a result, self-reliance is still a distant dream and the nation is forced to directly purchase

31. Air Mshl P.V. Athawale, *Indian Air Force: The Maintenance Paradigm* (New Delhi: KW Publishers, 2013), pp.64-65.
32. Manu Pubby, " What Went Wrong with LCA, Arjun Tank, Akash Missile," *The Indian Express*, March 3, 2009.

equipment from abroad, resulting in a long (almost unending) wait, high cost, a huge drain on the country's foreign exchange reserves, increased national dependency on foreign suppliers; and getting trapped into the aforementioned *triple trap.* Thus, the quest for the best is not working out for anyone – neither for the IAF nor for DRDO nor the industry as a whole. Rather '*the best is becoming the enemy of the good*'. Air Chief Mshl S.P. Tyagi has been cited telling his staff, "*Guys, get me the 2nd best in the world, but in time and of the right quality. I am tired of waiting for the best to come up*!"[33]

How do we address this huge gap between high user expectations and inadequate indigenous capability not able to match up? Should the IAF remain a technology intender; or should it make wholehearted efforts to boost the national R&D capability and promote design, development and production of cutting edge technology? Air Mshl P.V. Athawale, former Air Officer-Commanding-in-Chief (AOC-in-C) Maintenance Command, has addressed the issue of high user expectations and inadequate indigenous capability in a more practical manner. While recognising the critical relationship among R&D, industry as well as the IAF, he has explicitly explained their respective perceptions. Each organisation largely defends its own turf and apportions blame on systemic fault lines.

The Air Marshal has suggested a good and viable model which would suit all the stakeholders and synergise the system. While the IAF may continue to look globally for inducting the best in the world, it has no choice but to assume a greater role in scaling up the indigenous production process and about 30 percent of the inventory may be mandated for indigenous replacements. And for this 30 percent, the IAF needs to visualise and contract with the DPSUs and even the private sector for deliveries in a well defined time period, within clearly defined conditions. However, while defining the ASRs, the IAF must adopt a more realistic approach. Indigenous capability, relative cost and domestic constraints are to be kept in mind. The **IAF has to fundamentally change its role from a 'technology indenter' to a 'technology co-developer'.** Nevertheless, such projects need

33. Athawale, n. 31, p. 63.

to be actively monitored and steered by the IAF. To avoid time and cost overruns, which has largely remained a common denominator in the past, accountability has to be well defined at the contract finalisation stage.

Aggregation among research, manufacturing and the military sector is imperative. Many IAF veterans are also in its favour, and in their writings and in various discourses, they have strongly recommended a driving seat for the IAF with a permanent complement of research labs having elements of the airframe, aero-engines, avionics, Electronic Warfare (EW) capabilities, and electronics. It is also suggested that after the LCA programme, the Aeronautical Development Agency (ADA) could be shifted under the control of the Air Force, and on the lines of the Radar and Communication Projects Office (RCPO), a dedicated supporting structure may be created for design, development and projects. Establishment of a three-star PSO (Principal Staff Officer) as Director General (Design, Concepts and Projects) would go a long way in driving all the visionary design and development activities and related projects. The proposed Director General (DG) is to be given the command and execution function of research establishments, including the Software Development Institute (SDI), Aircraft & Systems Testing Establishment, (ASTE), Electronic Warfare Development Department and other laboratories and infrastructure dedicated to research activities. Institutionalisation of a specialised cadre of officers as well as airmen completely dedicated to design, development and R&D activities is essential since this work is entirely different from routine maintenance work.

At the same time, regular monitoring of the progress, with a provision for timely intervention and course correction are essential. The common practice of ascertaining the organisational accountability by looking at the end product towards the end of the project is an inherently faulty mechanism. This process is too unrealistic as it leaves very little scope for course correction amounting to nothing but a *fait accompli.* To avoid and minimise wastage of national resources, it is necessary to have a mechanism that regularly monitors the progress and does not allow a long rope beyond certain pre-defined limits.

A model with a well defined accountability and delivery schedule with embedded provisions for timely intervention and course correction would catalyse indigenous R&D and industry. And as the indigenous capability matures, the percentage of the indigenous share would keep growing and the nation would eventually be able to achieve self-reliance.

CONCLUDING THOUGHTS

The West took 300 years to reach this advanced stage of technology and industrial growth. But India would not have this luxury and needs to hasten the process before it becomes too late and the fleeting opportunities evaporate. It is time for the nation to reach out and create a vibrant Indian aerospace industry and leverage its economic and security benefits. To begin with, the leadership must define a vision, chalk out a strategy and show a will to execute its practical plans to achieve self-reliance in the aerospace industry. Measures like vertical integration in government agencies dealing with design, development and production of aircraft, with a decentralised decision-making process and horizontal links amongst all the stakeholders, are essential. Delinking the executive and advisory role of DRDO is another critical requirement. India has no choice but to promote innovation, PPP, joint ventures and harness the demographic dividend through attracting FDI and harnessing offsets.

The IAF needs to initiate concrete steps to energise the national aerospace industry through all possible means and like the Indian Navy, it has to become a co-developer rather than a mere indenter awaiting aircraft, avionics and weapon systems. Establishment of Director General (Design, Concepts and Projects) has to be an IAF strategic priority towards channelising its efforts in this direction.

NAVIGATING THE ARCTIC: PLAYERS FROM ASIA

JI YEON-JUNG

For the next few decades, the Arctic will provide problems and prospects which may induce inevitable competition for the lion's share among the stakeholders. While the Arctic was perceived as an undiscovered area and a non-navigable ice cap in the past, recent environmental and scientific changes have brought to the fore the assets of the region. The current size of the ice cap has shrunk by more than 40 percent compared to its size in the late 1970s, which has disclosed an area of open water. The enlarged open water provides the opportunity to explore more economic benefits, and for larger marine and other military activities. The major stakeholders sharing the coastal line of the Arctic are eight states members of the Arctic Council: Canada, Denmark, Finland, Iceland, Norway, Russia, Sweden and the United States. Presently, these states are putting in their utmost efforts into investigating and participating in exploring the Arctic, which will be the foundation of the legal claim for sovereignty.

However, the area afloat with ice is attractive not only for the current Arctic coastal states, but also potential stakeholders for economic, environmental, and military interests. East Asian countries like China, South Korea, and Japan are making strides in engaging in Arctic politics with their advanced maritime research and agendas. Those efforts encourage many other states to join the Arctic Ocean, which engenders the controversy of sovereignty on

Ms **Ji Yeon-jung** is a Visiting Fellow at Centre for Air Power Studies, New Delhi.

East Asian countries like China, South Korea, and Japan are making strides in engaging in Arctic politics with their advanced maritime research and agendas.

the common property of the region. The sovereign claims over natural resources and territorial lines around the North Pole will be the vital factor to alter the maritime security architecture anew, if a country's Arctic policy is successfully acclaimed and received.

Despite the complexity of the issue, the significance of adventure into the Arctic appeals to India as well. As an aspirant of global power with various drivers and scenarios, India has evolved its Arctic policy in a strategic calculation despite its physical distance from the area. Since the Arctic security architecture, or maritime regime is yet to be demarcated, the interested countries such as India, need to evolve a coherent and functional security policy. Thus, this paper explores the potential stakeholders in Asia as well as the current key players in the Arctic Council.

THE ARCTIC FIVE TODAY

The Arctic Ocean covers 2.8 percent of the earth's surface and nearly 4 million inhabitants share the environmental diversity of the region.[1] According to the US Geological Survey, the Arctic is estimated to enclose around 13 percent of the world's oil reserves, 30 percent of its natural gas[2], a full extent of minerals as well as rare earths, and potential spots for renewable energy such as tidal and wind resources.[3] With the growing energy demand in the world, the desire and need to access those resources increase, inviting proactive engagement by many countries, and creating the so-called Arctic gold rush.[4] At the same time, militarisation in this

1. Paul Arthur Berkman, *Environmental Security in the Arctic Ocean* (Abingdon: Routledge, 2009), pp.10-30.
2. Todd L. Sharp, "The Implications of Ice Melt on Arctic Security", *Defence Studies*, vol.11, no.2, 2011, p.297.
3. Melissa Bert, "The Arctic is Now: Economic and National Security in the Last Frontier", *American Foreign Policy Journal*, Vol.34, 2012, p. 5.
4. Roger Howard, *The Arctic Gold Rush: The New Race for Tomorrow's National Resources* (London: Continuum. 2009).

region may be observed regarding structuring the legal and non-legal bindings that will impact the global security framework. In particular, the Arctic Council countries are endeavouring to protect accessibility for economic interests and military assurance to achieve their security goals.

According to the US Geological Survey, the Arctic is estimated to enclose around 13 percent of the world's oil reserves and 30 percent of its natural gas.

At the outset, Russia seems to be the one of the countries that aspires for the largest stake in the Arctic, by preserving its stand in the global security architecture.[5] As a country with the largest territorial line, along with the Russian-Arctic population of nearly 2 million[6] and 22 percent of total export through this region, Moscow's interest is focussed on exploration and claims of economic and military needs.[7] Russia currently has the largest Exclusive Economic Zone (EEZ) and stretch of the Arctic shoreline, and is anticipated to seek more oil and gas fields after the Norwegian-Russian maritime delimitation treaty that took effect in July 2011.[8] Russia is exploring and investing in drilling in the new zone next to the Zemlya archipelago in the Kara Sea, the Pechora Sea, in the Yamal field, and the Prirazlomnoy oil field.[9]

For Russia, the Arctic policy represents a reinforcement of influence after the Cold War in competition with the US and North Atlantic Treaty Organisation (NATO). Russia's *National Security Strategy to 2020*, released in 2009, enumerates the priorities of the national security policy in the Arctic by focussing on physical control over the objective and the necessary process in compliance with the international regime.[10] By emphasising a pragmatic approach to maintain competitiveness in this region, *Russia's National Security Strategy to 2020* focusses on strengthening the protection

5. Michael Roi, "Russia: the Greatest Arctic Power?", *Journal of Slavic Military Studies*, vol. 23, 2010, pp. 551-573.
6. Berkman, n. 1, p.22.
7. Roi, n. 5, p. 561.
8. H.A. Conley, et.al, "A New Security Architecture for the Arctic: A Report of the CSIS Europe Program", Centre for Strategic & International Studies, 2012, pp. 3-5.
9. Ibid.
10. Government of Russia, *Russia's National Security Strategy to 2020*, http://rustrans.wikidot.com/russia-s-national-security-strategy-to-2020

of national interests in collaboration with the G-8, G-20, RIC (Russia, India, China), BRICS (Brazil, Russia, India, China, South Africa), yet is not in favour of NATO, and is conditional with the US.[11]

The military consideration seems to be an inevitable option for Moscow with the experience of the Cold War, competition in the European Arctic that ranges from the Barents Sea and Greenland-Iceland-United Kingdom to the North American continent.[12] Heavy naval preparedness around the Arctic coastal area is interpreted as "proof of Russia's serious intention to return to the world's oceans as a leading naval power".[13] Besides, the strategic necessity of the Arctic Ocean extends to military operations that support nuclear deterrence. For instance, Murmansk Oblast, located in the northwestern part of Russia, close to the Norwegian border, is a focal military base for the Russian Navy, providing a great extent of the nuclear triad-strategy inherited from the Cold War experience.[14]

Another aspect of physical protection in this area comprises the border and sovereignty issues. The increase of open water has become a watershed to motivate and generate commercial and strategic value. Moscow has put the Arctic border dispute on the front burner to accumulate information about the outer limit of further than 200 nautical miles (nm) agreed upon by the United Nations.[15] The Lomonosov Ridge, a 1,800-km-long underwater ridge discovered by the Soviet expeditions in 1948, is one of the highest priority security issues for Moscow in the long-term that is expected to be a conflicting point with Denmark. As the area has potential natural resources, it is presumed, mostly by the West, that Russia would obtain exclusive accessibility of this with a 1.2 million sq km EEZ, if and when its claim is taken up by the United Nations Convention on the Law of the Sea (UNCLOS).[16] In pursuit of its policy goal, there is alongside the development of Arctic

11. Ibid.
12. K. Åtland, "The Introduction, Adoption and Implementation of Russia's 'Northern Strategic Bastion' Concept, 1992–1999", *Journal of Slavic Military Studies*, vol. 20, no.4, 2007, p. 499.
13. Roi, n. 5, p.566.
14. Ibid., pp.564-565.
15. Ian G. Brosnan, "Cooperation or Conflict in a Changing Arctic?", *Ocean Development & International Law*, vol. 42, no.1-2, 2011, p. 173.
16. Conley, n. 8, pp.10-11.

science and technology in indigenous research that will also facilitate security missions. Also, tax-exemption rules have been introduced to boost local development that is anticipated to assist infrastructure in the field of oil drilling in the Teriberka and Yamal region. [17]

Due to the size and stature of the Russian Arctic, other European and Northern American states seem to be more cautious about protecting their assets and surmounting an asymmetric situation through individual security and multilateral mechanisms. Among them, Norway, with a long sea line along the Arctic (the so-called Arctic Norway), was one of the foremost countries in the two-bloc contests during the Cold War. Oslo played a big role in nuclear and maritime security, watching over the Soviets, especially their sea-based strategic force in the Kola Peninsula.[18] Oslo mulls over the Russian factor, mostly to envisage hard and soft security policies. In the perspective of hard security, and as a member of NATO, Norway's biggest concern is Russia's substantial investment in maritime security, allotting more than 40 percent of its defence budget to the navy, strengthening nuclear deterrence with strategic nuclear submarines such as nuclear ballistic-missile submarine forces (SSBNs), and airborne nuclear capability with Long Range Aviation (LRA).[19]

In view of the foreseeable scenario of melting ice, Oslo has been paying attention to the Northern Sea Route (NSR), including sea transportation and natural resources that are needed in order to render cost-effective policies. Norway perceives a necessity to seek economic advantage while contending with the Northern Sea Route Administration in Russia's supervised transportation system.[20] As all the strategic steps taken are related to the framework of legal and basic tools for the Arctic Ocean, Norway is exploring a new platform of the Arctic policy, launching the High North

17. Ivan Rubanov, "Gazprom in Europe: Russian Government Plans to Share Part of Yamal Gas Resources", October 29, 2009,. http://www.telegraph.co.uk/sponsored/russianow/6461238/Gazprom-in-Europe-Russian-government-plans-to-share-part-of-Yamal-gas-resources.html
18. Rolf Tamnes, "Arctic Security and Norway", in James Kraska, ed., *Arctic Security in an Age of Climate Change* (New York: Cambridge University Press, 2011), pp.47-48.
19. Ibid., pp.50-51.
20. "Russia Revives Northern Sea Route", *The Voice of Russia*, December 17, 2012, http://english.ruvr.ru/2012_12_17/Russia-revives-Northern-Sea-Route/

Policy, renovated in 2011.[21]

The High North Policy has evolved from the structuring of the Arctic governance, and encompasses complex security issues in the civil and military realms.[22] Although the geographical terms High North and Arctic are not synonymous, the policy embodies the Norwegian perspectives of the norms and multilateral mechanisms of the Arctic Council, within the European Union (EU) framework, along with a continuum of Norwegian security practices of cooperation and diplomacy, with Russia, in particular.[23] In the same manner, a joint nuclear safety commission was launched in 1988 by Norway and Russia, for the clean-up and storage mission of nuclear waste, with other EU countries.[24] However, from the perspective of Oslo, the intention of Moscow is acknowledged more as one aimed at security, rather than cohesive power.[25]

Another proactive country is Canada, a member of NATO and the Arctic Five, with the second-longest Arctic coastline. Ottawa's Arctic policy moves forward in a more practical manner to protect its assets against three dominant factors: Russia with its high-visibility defence force in the Russian Arctic, territorial disputes with the US in the Beaufort Sea where Alaska and the Yukon meet, and territorial disputes with Denmark over Hans Island, located in the Nares Strait.[26] However, in general, Canada's sovereign claim in the Arctic, the so-called Canadian Arctic, faces no challenges to its land except Hans Island.[27]

While Canada's identity in the Arctic was more peaceful than military before the Cold War, it is constantly being modified due to the change in climate, expectation of rights to natural resources, international maritime

21. Ministry of Foreign Affairs, Government of Norway (2011), *The High North: Vision and Strategie*,, Meld. St. 7 (2011-2012) Report to the Storting (White Paper), http://www.regjeringen.no/upload/UD/Vedlegg/Nordomr%C3%A5dene/UD_nordomrodene_innmat_EN_web.pdf
22. Odd Gunnar Skagestad, "The 'High North': An Elastic Concept in Norwegian Arctic Policy", *FNI Report*, 10/2010, Fridtjof Nansen Institute, pp.1-22.
23. n. 21.
24. Geir Flikke, "Norway and the Arctic" in James Kraska, ed., *Arctic Security in an Age of Climate Change* (New York: Cambridge University Press, 2011), pp. 70-71.
25. Ibid., p.72
26. Margaret Blunden, "The New Problem of Arctic Stability", *Survival*, vol. 51, no.1, 2009, pp.126-127.
27. Rob Huebert, "Canada and the Newly Emerging International Arctic Security Regime", in Kraska, ed., n. 24, p. 195.

regime, and defence policy. During the Cold War, the Russia and the US factors were dominant for Canada; for instance, Canada collaborated with the US in defence issues such as the Distant Early Warning (DEW) Line. Ottawa approved the US military transportation in addition to commercial transit.[28] Although Canada and the US are prone to taking pragmatic positions as neighbouring states, the use of the Northwest Passage evokes disagreement between Ottawa's sovereign claim (based on the bylaw of inland water) and Washington's position (based on common property).[29]

Legally, Canada is the first country to enforce its domestic law to prosecute a criminal case against a patrol of the Royal Canadian Mounted Police (RCMP) outpost in the Canadian Arctic that comprises a key element of its legal foundation of sovereignty.[30] Canada also commenced with an undersea mapping expedition to underpin its continental shelf submissions to the UN Commission on the Limits of the Continental Shelf (CLCS).[31] Canada's concern over the Arctic resources has led it to bolster its military presence in this region, to be able maintain a grip on the natural resources in the Arctic Ocean, in the event of a potential conflict.

Ottawa's strategic intent is presently visualised by establishing military infrastructure: a special Winter Warfare Training Centre at Resolute Bay in 2007, and a "deep-water" port at Nanisivik, Nunavut, which includes the expansion of a naval base during 2010-15 with a budget of US $ 100 million allotted. The current defence strategy that originated from the Stephen Harper government in 2006, specifically elaborates the Canadian Arctic policy by outlining the investment in "procurement of new equipment, expansion of special Arctic forces" by 2028.[32] The Royal Canadian Air Force extends and stresses its mission to patrol the Canadian Arctic through the deployment of CP-140 Anti-Submarine Warfare (ASW) aircraft, Unmanned Aerial Vehicles (UAVs), and helicopters. Furthermore, various plans have

28. Ken Coates, et. al., *Arctic Front: Defending Canada in the far North* (Toronto: Thomas Allen Publisher. 2008).
29. Todd L. Sharp, "The Implications of Ice Melt on Arctic Security", *Defence Studies*, vol. 11, no.2, 2011, p.305
30. Coates, n. 28.
31. Sharp, n.29, p.303.
32. Siemon T. Wezeman,, "Military Capabilities in the Arctic", *SIPRI Background Paper*, SIPRI, March 2012, p.1

been introduced to purchase new aircraft for the Arctic region, aimed especially at the Russian defence force.[33] A heavy investment is also seen in the Canadian Army and Navy to expand their capabilities by gathering scattered conventional military resources and purchasing new equipment. The Royal Canadian Navy has revealed its plan to procure imported armed and unarmed icebreakers for patrols.[34]

Competing in the Arctic rush, the US' Arctic policy is zooming in on two main points to break out of the perception of being a smaller stakeholder than its counterparts: wider and deeper engagement in the Arctic by establishing a historical and national identity, and providence of a strategic vision that strengthens the US leadership and international cooperation to mitigate the US' scarce capability and accessibility. Compared to Canada and Russia, the US has a shorter coastline and less population in Alaska, which calls for a more active Arctic policy by political and military policy coordination. In 2007, the US Arctic policy faced a new phase of development, with synchronisation between the National Security Council and the Department of State that became nurtured as the "Arctic Region Policy" under the guidance of the National Security Presidential Directive 66 (NSPD-66)/ Homeland Security Presidential Directive (HSPD) 25 in 2009.[35] Drawing up the policy objectives on securing the environment and natural resource management, the US clearly focusses on homeland security and defences.[36]

The goal of the Arctic policy seems to be extended and amplified by the cross-ministrial coordination, as seen in the Report to Congress on Arctic Operations and the Northwest Passage under the Department of Defence in 2011, with the elaboration of three steps of the Arctic operations: in the near-term (2010-20), the mid-term (2020-30), and the long-term (beyond 2030).[37] The operational capability is diagnosed by a Capability Assessment Approach, with tri-Service assessment in the Arctic, especially of the US

33. Ibid.
34. Sharp, n. 29, pp.305-6.
35. James Kraska, "The New Arctic Geography and U.S. Strategy", in Kraska, ed., n. 24, p. 246.
36. The White House, NSPD-66/HSPD-25, *National Security Presidential Directive and Homeland Security Presidential Directive*, January 9, 2009. http://www.fas.org/irp/offdocs/nspd/nspd-66.htm
37. Department of Defence, federal government of the United States , *Report to Congress on Arctic Operations and the Northwest Passage*, May 2011, pp. 3-16.

Navy's participation. The role of the US Navy has become one of the main drivers of the maritime strategy and "military presence, deterrence, maritime security, and Humanitarian Assistance/Disaster Relief (HA/DR)" that require larger investment in weapon platforms sensors.[38] The US Navy aspires to enhance tactical maritime and aerospace manoeuvrability as one of the primary strategic components of nuclear deterrence, mainly based on the SSBN.

However, Washington's global strategy mobility invites more than the navy's capability to operate in the Arctic Ocean to complete Ballistic Missile Defence (BMD), for instance. Since the Arctic region is a part of the US deterrence strategy, the joint deterrence concept is applied by having a role for the US Air Force to improve aerospace surveillance capability, with due consideration for the lack of military associated infrastructure such as deep-water ports or airfields. The US Air Force has operated the upgraded Cobra Dane radar since 2004 to maintain its strategic position for deterrence and aerospace missions in support of the National Aeronautics and Space Administration (NASA).[39]

Despite Washington's strong will to protect its Arctic assets, a lack of political consensus on the federal budget has made the progress on the policy perspectives somewhat slow. Arctic activities require more time and capital consuming investment than other foreign policy issues. On the Arctic issue, the US leadership faces the issue of cost-effectiveness, due to the low-threat environment.[40] Also, there are many critics in the domestic sphere, leading to a lack of focus on the communications, surveillance, and command and control in the areas of smuggling, terrorism, illegal fisheries, and environmental obliteration.[41]

THE ASPIRANTS IN ASIA

Since there is a basic understanding about the common property rights

38. David W. Titley, and Courtney C. St. John, "Arctic Security Considerations and the U.S. Navy's Roadmap for the Arctic", *Naval War College Review*, vol. 63, no. 2, 2010, pp. 43 and 45.
39. Kraska, n. 35, pp.253-255.
40. Ibid., p.256.
41. Bert, n. 3, p. 6.

China established its first and only Arctic scientific research base, the Yellow River Station in Ny-Ålesund, Svalbard, Norway, in 2003.

that calls for both sovereign rights and global governance, the Arctic sovereignty is claimed by many non-littoral states, especially from maritime-powered countries in East Asia: China, South Korea and Japan. Despite being non-littoral states, yet having high-altitude ports, the three countries are engaging actively in the Arctic politics in Asia with the status of ad-hoc observer. The complexity this adds to the Arctic Ocean was captured by their vibrant move in 2009, when China and South Korea applied for permanent observer status along with Norway, Italy, and the EU, which is yet to be granted.

Among all of these, as a "near-Arctic state"[42], China has received attention during the negotiations for higher status in the Arctic Council, seemingly depending on China-Nordic cooperation such as support from Sweden. However, it received opposition from Norway, Canada, and Russia.[43] It is complicated to judge whether and how Sweden's support to China can be demonstrated as an analysis of China's approach to the Arctic littoral states. According to Linda Jakobson (2010), only Canada and Norway have so far remained in engagement with China by formal bilateral talks.[44] For instance, China established its first and only Arctic scientific research base, the Yellow River Station in Ny-Ålesund, Svalbard, Norway, in 2003.[45]

However, there is disagreement about China's Arctic strategy or policy *per se*, whether and how aggressively the Arctic policy is formalised as an independent policy and as a part of its global strategy, as China's precise target in the Arctic seems to be presently structured around a goal of independent accumulation of scientific expeditions and technological cooperation with the circumpolar states. Despite that, China's involvement

42. Johan McClatchy Nylander, "China a 'Near-Arctic State': Swedish Think Tank", *Tribune Business News*, May 11, 2012.
43. Ibid. Also, Olga V. Alexeeva and Frédéric Lasserre , The Snow Dragon: China's Strategies in the Arctic, *China Perspectives*, no.2012/3, 2012, p.61.
44. Linda Jakobson "China Prepares for an Ice-free Arctic", *SIPRI Insights on Peace and Security*, March 2010, SIPRI, p.11.
45. "Arctic Yellow River Station", Polar Research Institute of China, http://www.pric.gov.cn/enindex.asp?sortid=17

in this region has invited strong and mixed reactions from the Arctic states after two events: China's admission into the International Arctic Science Committee (IASC) in 1996, and the unexpected appearance of China's research icebreaker in Canadian territory in 1999.[46]

Since then, China's engagement in the Arctic has been soaring due to its energy and security needs. Beijing's polar scientific research is in continuum with developing independent research expeditions with an indigenous polar expedition icebreaker, *Xue Long* (Snow Dragon), introduced in 2012 to cruise the Northern Sea Route to the Barents Sea and Bering Strait, and eventually to return.[47] On the other hand, China's Arctic exploration is not limited to use of the vessel, but by the need to purchase more airplanes, which are in the pipeline. China's plan for a sixth expedition in 2013 is going to involve more intensive research work to seek and evaluate its strategic interest in the region.[48]

China's growing interest in the Arctic shows that besides scientific research, the policy direction tends to cover three main priorities: energy security, maritime security (mainly regarding sea-based transportation), and participation in establishing an international regime, with China's leading role in global politics. In the light of assurances that China will share the largest portion of global energy demand by 2035[49], Beijing faces the inevitable option of active economic diplomacy with the Scandinavian states and Russia. China has signed several agreements with Norway, Denmark, Iceland, and Russia since 2001 to expand cooperation on joint Arctic research, natural resource exploitation, and academic exchange, and so on, via inter-governmental and non-governmental forums[50]. Compared to China-Nordic cooperation that continues in a reciprocal manner, Beijing's collaboration with the Northern American states is

46. Alexeeva and Lasserre, n. 43 . p.61.
47. Trude Pettersen, "China Will Continue its Presence in the Arctic and Plans to Launch its Sixth Expedition to the Region in 2013", *Barents Observer*, January 15, 2013. http://barentsobserver.com/en/arctic/2013/01/china-plans-new-arctic-expedition-15-01
48. "China Eyes More Polar Voyages, Bases", *People's Daily Online,* January 10, 2013. http://english.people.com.cn/202936/8087769.html
49. International Energy Agency (2012), "World Energy outlook 2012", November 12, 2012. http://www.worldenergyoutlook.org/media/weowebsite/2012/PresentationtoPress.pdf
50. Alexeeva and Lasserre, n. 23..

In consideration of its strategic interest, China is known to allot more to its budget on the Arctic Sea Route research than even the US.

limited, and presumed not to be accommodative to military competition with the US. [51]

Furthermore, China is keen to explore the openings on the Northern Sea Route (NSR) for "regular commercial transit".[52] Since the NSR was formally opened to vessels from foreign parts since 1991, China's approach to the NSR through its high altitude port has become one of its upfront investments, even as Russia attempts to remain dominant in this region.[53] It renders a number of strategic approaches from China: cooperation with Russia and the Scandinavian countries, establishing a geo-strategic point vis-à-vis NATO, and exploring a sovereign claim that will support China's position in a future maritime regime. In consideration of its strategic interest, China is known to allot more to its budget on the Arctic Sea Route research than even the US.[54]

Like its approach to Antarctica, China's Arctic policy aims at creating a leading role for itself in the Arctic. China has a large number of polar research institutions, including an independent research laboratory, which attracts intense attention from the Arctic Council countries. The Polar Research Institute of China (PRIC), with a staff of more than 140, only for polar research, the China Institute for Marine Affairs under the State Oceanic Administration (SOA), and the Institute of Oceanology under the Chinese Academy of Science represent China's keen interest in this region.[55] Furthermore, more than six universities are known to conduct Arctic research in different subjects, yet it is unknown how far the Arctic politics is studied, which will eventually vindicate its interest and claim to play a leading role in this international legal framework.

51. Ibid.
52. Margaret Blunden, "Geopolitics and the Northern Sea Route", *International Affairs,* vol. 88, no.1, 2012, p. 115.
53. Ibid.
54. "China Spending More on Arctic Sea Route Research than US", *Business Standard*, March 14, 2013.
55. Linda Jakobson, "China Prepares for an Ice-free Arctic", *SIPRI Insights on Peace and Security*, March 2010, SIPRI, pp. 4-5.

Another vibrant country, South Korea, also seems to be gaining momentum with three themes: exploring the natural resources, engaging in the shipbuilding industry and infrastructure sectors, and seeking an assured commercial and logistical interest in the NSR. In 2012, the South Korean President visited the Arctic, reflecting South Korea's ambition to become an influential player.[56] Following the visit, the President also toured Russia, Greenland, and Norway, with the goal of bolstering cooperative efforts and vying for a bigger stake in this region. In a reciprocal manner, Norway and Denmark blinked the green signal to Seoul to support Seoul's appeal for permanent observer status.[57]

As a country which heavily relies on energy supplies through the sea routes, South Korea is keen to secure its supply route through cooperation within an international legal framework.[58] South Korea is the sixth largest oil importer and is heavily dependent on the Middle East, indicating its need to diversify its sources of energy imports. With cutting-edge technology and infrastructure, Korea anticipates that shipbuilding and engineering will extend its collaboration with the Arctic countries.[59] The RV *Araon*, is expected to continue a mission for exploration and rescue, as its capability has been proved in the Antarctic region. The South Korean government budgeted US $ 93 million to build the icebreaking vessel in 2005 to concede the significance of polar activity, despite its high cost,[60] The government also sanctioned US $ 3.1 billion to reinforce research capability by 2020 for the "offshore industries and Arctic shipping sectors".[61]

Also, South Korea desires the protection of its logistical and commercial route. Seoul initiated the coordination between the Korean Transport Institute (KORI), and the Korea Maritime Institute (KMI) to fulfill the goal.

56. Steven Borowiec, "South Korea Angles for Influence on Arctic Policy", *WPR Briefing*, September 25, 2012, pp.2-3
57. "Map of Permanent Participants in the Arctic Council", *Alaska Dispatch*, September 26, 2012. "Korea, Denmark Team up for Arctic Oil El Dorado", *The Korea Herald*, March 10, 2013.
58. Blunden, n. 52, pp. 123-5.
59. "Korea Seeks Bigger Role in Arctic", *The Korea Herald*, May 15, 2012.
60. "The Icebreaker ARAON Exploring the Antarctic", February 21, 2012, http://www.korea.net/NewsFocus/Sci-Tech/view?articleId=98816
61. "South Korea Pledges $3bn to Offshore and Arctic Shipping Research", *Seatrade Global*, July 20, 2012. http://seatrade-global.com/news/asia/south-korea-pledges-$3bn-to-offshore-and-arctic-shipping-research.html

In 2009, a South Korean icebreaker sailed to Western Europe through the NSR with the hope of reducing the standard 10 days and approximately 3,500 miles required.[62] The marine transportation is one of Seoul's priorities that match its growing role in the region. Whereas China is obtaining a number of icebreakers and nuclear submarines, South Korea seems to be protecting its position by shipbuilding. Samsung Heavy Industries and Hyundai Heavy Industries have been developing advanced dual use vessels, beyond icebreakers.[63] Recently, Hyundai Heavy Industries accomplished the project of a 190,000-ton icebreaking iron ore carrier.[64] As many agree, Seoul's interest in the Arctic is mostly focussed on the commercial area as well as environmental issues.

The polar research in Korea is primarily guided by the Korea Polar Research Institute (KOPRI). In 2002, KOPRI launched the Dasan Station, a research centre for polar research, at Ny-Ålesund, Norway. Various strategies for promoting polar research are suggested for the domestic sphere: strengthening the feedback mechanism by legislating activity, utilisation of the institutional basis to interact with various types of expertise, and accumulation of scientific and policy materials.[65]

Japan is also moving forward, with efficient utilisation of the Arctic Ocean, with a purpose similar to that of China and South Korea. Tokyo claimed a stake in the Arctic with an application for observer status in 2009.[66] Japan launched the Arctic Environment Research Centre (AERC) as part of the National Institute of Polar Research (NIPR) in 1990 and reorganised it in 2004 with the cooperation of joint university ventures.[67] The Japanese government has also established a local research station at Ny-Ålesund to research glaciology, oceanography, terrestrial biology, and so on.

62. Borowiec, n. 56, pp.2-3
63. Blunden, n. 52, pp.123-125.
64. Borowiec, n. 56, pp.2-3
65. Bang-young Lee, "Strategy for Activation and Promotion of Polar Research", Korea Polar Research Institute 2010, vol.4, 2010, p.6.
66. "Japan Latest Non-Arctic Country to Claim Stake in North Pole", *Sun Media,* September 3, 2010.
67. Division for Polar Research, National Institute of Polar Research, Arctic Environment Research Centre, http://www.nipr.ac.jp/english/polar-research02.html

Presently, ministerial-level coordination is organised to bolster competitiveness and efficiency in the Arctic policy. The policy coordination among the Ministries of Education, Culture, Sports, Science and Technology (MEXT), Ministry of Foreign Affairs (MoFA) and Ministry of Land, Infrastructure, Transport and Tourism (MLIT) extends a policy-wide guidance at government level that includes the three pillars of the Japanese policy-making process: the civil service, politicians and business actors—an "iron triangle".[68] Since the Japanese government applied for permanent observer status in the Arctic Council, the task force team at the ministerial level has provided large-scale funding for the Arctic research project, in particular under the guidance of MEXT. In pursuit of a government-driven scenario, three major research institutions are at the forefront of lead research projects and the policy-making process: the National Institute of Polar Research (NIPR), Japan Agency for Marine-Earth Science and Technology (JAMSTEC), and Japan Aerospace Exploration Agency (JAXA). And ten universities are known to work on the Arctic and polar-related issues.[69]

After the National Institute for Defence Studies particularly stressed on the Arctic in the annual publication of the *Overview of the East Asia Strategy 2011*[70], Japan's Arctic diplomacy walks in step with it. In September 2012, the Japanese Prime Minister, Yoshihiko Noda, appealed for Russia-Japan cooperation on maritime issues, including the Arctic, during the Asia-Pacific Economic Cooperation (APEC) Summit meeting.[71] While the pattern of Japan's approach to the Arctic and the Arctic states is not dissimilar to the other two ad-hoc observer states in East Asia, the Ocean Policy Research Foundation (OPRF) in Japan especially stresses on cooperation between Russia and Japan.[72] Seemingly, it is the Russia-Japan territorial

68. Aki Tonami, and Stewart Watters, "Japan's Arctic Policy: The Sum of Many Parts", *Arctic Yearbook 2012*, p.94.
69. Ibid., pp.93-100.
70. The National Institute for Defence Studies (2011), *East Asian Strategic Review 2011*, http://www.nids.go.jp/english/publication/east-asian/e2011.html
71. Ministry of Foreign Affairs of Japan (2012), "Japan=Russia Summit Meeting on the Occasion of APEC Leader's Meeting in Vladivostok (Overview), Japan Foreign Policy Updates, Government of Japan. http://www.mofa.go.jp/announce/jfpu/2012/09/0908-03.html
72. "Developing a Japan Policy Towards the Arctic Ocean", *Conference Paper*, The Arctic Conference Japan, Ocean Policy Research Foundation, March 2012.

New Delhi's growing interest in the Arctic Ocean is a part of its large-picture security policy, independent of the Antarctic policy.

conflict over the Kuril Islands that affects access to the Sea of Okhotsk and the Bering Strait. Tokyo's keen interest in the NSR is endeavoured by the independent department of the Japan Northern Sea Route Programme (JANSROP)[73] that vindicates its perspective on maritime security to keeping the Arctic as a critical component in arguments of territorial right, based on UNCLOS and the seabed treaty in the long-term.

INDIA'S ENTRY NOTIFIED

The jigsaw on the current security architecture for the Arctic presents India with a conundrum among policy-makers and strategic thinkers as to how India's Arctic policy should be established. The Arctic has been a subject of study since the Department of Ocean Studies was established in 1981 which, in fact, highlights more of the Indian Ocean and connected regions than the Arctic itself. Even after the extension of the Arctic Ocean due to climate change, scepticism looms over India's geographical limitation to access in the NSR or the Northwest Passage of the Arctic Ocean, which might result in India's approach being deemed unsatisfactory.

However, it seems clear that New Delhi's growing interest in the Arctic Ocean is a part of its large-picture security policy, independent of the Antarctic policy. In 2007, India launched an Arctic research station, Himadri, along with other Asian giants, at Ny-Ålesund which it inherited from its Arctic research programme.[74] Himadri is under the guidance of the National Centre for Antartic and Ocean Research (NCAOR), which manages a number of polar expeditions for scientific research as well.[75] As prey to climate change, India's environmental interests cause Delhi to take a larger role in preventing the acceleration of global warming, what with the

73. Tonami, n. 68, p.94.
74. P. K. Gautam, "The Arctic as a Global Common", *IDSA Issue Brief*, September 2, 2011, p. 7.
75. "New Indian Research Station at the Arctic", *The Hindu*, July 2, 2008.

impact of the monsoons to the agriculture sector.[76]

Apparently, it is interrelated to the concern over the economic interest in the growth of the agriculture sector as well as the oil and natural gas demand, which is a decisive factor in the fulfillment of India's economic plans. According to the *World Energy Outlook* of the International Energy Agency, India is expected to be the largest oil importer before 2025[77]. New Delhi hopes to participate in active exploration and cooperation with the Arctic littoral states to access the huge deposits of oil and gas. In the same manner, India has initiated a robust and extensive approach to Russia and the Scandinavian countries.[78] India's historical engagement with Russia, such as in the Sakhalin project in 2009 seems to be helpful in extending its effort.[79] India is aware that competence in financial and technical capabilities in the energy sector calls for a greater role by the Indian public and private industry to invest in Research and Development (R&D).[80] As nearly 35 universities are involved in undertaking energy research, the Arctic Ocean is expected to be paid more and more attention.[81]

Pursuing the policy goal in the Arctic, India aims to seek observer status in cooperation with the core members of the Arctic Council.

India has established a goal of active participation in the international maritime regime, given its current status and participation in other international regimes, in general, as an active actor. Pursuing the policy goal in the Arctic, India aims to seek observer status in cooperation with the core members of the Arctic Council.

76. Sergey Luney, "India Goes to the Arctic", *Analysis*, April 2, 2012, Russian International Affairs Council, http://russiancouncil.ru/en/inner/?id_4=281
77. "FACTBOX-IEA's India Energy Outlook to 2030", *Reuters*, November 7, 2007. http://in.reuters.com/article/2007/11/07/idINIndia-30378820071107
78. "Canada to Help India Get on Arctic Council", *Hindustan Times*, January 29, 2013. http://www.hindustantimes.com/world-news/NorthAmerica/Canada-to-help-India-get-on-Arctic-Council/Article1-1003595.aspx
79. Sergey Luney, "India Goes to the Arctic", *Analysis*, April 2, 2012, Russian International Affairs Council, http://russiancouncil.ru/en/inner/?id_4=281
80. Kirti Joshi, et. al. "India's Capability and Competence in Energy Sector R&D", S&T and Industry, CAIR-National Institute of Science Technology and Development Studies, 2008, http://www.nistads.res.in/indiasnt2008/t4industry/t4ind22.htm
81. Ibid.

CONCLUSION

Presently, the Arctic invites more states whose interests encompass interlinked issues such as environmental, commercial, strategic, and legal issues. While a comprehensive and open approach to the Arctic is needed, it would be difficult to penetrate the Arctic Council that is already empowered to determine the entry of new members and the broad perspective of the legal bindings in the future. In particular, Russia, Canada, and Norway will gain more impetus owing to their geographical advantage. The growing number of players in Europe and Asia inevitably attracts competition over access by states that have investments, research capabilities and advanced technology.

In a more positive perspective, more players can take different roles regarding geographical accessibility, technological development, and security policies that do not overlap with their plans. One could say that the common general interest is to prevent environmental damage such as dumping nuclear waste in the Arctic Ocean, and to manage the natural resources for sustainable development in the Arctic. An international maritime regime for common strategic priorities only can be formulated by a larger number of stakeholders with comprehensive agendas covering various issues.

However, strategic consequences, driven by socio-economic demands in individual countries, will possibly result in unrestrained competition. The Arctic policy that began with larger players, from global power aspirants such as China, South Korea, Japan and India, in particular, is placed at the global geo-political level. Therefore, the key players are likely to plan for proportional power-sharing, not allowing the entry of new challengers. Also, their strategic needs, as envisaged by the major players, may bring in conflict into the robust bilateral or alliance-based steps in the region. Hence, from the perspective of the Asian countries, a potential conflict may be inevitable since the Arctic cooperation is to be strengthened by, and around, the Arctic Council.

NUCLEAR SAFETY-SECURITY-SAFEGUARDS: THE INTRICATE INTERFACE

SITAKANTA MISHRA

Since its inception, nuclear technology has evoked a sense of zeal as well as awe because of its immense constructive and destructive potential. By now, the world has come a long way, experiencing both: around 540 nuclear reactors operating in 31 countries producing 372,000 MWe (13.5 percent of the world's electricity)[1], radioactive materials used in many sectors enriching human life; on the other hand, two nuclear bombs have been used in war and around 19,000 more are stockpiled; during the same time, three major nuclear accidents occurred,[2] resulting in some human suffering, and misuse of nuclear material by non-state actors is widely apprehended. Therefore, the balance sheet may be argued to be mixed, implying that we succeeded as much we failed with nuclear technology. After the Fukushima nuclear disaster, what would be the fate of nuclear technology or which direction the nuclear energy discourse will move in has been a matter of speculation. This study, premised on the assumption that nuclear technology or nuclear energy *cannot be ignored* as it has an edge over other forms of energy, argues for a better management paradigm by *looking beyond the design basis threats* to address inherent loopholes. Deconstructing the real and assumed threats (accident, misuse, and terror), this study prescribes a

Dr **Sitakanta Mishra** is a Research Fellow at Centre for Air Power Studies, New Delhi.

1. World Nuclear Association, "Nuclear Power in the World Today", http://www.world-nuclear.org/info/inf01.html
2. Chernobyl (USSR), 1986; Three Mile Island (USA) 1979; and Fukushima (Japan) 2011.

coherent and integrated strategy devoid of political and social panic.

EDGE OVER OTHER FORMS

Despite the past half century's global experience, it is not yet fully established that "nuclear power has an edge over other forms of energy, in terms both of limiting day-to-day adverse health and environmental effects, including greenhouse gas emissions, and in terms of the frequency and toll of major accidents".[3] In comparison to coal, gas, hydro, and wind energy sources, the morbidity and greenhouse gas emission per terawatt-hour in the case of the nuclear energy source is much lower. According to a study by Edward D. Blandford and Michael M. May of the American Academy of Arts and Sciences, nuclear energy, that constitutes 14 percent of global energy consumption, has the lowest morbidity (0.04) compared to the coal-related energy production process (161) that constitutes 42 percent of global energy consumption. In terms of greenhouse gas emissions, while coal produces 800-1,400 tons per gigawatt-hour, the nuclear industry produces less than 50 tons.[4]

Table 1: Sources of Electricity, their Morbidity and Greenhouse Gas Emission Per Unit of Electricity Produced

Source (% of world use, 2007)	Deaths per terawatt-hour	Tons of greenhouse gas emissions per gigawatt-hour (life)
Coal (42%)	161 (U.S. average is 15)	800–1,400
Gas (21%)	4	300–500
Hydro (16%)	0.1 (Europe)	Small–100
Wind (<1%)	0.15	Small–50
Nuclear (14%)	0.04	Small–50

Source: Edward D. Blandford and Michael M. May, "Lessons Learned from Lessons 'Learned': The Evolution of Nuclear Power Safety after Accidents and Near-Accidents", American Academy of Arts and Sciences, 2012, p. 23.

3. Edward D. Blandford and Michael M. May, "Lessons Learned from 'Lessons Learned': The Evolution of Nuclear Power Safety after Accidents and Near-Accidents", American Academy of Arts and Sciences, 2012, p. 23.
4. Ibid., p. 23.

The low morbidity in the nuclear sector is mainly owing to the fact that the same amount of electricity can be obtained from about 200 to 300 tons of uranium ore as from 3 to 4 million tons of coal or similarly large quantities of gas or oil. Moreover, no combustion is involved in nuclear energy generation; rather, smaller tonnage is mined, transported, and processed in comparison to other sources. However, the relative costs and benefits of nuclear energy have remained a subject of heated debate. While critics argue that nuclear energy is not only dangerous but also unnecessary for tackling climate change, supporters claim that the risks are small and that abandoning the nuclear source would make an already huge challenge even more difficult and expensive.

There is a lot of uncertainty about the cost of nuclear power compared to the alternatives and these uncertainties increase as one looks towards the future.

Undoubtedly, there is a lot of uncertainty about the cost of nuclear power compared to the alternatives and these uncertainties increase as one looks towards the future.[5] Decarbonising electric power will be critical for solving climate change concerns. The world will need twice as much electricity in 2050 as it does today. As other alternatives are depleting or not up to the mark, nuclear power has the potential to address both the concerns provided the uncertainties are clarified at the earliest. The Committee on Climate Change, UK, in a study has estimated the cost of nuclear energy as falling somewhere above 'low cost' options such as onshore wind, mini-hydro and some bio-fuels, but below 'expensive' options such as offshore wind and Carbon Capture and Storage (CCS).[6] The report asserts that deep reductions in levelised costs are possible if the policy, regulatory, and licensing regimes are supportive.[7] A lot more needs to be accomplished in these matters to clear much of the air which will automatically facilitate greater social acceptance of nuclear power.

5. "Is Nuclear Power Necessary for Solving Climate Change?", *The Guardian*, December 21, 2012.
6. "Costs of Low-Carbon Generation Technologies", Committee on Climate Change, London, May 2011, http://hmccc.s3.amazonaws.com/Renewables%20Review/MML%20final%20report%20for%20CCC%209%20may%202011.pdf
7. Ibid., pp. 7-12.

However, it is necessary to keep in mind that accidents or incidents may occur in the nuclear industry like in any other industry; the chances of misuse of nuclear knowhow are likely to remain; and the fear of nuclear technology falling into terrorists' hands will persist. All this does not mean that there is no future role whatsoever for nuclear technology or nuclear energy. Partly, the fear of radioactive mutated monsters generated by anti-nuclear propaganda has turned the atomic dreams, and atomic nightmares into "one of the most powerful complexes of images ever created outside of religions".[8] And there is no easy solution to these fears except bringing abundant benefits out of nuclear energy to the people as early as possible, while addressing their concerns wholeheartedly.

THREAT TRIANGLE

Especially in the aftermath of 9/11 and 3/11, safety, security, and safeguarding of nuclear material and technology has been a major global concern. Many assume that "catastrophic nuclear accidents are inevitable, because designers and risk modelers cannot envision all possible ways in which complex systems can fail"[9] as there is no 'absolute safety'; security measures can become obsolete as time passes; and misuse of technology is inevitable. Undoubtedly, "assuring safety is hard work" and "an obligation that demands constant attention".[10] However, to fathom "how much safe is safe enough" is probably the most stupendous task in the security discourse. There is also the view that the risk is inherent in every industrial activity, including nuclear, but it can be made quite small. With proper management techniques, the security risks, proliferation hazards, and safety risks can be minimised to the extent that the benefits can outweigh the inherent risks. Noteworthy safety-security lapses continue to occur in every industrial sector, including at Nuclear Power Plants (NPPs) around the globe, even in countries with extensive operational experience and strong regulatory capabilities. The world has not abandoned those industrial projects—rather

8. P.D. Smith, "*The Rise of Nuclear Fear* by Spencer R. Weart – Review", *The Guardian*, April 3, 2012.
9. M.V. Ramana, "Beyond Our Imagination: Fukushima and the Problem of Assessing Risk", *The Bulletin of the Atomic Scientists*, April 19, 2011.
10. Richard A. Meserve, "The Global Nuclear Safety Regime", *Daedalus*, Fall 2009, p. 102.

the focus has been to study what went wrong and try to fix it.

Today, the nuclear industry is "suffering from the cumulative impacts of the world economic crisis, the Fukushima disaster, ferocious competitors and its own planning and management difficulties."[11] Which way the nuclear energy discourse will move is a matter of conjecture. Taking the middle position, this study advocates that *safe nuclear power is possible and desirable*. This could be a reality by a balanced understanding of technology-society correlation – if technology is misunderstood, development is missed, and if technology is uncontrolled, civilisation is at stake. The imperative is to make this correlation even-handed or objective. However, when both sets of issues (the efficacy of nuclear power as a viable source of energy, and the threat to the nuclear industry) are clubbed together, as everyone tends to do, nuclear technology becomes the subject of myriad controversies.

Clandestine nuclear programmes and technology transfer networks have warranted attention to ensure adequate safeguarding of nuclear materials.

First of all, it is to be kept in mind that the threat to the nuclear industry emanates largely from the nature of the strategic environment. 9/11 and terrorists activities have increased attention to ensure adequate security at nuclear installations. Clandestine nuclear programmes and technology transfer networks have warranted attention to ensure adequate safeguarding of nuclear materials. At the same time, nuclear accidents have long provided the justification for a particular emphasis on safe operations at nuclear power plants. The nuclear industry, therefore, is subject to intricacies and concerns of safety, security and safeguards. Safety is aimed at preventing accidents; security is aimed at preventing intentional acts that might harm the nuclear power plant or result in theft of nuclear materials; and safeguards are aimed at preventing the diversion of nuclear materials

11. Mycle Schneider and Antony Froggatt, "The World Nuclear Industry Status Report 2012", July 2012, http://www.worldnuclearreport.org/IMG/pdf/2012MSC-WorldNuclearReport-EN-V2-LQ.pdf, p. 4.

for nuclear weapon purposes.[12]

Nuclear Safety: Like any other industrial enterprise, safety risks are inherent in every component of the nuclear industry: uranium mining, reprocessing, conversion, energy generation, waste management, and even at the decommissioning phase. According to the International Atomic Energy Agency (IAEA) *Safety Glossary*, nuclear safety denotes "the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards".[13] This suggests that safety evaluations focus on risks arising from unintended events initiated by natural phenomena (like earthquakes, tsunami, tornadoes, or flooding), internal hardware interruptions (such as fire, pipe breakage, or loss of electric power supply), or human mistakes (such as the incorrect application of procedures, or incorrect alignment of circuits). So, nuclear safety involves designing, construction and operating of nuclear facilities to protect against the accidental release of radioactive material to the workers, the public or the environment. It also includes the responsibility to respond effectively to an incident or accident to minimise the radiological and other consequences.[14] However, with adequate caution and management techniques, these can be effectively minimised.

Normally, every nuclear facility is designed and built to withstand a postulated accident (design-basis threat) without loss to the systems, structures and components necessary to ensure public health and safety.[15] To ensure this, the basic requirement is adequate infrastructure as well as commitment of the national government, the operator, regulator, vendor and other organisations, to achieve the best possible safety. This involves creation and application of excellent management, design and operation of the nuclear organisation strictly as per the guidelines laid down.

12. IAEA, "The Interface Between Safety and Security at Nuclear Power Plants", INSAG-24, 2010.
13. IAEA, "Nuclear Safety & Security", http://www-ns.iaea.org/standards/concepts-terms.asp; "Nuclear Security", http://www.iaea.org/Publications/Booklets/NuclearSecurity/ns0312.pdf
14. Mark Fitzpatrick, ed., "Nuclear Safety and Security", in *Preventing Nuclear Dangers in Southeast Asia and Australia, IISS Strategic Dossier*, 2009, p. 31.
15. Duyeon Kim and Jungmin Kang, "Where Nuclear Safety and Security Meet", *The Bulletin of the Atomic Scientists*, 68 (1), 2012, p. 87.

Normally, the "defence-in-depth" concept is employed within the nuclear safety arena to lessen the frequency of trigger events; to prevent them from leading to more severe events; and to mitigate the consequences, if they occur. In addition, there is nurturing of a national "nuclear safety culture" (safety values and behaviours modelled by its leaders and internalised by the members involved to make nuclear safety the overriding priority), an intangible concept based on a safety-conscious work environment, and collective responsibility to adhere to the safety principles is the cardinal virtue.[16] A variety of international legal instruments, including conventions and codes of conduct and the IAEA safety standards, supplemented by IAEA safety support programmes, and a global network of experts constitute the global nuclear safety regime.

Nuclear Security: In the IAEA statute and publications, the term "nuclear security" is often abbreviated to 'security'. However, a working definition of nuclear security, according to the IAEA *Safety Glossary*, is "the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear or other radioactive substances or their associated facilities".[17] To further amplify, one can demarcate nuclear security as certain responses to mainly four threats: (1) theft of nuclear material; (2) nuclear explosive devices manufactured using the stolen nuclear material; (3) dispersion of devices for radioactive material (dirty bombs); and (4) sabotage or destruction of nuclear power facilities or of radioactive material in transport.[18] Another type can be a combined disaster, in which opportunistic antagonists time their malicious activity to take advantage of natural disasters that weaken nuclear safety systems. The apparent lack of security in the immediate aftermath of the Fukushima meltdown highlighted the need for planning for such combined nuclear dangers.[19]

16. "Principles for a Strong Nuclear Safety Culture", November 2004 http://www.efcog.org/wg/ism_pmi/docs/Safety_Culture/Dec07/INPO%20PrinciplesForStrongNuclearSafetyCulture.pdf
17. IAEA, n. 13.
18. Tetsuya Endo, "Countries Planning to Introduce Nuclear Power Generation and the 3Ss: Making the 3Ss an International Standard", The Japan Institute of International Affairs, June 2009, p. 5.
19. Kim and Kang, n. 15, p. 90.

One can find a gradual expansion of concern from the physical security of nuclear material to the security of NPPs, technology, and knowhow.

All these aspects necessitate strict physical protection measures like guards, guns, limits on access to vital areas, and intelligence on adversaries to thwart their nefarious designs. With a sound management system and shared responsibility by operators and authorities, and confidentiality of information regarding the facility, unauthorised access can be prevented. Nuclear security, therefore, "deals with any activity or system that contributes to the protection of nuclear and high hazard radioactive materials from unauthorised access, theft, diversion or sabotage, including *inter alia* guarding, physical protection, facility design, personnel vetting, IT security, technical measures, etc."[20] According to a report, between 1972 and 2007, altogether 17 major terror attacks or acts of sabotage have been carried out against nuclear power plants although none of them resulted in an uncontrolled radioactive release.[21]

At the beginning of the nuclear age till the late 1950s, nuclear security was not specifically regarded as a matter of grave concern in comparison to nuclear safety and safeguards. However, during the 1960s and 1970s, nuclear security issues were first taken up from the perspective of the physical protection of nuclear material as, during the same period, there was a sharp rise in nuclear reactors transfers and nuclear energy production the world over. Therefore, in 1975, the IAEA brought out a recommendation (INFCIRC225, 1975), adopted as the Convention on the Physical Protection of Nuclear Material in 1977 as a legally binding document. With nuclear terrorism becoming a realistic scenario during the 1990s and more so after 9/11, nuclear security issues began to be examined in earnest.[22] One can find a gradual expansion of concern from the physical security of nuclear material to the security of NPPs, technology, and knowhow. Therefore, a comprehensive security structure encompassing

20. WINS, "An Integrated Approach to Nuclear Safety and Nuclear Security", World Institute for Nuclear Security (WINS), 2010, p. 3.
21. F. Steinhausler, "Countering Security Risks to Nuclear Power Plants", *Nuclear Power* (Session 5/No 4), International Symposium on the Peaceful Applications of Nuclear Technology in the GCC Countries, Jeddah 2008.
22. Endo, n. 18.

personnel, material, technology, knowhow and their movement is devised along with the legal obligations.

To manage security risks to nuclear installations, the method of 'vital area protection' is adopted. 'Vital area' is an area that contains vital equipment whose destruction or manipulation could endanger public health and safety by exposure to radiation. Normally the nuclear installations take into account the Design Basis Threat (DBT) and embed many security measures in the design itself as certain threats are predictable. The DBT concept is based on the assumption that terrorist acts show a considerable degree of predictability with regard to their method of attack as well as the scope of their criminal action. As a standard practice, site-specific DBTs are classified for security reasons. However, the major components of a DBT, taking into account the threat from both insiders and outsiders, are: (1) identification of the threat; (2) defending against potential attackers; (3) delaying the attackers until security reinforcements have arrived.[23]

To protect against intruders, a series of fences with various sensors and multiple CCTV cameras is installed on-site and at the site perimeter; and inspection of all persons and vehicles entering the site is carried out. To deal with the probable threats from the insiders, personnel reliability programmes are put in place, with criminal background checks and psychological tests of employees. Mock attacks on NPPs are planned and carried out to test the security readiness of the on-site security forces at successive intervals and sometimes without prior notice. After 9/11, the security arrangements in and around the NPPs have also been designed to defend against aerial attacks and cyber attacks. To address the threats from the air, no-fly zones and anti-aircraft guns, etc. have become an integral part of the security system. Defending against cyber terrorism is a complex endeavour. A tiny disk or hard drive is enough to execute a cyber terror plan even if the computer system in a plant is isolated from the internet. The primary objective of any cyber security programme is to protect the confidentiality, integrity and attributes of electronic data or computer systems and processes in a highly complex and integrated environment. Appropriate measures against cyber

23. Ibid.

attacks targeting the digital Information and Communication Technology (ICT) systems of nuclear plants, therefore, include detection, response, mitigation, recovery.[24] However, the global nuclear security regime is not as mature as the safety regime.[25] It comprises some international legal instruments, including conventions and codes of conduct and the IAEA Nuclear Security Series publications, and IAEA security services.

Nuclear Safeguards: As the same technologies, infrastructure and materials used for civilian applications are also used in the nuclear weapon programme, chances of their diversion leading to misuse is always apprehended. Safeguards measures, therefore, aim to prevent the diversion of nuclear technology and materials for nuclear weapon purposes. The first official reference to "safeguards" with respect to nuclear power can be found in the November 1945 Declaration on the Atomic Bomb by President Harry S. Truman and Prime Ministers C.R. Attlee and W.C Mackenzie King of the UK and Canada respectively. The "Atoms for Peace" speech to the UN General Assembly in December 1953 led to the creation of the IAEA in 1957 whose primary duty is to promote the peaceful use of nuclear energy and implementing of safeguards. The nuclear Non-Proliferation Treaty (NPT) and the IAEA constitute the core of the non-proliferation regime looking into nuclear safeguards issues.

However, the global nuclear non-proliferation regime today faces three intricate challenges: enforcement; a crisis of confidence; and the three "T's" – theft, trafficking and terrorism.[26] Non-compliance by countries like Iraq, North Korea, Libya, and Iran has greatly undermined confidence in the regime. Also, the regime contains a number of loopholes that are exploited by the state parties. A state can acquire all the elements of the nuclear fuel cycle as long as it declares them and subjects them to safeguards. But, on six months' notice, it may withdraw legally from the treaty on national security

24. Sitakanta Mishra, "Cyber Threat to Nuclear Installations", *Scholar Warrior*, Autumn 2012, pp. 111-112.
25. IAEA, INSAG, n. 12, p. 6.
26. House Hearing, 111 Congress, "Stopping the Spread of Nuclear Weapons, Countering Nuclear Terrorism: The NPT Review Conference and the Nuclear Security Summit", Hearing before the Committee on Foreign Affairs, House of Representatives, Second Session, April 21, 2010, Serial No. 111-90, http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg56092/html/CHRG-111hhrg56092.htm

grounds and move immediately to acquire nuclear weapons, the way North Korea did.

Instances of nuclear material smuggling are on the rise and their slippage into the wrong hands would be disastrous.

Among various legal and technological procedures, the non-proliferation regime relies on inspections as the primary element in investigating any diversion of nuclear technology and material. The IAEA initially implemented certain provisions of safeguards and after the NPT came into force in 1970, it was given responsibility for full-scope safeguards under the NPT. In the 1990s, an Additional Protocol and supplementary measures were implemented to streamline the safeguards. In the safeguards agreements pursuant to the NPT, a state is required to establish and maintain a State System of Accounting and Control (SSAC) of nuclear material within its territory, jurisdiction or control.[27] However, instances of nuclear material smuggling are on the rise and their slippage into the wrong hands would be disastrous. The endeavour has been to put in place both legal obligations as well as technical measures to reduce the chances of diversion or misuse of nuclear materials. While many bilateral and multilateral non-proliferation regimes are in place, efforts are on to invent proliferation resistant reactors and fuel cycle.

The Intricate Interface: The trio – safety, security, and safeguards – represent specific aspects of the nuclear domain, symbolising an exclusive sphere of responsibilities, but they overlap in many respects. However, the three aspects have been regulated and managed traditionally in isolation from each other. While safety management has been the responsibility of operators, engineers, safety managers and scientists, ensuring security tends to be the responsibility of the security personnel with a different professional background and a range of competencies.

As all the three overlap considerably, the interface among them is extremely intricate. "As the security framework matures, safety and security obligations serve to reinforce each other. Measures related to non-proliferation

27. Sven Thorstensen, "Nuclear Material Accounting and Control: Coordinating Assistance to Newly Independent States", *IAEA BULLETIN*, 1/1995, p. 29.

(safeguards) also contribute to the overall goal of protecting public health and the environment…."[28] Especially, interconnectedness between safety-security, security-safeguards, and safeguards-safety denotes an intricate paradigm that is to be coherently addressed. To ensure a safe and secure nuclear project, better understanding of the three interfaces is necessary.

Firstly, the objective of all these three aspects is the same – protection of the people, society and environment. Such protection is achieved by preventing a large release of radioactive material. Second, as their spheres overlap, and are, therefore, mutually reinforcing, the principles to ensure protection and consequent elements or actions are common even though their implementation may differ. Thirdly, the philosophy applied to achieve the fundamental objectives of the three domains is similar. While nuclear security aims to follow the 'defence in-depth' philosophy by establishing a series of protective layers, nuclear safety strives to address 'design basis threats' by a comprehensive strategy for the defence of the facility to withstand a postulated event. The principle of optimisation of protection is common to both safety and security and based on the idea that radiation risks must be kept as low as reasonably achievable (ALARA).[29] Also the steps taken to provide protection against malicious acts incorporate specific features to ensure physical protection, and rely on provisions that may have been installed for safety reasons. For example, nuclear plants are constructed with protective barriers of steel and reinforced concrete that serve both a security and a safety function.

There are many other arrangements that enhance both safety and security simultaneously. For example, the reactor containment serves to prevent release of radioactive material to the environment in the event of an accident, while simultaneously providing a robust structure that protects the reactor from a terrorist assault. Similarly, controls to limit access to vital areas not only serve a safety function by preventing or limiting exposure but also serve a security purpose by inhibiting unauthorised access by intruders. Especially, there are five elements that are central, and

28. Ibid.
29. IAEA, INSAG, n. 12, p. 3.

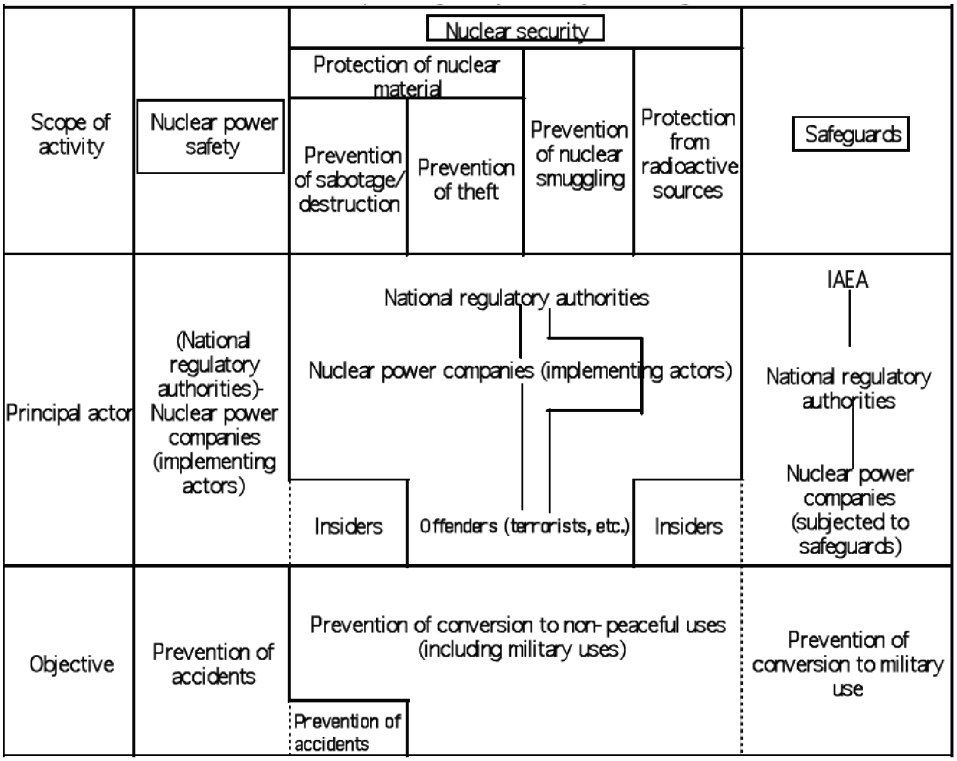
have direct applicability, to the nuclear security regime: (a) regularised assessments; (b) information sharing; (c) peer review; (d) reviews of the implementation of relevant international conventions; and (e) strong trade organisations.[30]

Further, "peace" and "safety" are the keywords for securing and regulating nuclear power. Preventing nuclear material and technology from diversion to military purposes or slippage into wrong hands constitutes another dimension of nuclear security, and is aimed to deter and detect unauthorised removal of nuclear material – to provide assurance that all nuclear material is accounted for. Therefore, safeguards measures enhance safety by preventing diversion and misuse of nuclear material, mainly relying on the methods of 'safeguards by design' and proliferation resistant technology. There are areas where safeguards and security can interact to improve effectiveness and efficacy in achieving their objectives like R&D and surveillance system, analysis capability (nuclear forensics), nuclear trade and illicit trafficking analysis, advisory missions, Information Technology (IT) security, quality management system, risk assessment and emergency response.[31]

Therefore, the interrelationship among the three spheres is straightforward: safeguards can be thought of as addressing "peace"; nuclear safety as addressing "safety"; and nuclear security as spanning both "peace" and "safety".[32] While nuclear security focusses on prevention, detection of, and response to, the theft of nuclear material that can be used for nuclear weapons or nuclear explosive devices (therefore, connected with "peace"), nuclear safety addresses the malicious intentions of terrorists. In other words, nuclear safeguards fundamentally target state actors, nuclear security focusses on terrorists, and nuclear safety covers engineering phenomena but all aim to ensure safe and secure nuclear power.

30. Kenneth Luongo, Sharon Squassoni, Joel Wit, "Integrating Nuclear Safety and Security: Policy Recommendations", CSIS, December 13, 2011.
31. Kenji Murakami, "Nuclear Safeguards Concepts, Requirements, and Principles Applicable to Nuclear Security", Nuclear Security Governance Experts Group, July 2012, p. 9.
32. Endo, n. 18, p. 6.

Fig 1: Interrelationship Among Safety, Security, and Safeguards



Source: "Countries Planning to Introduce Nuclear Power Generation and the 3Ss: Making the 3Ss an International Standard", http://icnnd.org/Documents/endo_3s_int_standard.pdf, p. 8.

THE DILEMMA

Taking into account the increasing number of nuclear reactors under construction in various parts of the world, one may assume that problems related to safety, security and safeguards are inevitable. Since the three spheres overlap considerably, the importance of a coordinated approach to nuclear safety, security and safeguards with the objective to have greater uniformity is oft-emphasised. However, there exist some tensions between each of these aspects that may lead to a dilemma if they are frantically integrated. For example, nuclear safety measures rely on transparency and a culture that strongly encourages an open review of past mistakes; nuclear security, on the other hand, relies on confidentiality of information that

may be of use to an adversary.[33] Nuclear security relies on limiting access to vital areas of plants, while an effective emergency response may require immediate access by nuclear safety personnel and emergency responders. For example, the introduction of delay barriers for security reasons can limit rapid access to respond to a safety event or can limit emergency egress by plant personnel. Security considerations might serve to bar plant personnel from certain areas to the facility in the event of an attack that might need to be accessed for safety reasons. In the same way, certain safeguards are considered confidential, whereas nuclear security, by its very nature, requires the maintenance of secrecy and, thus, is not suited to public disclosure. The focus on sovereignty with respect to nuclear security is especially highlighted in the area of information security. Therefore, "information exchanges and peer reviews have not played a large role in the nuclear security regime" so far.[34]

Moreover, the three regimes are at different stages of their evolution. While the nuclear safety regime encompasses a broad spectrum and a long history, the nuclear security regime has a shorter history and the security culture has not matured as much as the safety culture. The IAEA security guidance has been developed but is viewed as somewhat less comprehensive/mature than the counterpart safety standards. The fact is, nuclear safety and security have developed along different trajectories in the last few decades. The nuclear safety regime, comprising national laws and regulations, voluntary international agreements and conventions, has matured relatively quickly following the Three Mile Island and Chernobyl incidents. The nuclear security regime has advanced largely in response to the 9/11 attacks. The nuclear safeguards regime, on the other hand, is not yet universal and the non-proliferation regime is marred by numerous controversies. Above all, the implementation of nuclear safety and security measures is largely voluntary and national in nature.

Therefore, strengthening the safety-security-safeguards interface is a complex undertaking. A security-heightened approach, though necessary,

33. Fitzpatrick, n. 14, pp. 31-32.
34. Luongo, n. 30.

would not suffice to address all safety threats. Similarly, a culture of nuclear safety practice is necessary, but that alone cannot protect people or the environment from malicious acts. What is needed, therefore, is a *new strategic paradigm* in the development and expansion of nuclear energy based on the 3S (Safety, Security, and Safeguards).[35] An international initiative on the 3S-based nuclear energy infrastructure was first proposed in the G8 Summit 2008 at Chitose, Hokkaido, Japan. The G8 Initiative on Nuclear Energy Infrastructure recognised "the need to establish common understanding that implementation of non-proliferation/safeguards, safety and security (3S) is indispensible for the use of nuclear energy."[36] Against this background, the G8 Initiative, aimed at raising awareness of the importance of 3S worldwide and assisting the countries concerned in developing the 3S, was discussed in the Nuclear Safety and Security Group (NSSG), established at the Kananaskis Summit, and found broad support.[37]

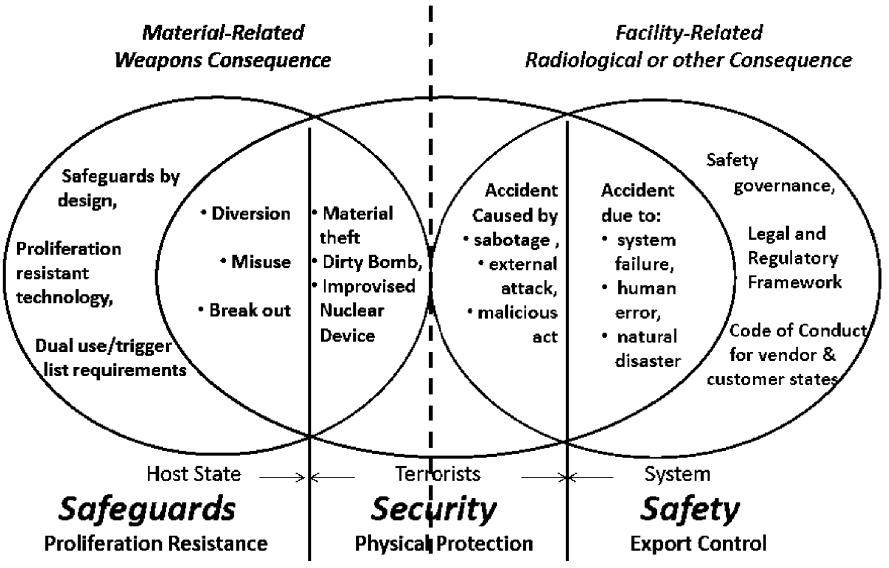
The first Nuclear Security Summit in Washington DC (2010) focussed on the theme of securing nuclear materials and preventing illicit nuclear trafficking and nuclear terrorism. Therefore, it aimed at a 2S approach by integrating safeguards and security measures on nuclear materials. The 2012 Nuclear Security Summit at Seoul focussed on nuclear security and safety to address facility related radiological consequences.

The Seoul Communiqué at best renewed the political commitments generated from the 2010 Washington Summit "to work toward strengthening nuclear security, reducing the threat of nuclear terrorism, and preventing terrorists, criminals, or other unauthorized actors from acquiring nuclear materials."[38] The summit stressed the states' fundamental responsibility to maintain effective security of all nuclear material through measures which would not hamper their right to develop and utilise nuclear energy for

35. Jor-Shan Choi, "An Integrated Approach to Nuclear Safety and Security: In the Context of 3S (Safety, Security, and Safeguards)", http://www.jaea.go.jp/04/np/activity/2011-12-08/2011-12-08-22.pdf.
36. "Report of the Nuclear Safety and Security Group", G8 Summit, 2008, Hokkaido, Toyako, May 29, 2008, p. 3.
37. Ibid.
38. "Seoul Communiqué, 2012 Seoul Nuclear Security Summit", http://www.thenuclearsecuritysummit.org/userfiles/Seoul%20Communique_FINAL.pdf

peaceful purposes. The summit also urged for universal adherence and support to multilateral instruments like the Physical Protection of Nuclear Material (CPPNM), International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT), Global Initiative to Combat Nuclear Terrorism (GICNT), and Global Partnership against the Spread of Weapons and Materials of Mass Destruction.[39] Moreover, the leader of the summit recognised the importance of 'capacity building' as fundamental to promote a strong nuclear security culture and "maintain robust communication and coordination of activities". In this regard, it reaffirmed "the need for various public diplomacy and outreach efforts to enhance public awareness of actions taken and capacities built to address threats to nuclear security, including the threat of nuclear terrorism".

Fig 2: International Initiative on 3S-based Nuclear Energy Infrastructure (Proposed first in the G8 Summit 2008, Japan)



Source: Jor-Shan Choi, http://www.jaea.go.jp/04/np/activity/2011-12-08/2011-12-08-22.pdf

39. Ibid.

The best practices of different countries can be shared and utilised for safe and secure nuclear energy production globally.

GLOBAL NUCLEAR GOVERNANCE

A cursory look at the concerns raised and initiatives undertaken bring one the impression that the world is standing at a "nuclear turning point".[40] A resolve seems to be emerging to strengthen the global concerns to pursue the objectives of reducing the nuclear threat by building a tangible foundation[41] through the Nuclear Security Summits (NSS) which strive to balance national sovereignty vis-à-vis international obligations of nation-states in the sphere of global nuclear governance.

So far, atomic power has remained the exclusive sphere of the state domain and the 'responsibility for nuclear safety rests with the state'. For the last few decades, there has been increasing fear of non-state actors gaining access to nuclear technology. Therefore, the issue of safety and security of nuclear technology has become more acute. Secondly, a nuclear disaster respects no national border and radiation can travel far, affecting surrounding nations. The nuclear industry, therefore, needs to be based on consensus and cooperation, taking into account the different stakeholders. Thirdly, the best practices of different countries can be shared and utilised for safe and secure nuclear energy production globally. All these indicate an effective global *nuclear governance* architecture regulating all aspects of the nuclear energy process. This is increasingly being shared among states, inter-governmental and non-state actors through standards and best practices that play complementary and parallel roles in ensuring nuclear safety, security and safeguards in the last two NSS.[42]

In the current international political lexicon, 'nuclear governance' refers to "the web of international treaties, agreements, regulatory regimes, organizations and agencies, monitoring and verification mechanisms and

40. Bates Gill, "Good Nuclear Governance and Nuclear Security Challenges, Implications, and Responses", *IFANS Review*, 18 (2): 2.
41. Ji Yeon Jung, "Prospects of the Seoul Nuclear Security Summit, 2012", *Defence and Diplomacy*, January-March 2012, pp. 69-70.
42. Ramesh Thakur, "The Global Governance Architecture of Nuclear Security", *Policy Analysis Brief*, Stanley Foundation, March 2013, p. 9.

supplementary arrangements that help determine the way that the peaceful uses of nuclear energy, notably the generation of nuclear electricity, is governed".[43] They exist at the international, regional and sub-regional or bilateral levels and largely depend on national implementation arrangements which ensure that each country fulfills its obligations in the nuclear field. It is a collaborative enterprise involving many players at various levels that indeed emphasises on a holistic approach.[44]

The current status of global nuclear governance is linked mainly to various regimes in its nuclear safety, security and non-proliferation arena. The 1994 Convention on Nuclear Safety (CNS) that entered into force in October 1996 is the most important legally-binding instrument in the nuclear safety field. Though the treaty applies to land-based civilian nuclear power reactors, radioactive waste management, and storage of spent fuel, it excludes other nuclear fuel cycle facilities for fuel fabrication, uranium conversion and enrichment, and reprocessing. In fact, fuel cycle facilities face unique nuclear safety challenges which need urgent attention. Also, the CNS has no monitoring, verification or compliance system and no penalties for non-compliance. It is alleged that the CNS suffers from a lack of openness and transparency, making it impossible for outsiders to truly assess the system's effectiveness.[45]

The IAEA is considered as the global hub of nuclear safety and security. It acts as the secretariat for all the new safety-related conventions, and sets and promotes safety standards, safety advisory missions and management of peer review processes. It also establishes guidelines and codes of conduct and provides significant advice and assistance to member states on all nuclear-related matters. The Operational Safety Review Teams (OSART) programme is designed to aid states in improving the operational safety of their nuclear plants essentially through the process of peer review. The IAEA's Integrated Regulatory Review Service (IRRS) provides advice and assistance to enhance the effectiveness of regulatory infrastructure for both

43. Trevor Findlay, *Nuclear Energy and Global Governance* (London: Routledge, 2011), pp. 2-3.
44. Ibid., p. 3.
45. Ibid., p. 106.

safety and security. The IAEA Incident Reporting System (IRS) collects information from participating states' national regulators on unusual events in nuclear power plants, assesses, analyses and extends feedback to operators to prevent similar occurrences at other plants. However, all these do not legally oblige states to implement IAEA standards. Many countries do not even report to the IAEA. The question arises as to whether such standards and practices should be made legally binding and compliance with them verified by international inspectors, as in the case of nuclear safeguards. In 2000, the IAEA initiated the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) and released the INPRO methodology. However, the boundary between the capacity to produce nuclear energy and nuclear weapons is thin, therefore, difficult to monitor. Countries, by availing all international cooperation on civilian nuclear technology, can also attain the capability to produce nuclear weapons at short notice. North Korea, after availing multilateral nuclear technology support through the NPT, withdrew from the regime and opted for nuclear weapons. It has been apprehended for long that the spread of nuclear weapons to more states increases the chance of their misuse.

Many other international bodies have also undertaken the responsibility of ensuring nuclear safety like the World Association of Nuclear Operators (WANO), Nuclear Energy Agency (NEA), World Nuclear Association (WNA) European Atomic Energy Community (Euratom) and European Commission (EC). Especially, WANO runs a peer review system to facilitate "communication, comparison and emulation" and technical support missions among its members in order to maximise safety and reliability. The NEA focusses on research and information exchange in selected areas like nuclear sciences, safety, regulation, waste management, technical and economic studies, nuclear law and radiation protection. The Euratom helps promote nuclear safety through the cultivation of common views and by identifying best practices. The European Nuclear Safety Regulators Group (ENSREG) is the focal point of cooperation between European regulators and intends to lead to continuous improvement in nuclear safety, especially in new reactors.

The oldest but least understood legal regime fostering nuclear safety is the 'liability' one that emerged in the 1960s. This is the most important legal mechanism by which an operator can be held internationally accountable for a nuclear accident that causes trans-boundary hazards. Also, it aims to sustain public confidence in nuclear energy by ensuring adequate compensation to those harmed if an accident occurs. While imposing responsibility on operators to run the reactors safely, the regime provides stronger legal protection against unlimited liability for vendors that operate outside their own countries.

However, the liability regime has remained "paradoxical" and "less welcome" for various reasons.[46] It is alleged that it reduces the incentive for pursuing nuclear safety as it is based on the idea that the operator is ultimately responsible for the safety of its reactors. As the cost of liability insurance is not internalised, it provides a small but hidden subsidy to the nuclear industry, making it cheaper than it normally would be. Further, the liability regime has become complex as it is based on two separate international legal frameworks. The oldest is the Paris/ Brussels framework, established under the auspices of the Organisation for Economic Cooperation and Development (OECD)/NEA, covering the OECD members. The Vienna framework, under the IAEA auspices, was intended to be universal by providing the framework for a global regime. The 1997 Protocol to Amend the Vienna Convention and the 1997 Convention on Supplementary Compensation for Nuclear Damage are two attempts to modernise the regime. The Convention Relating to Civil Liability in the Field of Maritime Carriage of Nuclear Material, 1971, deals with the liability issue with nuclear operators who transport nuclear material. More importantly, it has been marked that states have been remarkably reluctant to become parties to the liability conventions and protocols. According to different studies, fewer than half of the world's nuclear power plants are currently covered by the regime and the largest civil nuclear programmes

46. Ibid., p. 124.

have stayed away, providing disincentives for other states to join in.[47]

The nuclear global governance, especially on the security aspects and the regime thereof, is nowhere near as extensive, advanced or entrenched as the regime for nuclear safety governance is. Comparatively, there is less collaboration between nuclear plant operators worldwide in this sphere. Practically, there is no peer review as there exists an abiding sense that nuclear security is too sensitive an issue to be subject to global governance. In fact, "the pervasive secrecy surrounding nuclear security means that no global mechanism is in place to identify the worst security performers and help them come up to the level of the best performers".[48] Even the treaties and conventions that exist are laden with many handicaps that are challenging to address. The CPPNM (1980) strives to commit states to ensure nuclear material protection and organise review conferences every five years to assess the implementation of the convention as a whole. However, it does not focus on the compliance of individual parties. There is no peer review mechanism, nor does the IAEA have any particular role beyond transmitting information about national contact points.[49] An amendment to the convention was brought in 1998 to extend its ambit to domestic use, storage and transport aspects of nuclear activities. However, the amendment is not yet in force. In the same manner, the ICSANT entered into force in July 2007 and as of 2010, there were only 63 state parties and 115 signatories. It also does not have any monitoring, verification or compliance provisions or system of peer review, accountability or review meetings. The Security Council Resolution 1540 is a valuable and novel addition to global nuclear governance, but even its compliance and implementation have been "slow and uneven".[50]

47. Ann MacLachlan, "US Ratification Boosts Plan for International Nuclear Liability", *Nucleonics Week*, March 19, 2008; Johan Rautenbach, Wolfram Tonhauser and Anthony Wetherall, "Overview of the International Legal Framework Governing the Safe and Peaceful Uses of Nuclear Energy – Some Practical Steps", *International Nuclear Law in the Post-Chernobyl Period*, joint report by OECD/NEA and IAEA, 2006.
48.. Roger Howsley, "The World Institute for Nuclear Security: Filling a Gap in the Global Nuclear Regime", *Innovations*, vol. 4, no. 4, Fall 2009, p. 204.
49. Findlay, n. 43, p. 131.
50. Stanley Foundation, "Implementing UNSCR 1540: Next Steps Towards Preventing WMD Terrorism", *Policy Memo*, December 18, 2009, www.stanleyfoundation.org/publications/policy_memo/ImplementUNSCR15401209PM.pdf.

The global non-proliferation regime is comparatively more binding and relies on the compliance and verification process. Though the NPT has managed to restrict the number of nuclear weapon states to within ten, serious cases of non-compliance have undermined its credibility over the years. Successive Review Conferences have been forums of contention, and without tangible outcomes. Article VI of the treaty prescribes "negotiations in good faith" for all NPT parties to achieve nuclear disarmament; however, no significant step has been undertaken in this regard by any state-party yet. The IAEA safeguards framework has been increasingly authoritative and intrusive. At the same time, it could only monitor and inspect materials and facilities formally declared to it by the parties. There are reports saying that at least 24 states have not complied with their obligation to have a comprehensive safeguards agreement. As of December 2009, 93 states had an Additional Protocol in force, 34 had signed one and another eight countries' agreements had been approved by the IAEA Board of Governors (BOG).[51] Iran's clandestine nuclear weapons programme brings home the fact that the old safeguards system failed to detect its almost 20 years of non-compliance and, therefore, was inadequate. The widely-proclaimed strengthened safeguards arrangements, including the Additional Protocol, are still viewed to leave space for non-detection of undeclared facilities. The IAEA is viewed to be away from the "anytime, anywhere" verification capability and the "special inspection of cases" remains a highly politicised option within the BOG.

There are reports saying that at least 24 states have not complied with their obligation to have a comprehensive safeguards agreement.

Informal non-proliferation arrangements have emerged in the last few decades, sometimes supplementing the NPT and sometimes in reaction to its loopholes. The Zangger Committee and the Nuclear Suppliers Group (NSG) are multilateral arrangements that strive to restrict and monitor nuclear technology flow. However, their role has been criticised by many as "they breach the spirit if not the letter of states' inalienable right to the

51. Findlay, n. 43, p. 146.

peaceful uses of nuclear technology under the NPT". They seem to remain as "political lightning rods", therefore, the question arises whether these frameworks can ever be integrated into the formal structures of the IAEA.[52]

Three other relatively recent frameworks are the Proliferation Security Initiative (PSI), Global Nuclear Energy Partnership (GNEP) and Nuclear Security Summit (NSC). The PSI, which aims to interdict WMD technologies, started in 2003 and a growing number of countries are becoming its members. However, China objects to the PSI, regarding it as a threat to the Law of the Sea and interdiction of dual use technologies. The GNEP, while promoting civilian nuclear applications through the highest non-proliferation standards, aims to develop 'proliferation resistant' technology which is yet to be developed. The two NSCs have been successful to a certain extent in highlighting the imperatives of nuclear security and the substantive measures to be undertaken. However, there is considerable dilemma on how to reconcile national sovereignty with global responsibility to meet nuclear security objectives. It is really worrisome as some countries do not recognise the nuclear threat at all and even countries that do recognise the threat, may not recognise its full scope.[53]

Examining the contemporary harsh realities, Graham Allison says, "It is hard to avoid the conclusion that, on our present trajectory, the likelihood of a nuclear avalanche is greater than the prospect of reaching the peak".[54] While Iran and North Korea have produced enough nuclear material, Pakistan, a troubled state, is hurrying to expand its inventory. According to the IAEA Illicit Trafficking Data Base, from January 1993 to December, 2012, a total of 2,331 incidents was reported out of which 419 involved unauthorised possession and related criminal activities.[55] Unless and until "a brand-new innovative design, or architecture, based on long range views

52. Ibid., p. 151.
53. "Global Dialogue on Nuclear Security Priorities", Rapporteur's Report, Airlie Centre, Virginia, August 9, 2012, http://www.nti.org/media/pdfs/1st_Global_Dialogue_Rapporteurs_Report_July_2012.pdf?_=1353368765
54. Graham Allison, "Obama's Nuclear Vision – or Illusion?", *The Boston Globe*, April 5, 2013, http://www.bostonglobe.com/opinion/2013/04/04/obama-nuclear-vision-illusion/aj3Bn8W1iPZ5so00LdgPHP/story.html
55. IAEA, "IAEA Incident and Trafficking Database (ITDB)", http://www-ns.iaea.org/downloads/security/itdb-fact-sheet.pdf

and shared understanding of risks and their transversal impacts"[56], which the NSS is aiming to for, is put in place within a specific timeframe, the nuclear industry would only inch towards doomsday.

Many other regional and bilateral security frameworks like Nuclear Weapon-Free Zones and non-attack of nuclear installations seem to have been effective in certain cases. One nuclear weapon-free zone treaty – the African Nuclear Weapon-Free Zone Treaty (ANWFZ), known as the Treaty of Pelindaba – contains provision for ensuring the physical security of nuclear materials. It extends to the entire African continent and bans attacks on nuclear facilities. The treaty facilitates exchanges of information, consultations and compliance with the treaty obligations. Similarly, in South Asia, India and Pakistan have signed the treaty on Non-Attack on Each Other's Nuclear Facilities. The treaty was drafted in 1988, signed by the Pakistani Prime Minister Benazir Bhutto and her Indian counterpart, Rajiv Gandhi, on December 21, 1988, and entered into force in January 1991.[57] This obliges each party to refrain from undertaking, encouraging, or participating in, directly or indirectly, any action aimed at causing destruction or damage to any nuclear installation or facility in either country. It specifies each party to inform the other of the precise locations (latitude and longitude) of nuclear installations and facilities by January 1 of each year and whenever there is any change. For the last two decades, both countries have maintained the sanctity of the treaty and it has remained a significant nuclear (security) Confidence Building Measure (CBM) between them.

Most critical to global nuclear governance is the **role of national nuclear regulators.** They comprise the channel through which global governance norms, treaty obligations and recommended standards are implemented. A clear-cut separation of responsibilities between the nuclear regulatory and promoting agency is prescribed for strict and unbiased implementation

56. Irma Arguello, "Basis of a New Global Order for Nuclear Security", March 2012, http://www.nsgeg.org/Basis%20of%20a%20New%20Global%20Order%20for%20Nuclear%20Security%20-%20Irma%20Arguello.pdf
57. *Agreement between India and Pakistan on the Prohibition of Attack Against Nuclear Installations and Facilities (India-Pakistan Non-Attack Agreement)*, http://cns.miis.edu/inventory/pdfs/aptindpak.pdf

To utilise the best practices and benefit from each other's experiences, the effort has been to establish cooperation among nuclear regulators across the globe.

of safety standards. Having a regulatory body too close to organisations that promote nuclear projects is not healthy for the fact that it may compromise on implementation of safety rules and procedures. It is alleged that regulatory bodies in Brazil, India and South Africa are more proximate to the promoting agency. However, to utilise the best practices and benefit from each other's experiences, the effort has been to establish cooperation among nuclear regulators across the globe. There are now many such forums that facilitate interaction and cooperation. For example, the Network of Regulators of Countries with Small Nuclear Programmes (NERS); CANDU Senior Regulators; Cooperation Forum of State Nuclear Safety Authorities of Countries which operate WWER Reactors; and European Nuclear Safety Regulatory Group (ENSREG). The International Nuclear Regulators Association (INRA) established in 1997, having 31 regulators as its members provides a periodic forum to discuss nuclear safety and collective strategy. However, there is no universal international organisation that encompasses all regulators worldwide.

BALANCING SOVEREIGNTY WITH RESPONSIBILITY

Nuclear safety and security comprises a sovereign responsibility but only individual state determination of standards and their implementation is not enough. Strengthened international cooperation and accountability are urgent for early detection, prevention of attack, theft, sabotage and accidents involving nuclear material. For this to be achieved, "threat awareness" needs to be understood globally, at least, the "base level awareness." The goal is not only good global governance but "effective nuclear security implemented at all sites where it is needed." Global governance is "one tool to move toward that goal but not the only tool."

In case the global governance is in contradiction with the national responsibility, the necessity is a fine balancing of sovereignty with

international responsibility of nation-states so that both are served simultaneously. On the other hand, extremely strict guidelines/standards to integrate the three spheres when a country newly introduces nuclear power generation may prove impractical. So, all standards should be limited to the minimum necessary. More importantly, instead of leaving the nomenclature of standards in the domain of individual states, it would be preferable to have the IAEA develop these standards.

To emphasise the need for a global response and national accountability, Senator Sam Nunn has identified the three biggest challenges to global nuclear safety and security initiatives today that need to be addressed urgently: (a) the state that does not recognise the threat of nuclear terrorism; (b) the state that does not take protective action; (c) the state that is complacent.[58] A collective responsibility for a "more robust, effective, and flexible" nuclear management system is the need of the hour. As the current achievements are not necessarily faring much better, the nuclear industry has not been able to obtain a wide range of public support.[59] In the meantime, nuclear disasters may occur, giving rise to further 'nuclear fear'. Realistically, every defence is time critical and can deteriorate as time passes. Therefore, the *nuclear defence* architecture that encompasses safety, security and safeguards, must be structured beyond design-basis threats, taking into account the intricacies of technical interfaces, professional integrity, social psychology, national obligations, and international collaborations.

58. Sam Nunn, "Remarks at the Global Dialogue on Nuclear Security Priorities", http://www.nti.org/analysis/speeches/remarks-global-dialogue-nuclear-security-priorities/, July 23, 2012.
59. Atsuyuki Suzuki, "Toward a Robust Nuclear Management System", *Daedalus*, Winter 2010, p. 82.

GEO-POLITICS AND STRATEGY FORMULATION

PRATEEK KAPIL

Is there a limit to human will? Is geography a constraint or a legitimate determinant which checks human zeal? Are political geographers overtly deterministic in their analyses and detached to the possibilities of human capabilities? Or are they prudent realists who see the world as it is and not how it should be? These questions form the essence of the use of geo-politics in strategy formulation. It is often rued that American power oscillates among the Vietnam psyche of overstretch, lack of exit strategy or disproportionate force to the Munich psyche of interventionism, regime change, human rights and promulgation of a liberal international system even at stretched costs. The wars of Iraq and Afghanistan are symptomatic of the former while the Yugoslavian intervention was symptomatic of the latter. Renowned strategist Robert D. Kaplan argues that while there are many human processes at work, such extremes can be avoided if nations prioritise one major factor in their calculation: geography.

GEO-POLITICAL THEORY: KEY PROPONENTS AND CONCEPTS

Friedrich Ratzel[1] (1940) presented a number of key concepts that would be developed further by others in the field of geo-politics. For example, it was Ratzel who gave the earliest and most complete definition of the

Mr **Prateek Kapil** is a Research Associate at the Centre for Air Power Studies, New Delhi.

1. W.J. Cahnman, "The Concept of Raum and the Theory of Regionalism," *American Sociological Review*, 9(5), 1994, pp. 455-462.

The frontier region creates opportunities for the emergence of enclaves of ethnic sub-groups that struggle to exercise a degree of political power and influence over the larger society.

term *raum,* or room. Alternatively understood as "space," this concept relates to Ratzel's conceptualisation of organic state theory and states as spatial organisms that require room or space in which growth is possible. Borders become insignificant in that a developing state or one that is advancing is likely to require annexation of territories that are controlled by other less powerful states. Ratzel recognised, as did Darwin, that there is an inevitable struggle for life that occurs even in the case of nation-states. Such a struggle requires a state to grow or to die, losing or gaining influence in direct proportion to its capacity for defeating or overcoming its rivals.

Frederick Jackson[2] Turner proposed a major thesis focussed on the role of the frontier in political life. Turner held that the frontier was a major influence in shaping the unique character of America and American culture. It was his contention that the experience of the rugged and challenging life in the frontier regions of the country as it expanded ever westward was instrumental in fostering self-reliance and sectionalism. Sectionalism, in his view, was a direct result of the coming together of specific ethnic and other groups in a particular place, creating in essence a unique sub-section of the American polity that would come to define a place as well as a people.

The frontier region creates opportunities for the emergence of enclaves of ethnic sub-groups that struggle to exercise a degree of political power and influence over the larger society. However, Turner's most significant contribution is his understanding of the role played by the frontier in shaping national character and in forging sectional relationships and sectional conflict.

Friedrich Naumann's (1917) text, *Muittel-Europa*, proposed that within Europe there existed a central entity composed of the Germanic countries which should be joined together to create a formidable force to be called

2. Ibid.

"Central Europe." Such a force would have the political and ideological capacity to stave off any and all attacks or threats from other European countries. It would further be capable of preventing the Ottoman Empire, then one of the most powerful and aggressive forces in the world, from making further inroads into the European heartland. For Naumann, the combined forces of the German *volk* were of such substance that they could, working in concert, achieve European hegemonic domination. Using a military organisation as the basis for this new state entity, in Naumann's view, would establish a viable source of European security in a perilous age. There is also the contrarian concept – a liberal dream – of Mittel Europa which should be spread throughout the world with its liberal political philosophy but which, as shown by the current European crisis, has fallen prey to the nationalistic geography driven ethnic divisions. Although the European Union (EU) supra state is alive and feasible, its future evolution and consequent relations with the US and Russia will have strong geo-political considerations and irritants.

Halford MacKinder[3] (1904, 1919) proposed that the world had experienced three unique geo-political periods. The closed heartland of Eurasia was the geographical pivot or location that was central to establishing global control. This was premised on the conviction that the age of maritime exploration which began with Columbus was drawing to a close as the 19th century ended. The next period of geo-political influence would be based upon land transportation technology which would reinstate land-based power as opposed to sea power as essential to political dominance. This would lead to a resurgence of Eurasia because it was adjacent to the borders of so many important countries, was not accessible to sea power, and was strategically buttressed by an inner and outer crescent of landmasses. The third or preliminary period of geo-political interaction was also a period in which land transportation dominated. Thus, MacKinder (1919) proposed the periods of land, sea, and land transport again as shaping geo-political relationships while the heartland remained the key position on the global battlefield regardless of which type of transportation dominated.

3. H. MacKinder, "The Geographical Pivot of History," *Geographical Journal*, 23(2), 1904, pp. 421-444.

Rimland states such as Japan, India, China were likely to become superpowers over time.

Alfred Thayer Mahan,[4] on the other hand, was convinced that beginning with the Age of Exploration, the nation-states that achieved great power status did so because they had mastered sea power. He further contended that the mastery of commercial activities that elide on seaborne transportation was critical not only in times of war but also in times of peace. He felt that any country building a fleet that could destroy an enemy's main force in a single battle would become a hegemonic force. Mahan's fundamental assumption regarding the importance of sea power was his belief that economic competition sat at the heart of all rivalry between nations. One should recall that when Mahan presented his ideas, there were limited methods of communicating and transporting ideas as well as goods from one part of the world to the other. Mahan emphasised the highway aspect of the sea and argued that any country that was dependent on the world economy needed to be able to secure access to the world and could do so only if no enemy fleet dominated the seas. What differentiates Mahan from other thinkers is his constant emphasis on the overarching significance of sea power and sea transport which he felt were destined to remain the dominant mode of international interaction even in an era when the railroad and land transport systems were expanding at a dramatic rate.

For Nicolas Spykman (1938), Eurasia's periphery and not its core are seen as the key to global power. This periphery in Spykman's viewpoint should be known as a rimland. Rimland states such as Japan, India, China were likely to become superpowers over time. Because rimland states had greater contact with the outside world or the countries that were not part of the heartland itself, they received more in terms of innovation than did the heartland countries. Rimland states also possessed a wealth of natural resources and though Spykman agreed with MacKinder on this particular concept, he gave greater credence to the capacity of rimland states to

4. A.T. Mahan, "The Influence of Sea Power Upon History," 2008, available at www.guttenberg.org/files/13529

capitalise on their natural advantages and resources than did MacKinder[5].

Moving on, Deibel and John Lewis Gaddis (1986) suggest that the policy of containment evolved over time as the United States moved away from direct military confrontation of Communist expansionism in South Korea and Vietnam to a less militaristic response that employed economic and foreign aid as a means of leading the non-aligned nations into the Western sphere of influence. At the same time, the continued willingness of the US to participate in the arms race which lasted into the Reagan Administration was very much a military response to the perceived Soviet threat. Containment emerges as a strategy that was designed to offset Soviet hegemonic ambitions in terms of the Eurasian heartland and countries within the periphery or the rimland. It is an excellent example of great power politics being played out in a bipolar world wherein two determined superpowers are willing to compete almost indefinitely for dominance.

Saul B. Cohen[6] (2003) makes use of the related concepts of gateways and shatterbelts. A shatterbelt is a region of the world wherein enormous political volatility exists and wherein conflict is endemic and dominant world powers are often seen as threatening entities which must be resisted. Cohen claims that the Middle East is an excellent example of a contemporary shatterbelt wherein tensions run high and the potential for conflict that could spread outside the region is also present. Gateways, in comparison, are seen by Cohen as points of entry into autonomous or semi-autonomous heartlands. Eastern Europe, the Trans-Caucasus, and Central Asia are gateways that have at times also been shatterbelts. The difference between a shatterbelt and a gateway depends on the degree of internal stability that the region has achieved or which it is able to maintain in the face of internal and external ideological and economic forces. While Samuel Huntington foresaw a clash of civilisations as a consequence of the end of the Cold War, Cohen suggests that globalisation and the diffusion of technology will favour accommodation even within the highly volatile shatterbelts. Cohen's

5. N. Spykman, "Geography and Foreign Policy," *American Political Science Review, 32(1)*, 1938, pp. 28-50.
6. S.B. Cohen, *Geopolitics of the World System* (Lanham, MD: Rowman & Littlefield, 2003).

(2003) analysis identifies a new hierarchy of geo-political units. These units range from the sub-national to the geo-strategic and global. By emphasising the interaction between these units, Cohen has essentially proposed that a new world order is likely to develop as a consequence of new economic activities.

CONTEMPORARY GEO-POLITICS

Geo-politics as a field of study was furthered in its cause by many of these strategists like Mackinder, Spykman, Braudel, Bracken, Hodgson and A.T. Mahan. Mackinder theorised (in the language of his time) that whoever controls the Eurasian landmass controls the World Island. Spykman and later A.T. Mahan posited that the rimland on the southern periphery of the Eurasian landmass, with insistence on sea power, was critical to projection of power on the Eurasian landmass. He also considered India the core region of the rimland with potential to project sea-based power across East-West in the Indian Ocean. The Turkish and Arab Middle East which approximates Hodgson's Oikoumene and Mackinder's continental satellite, North America, are two other crucial actors in this geo-political international system. All these analyses have been familiar constructs over the past century, especially during the World Wars and the Cold War. Undoubtedly, however, these 20th century analyses have undergone critical corrections over the last 20 years, especially due to the revolution in communications, technology and globalisation. The end of the Cold War was hailed as the end of history with American preponderance consolidated by the global proliferation of liberal democracy and modern capitalism. The rate of technological progress compressed distance and time, and "a flat world" was born, in the words of Thomas Friedman. Yet globalisation that has brought people together, has simultaneously accentuated nationalist and sovereign trends as well. Consider the Arab spring as an example where self-immolation by a Tunisian fruit seller, while initiating region-wide demonstrations across countries, eventually progressed in very different ways in each of these countries. The results have been different in Egypt, Libya, Syria, Bahrain, Yemen, Saudi Arabia and Tunisia. The difference

lies in the fact that human processes and actions can instigate short-term and middle-term factors but certain features of a nation remain deeply ingrained due to the long-term glacial processes of culture, state formation, societal changes all of which are affected by the most inflexible of them all – geography. Kaplan in his book, *The Revenge of Geography*, eloquently elucidates why certain countries in spite of their vigorous societies and dynamic institutions owe a lot of their success and failure to geography! The US, protected by oceans on either side and the Arctic belt on the north, Britain with the English Channel separating it from continental Europe, Russian land-based power with no outlet to the sea because of the frozen sea lanes on the north, the historical northwest threat to the Indian subcontinent, the Chinese continental power along with natural harbours and vast coastline, the Anatolian land-bridge that is Turkey and the fragmented geography of Iraq are all good examples. The point I'm trying to make is that while human constructs and processes can achieve a lot, human strategies need to be seriously tempered by geographical constraints. Although somewhat basic, this has often been overlooked and taken for granted in the 21st century strategy formulation. US neo-conservatives proved it in Iraq. The Soviet Union had proved it in Afghanistan. India too suffered a setback in 1962 due to these reasons.

Geography helps in determining the probability and feasibility of long-term grand strategic goals.

This is not to say that geography is a roadblock – after all, science and technology have proved otherwise. In fact, geography helps in determining the probability and feasibility of long-term grand strategic goals. For example, while the Munich mentality of the 1990s was at work during the American intervention in Afghanistan, further justified by the proven culpability of a completely rogue and irrational Taliban regime in the 9/11 attacks, the post-Vietnam mentality would have called for a coherent exit strategy which, in turn, would be governed by the geo-political fact that Afghanistan over centuries has remained stable only when ruled by a central Kabul with power sharing agreements with the provincial governments, devoid of external intervention. Further, geo-political logic would suggest

that the stabilisation of the Afghan economy centres on minerals and energy transit facilities for Iran, Central Asia, Pakistan, India and China. This, in a nutshell, is the role geo-politics plays in the articulation of any Grand Strategic Goals. The *zeitgeist* of the time is to respect your weaknesses more than your strengths.

China is proceeding with the same after witnessing American predicaments. The US itself is trying to realign strategy in this direction as shown by the pull-outs, pivot to Asia and budget sequestration. Beyond a point, it has to be realised that intervention may be necessary in the case of a regime like the Taliban, but perhaps not in the case of a regime like Saddam's, and an exit strategy respecting the geo-political factors of the region has to be thought out to avoid a quagmire. A look at Iraqi geography would have showed that the fragmented politics of the mountainous Kurds, the central Sunnis and the Iran influenced minority Shias has always required a strong semi-dictatorial central control, and absence of a modern liberal political philosophy in the region would result in violent power struggles in case of a power vacuum. It is undeniable that the Saddam regime had allegations of excesses but the dilemma to be answered in 2003 was: what kind of Iraq was the US striving for? As it turned out, the US made the wrong choice in initiating that action. A history of the geo-politics of Iraq could have served as deterrence. In geo-political terms, the Vietnam mentality is about limits; the Munich mentality about overcoming them. Each extreme can be dangerous on its own. It is only when both are given equal measure that the right strategy has the best chance to emerge. As the dictum goes, "The art of statesmanship is about working as close to the edge as possible, without stepping over the brink."

CLASSICAL REALISM: A THEORETICAL CONFIDANT OF GEO-POLITICS[7]

Modern realism was most comprehensively summed up in 1948 by Hans J. Morgenthau in *Politics Among Nations: The Struggle for Power and Peace*.

7. Robert D. Kaplan, *The Revenge of Geography* (New York: Random House Publications, First Edition, 2012), ch. 2, pp. 23-38.

Morgenthau begins his argument by noting that the world "is the result of forces inherent in human nature" And human nature, as Thucydides pointed out, is motivated by fear, self-interest and self-help. "To improve the world," writes Morgenthau, "one must work with these forces, not against them". Realism appeals to historical precedent rather than to abstract principles and aims at the realisation of the lesser evil rather than of the absolute good without ruling out the achievement of the latter in the process. Good intentions have little to do with positive outcomes, according to Morgenthau. All nations are tempted—and few have been willing to resist the temptation for long—to clothe their own particular aspirations and actions in the moral purposes of the universe. To know that nations are subject to the moral law is one thing, while to pretend to know with certainty what is good and evil in the relations among nations is quite another. Furthermore, states must operate in a much more constrained moral universe than do individuals. The individual may say to himself, "Let justice be done, even if the world perishes," but the state has no right to say so in the name of those who are in its care. Realists expect conflict and realise it cannot be avoided; they are less likely to overreact to it. It is, ultimately, only the existence of a universal moral conscience which sees war as a "natural catastrophe" and not as a natural extension of one's foreign policy that limits war's occurrence. Realism does have a tendency of making people uneasy. Realists understand that international relations are ruled by a more anarchic limited reality than that governing domestic polity. Domestic polity is defined by laws because a legitimate government monopolises the use of force, and the international system is still in a state of nature, in which there is no Hobbesian leviathan to punish the unjust. Realists prioritise order above value judgements: for them, the latter become important after the former has been established. In Iraq, the order, even of totalitarian dimensions, turned out to be more humane than the lack of order that followed. And because world government will forever remain elusive, since there will never be a fundamental agreement on the ways of social betterment, the world is fated to be anarchic and ruled by different kinds of regimes.

On the relatively stable foundation of geography, the pyramid of national power arises.

On the relatively stable foundation of geography, the pyramid of national power arises. For at the root, realism is about the recognition of the bluntest, most uncomfortable, and deterministic of truths: those of geography. A state's position on the map is the first thing that defines it. A map, explains Halford Mackinder, conveys "at one glance a whole series of generalizations". Geography, he goes on, bridges the gap between arts and sciences, connecting the study of history, politics and culture with environmental factors, which specialists in humanities sometimes neglect. "That technology has cancelled geography contains just enough merit to be called a plausible fallacy" writes Colin S. Gray. Having said that, factors like geography, history and ethnic characteristics influence but do not determine future events. Immediately the question beckons: how do you split the difference between recognising the importance of deterministic factors and the danger of overemphasising them? Raymond Aron tried to solve this question with his concept of probabilistic determinism. Strategy, he concluded, should always come out of a rigorous probabilistic analysis of determinist, individualist and miscellaneous factors.[8]

INDIAN GEO-POLITICS AND STRATEGY

The traditional threat to the Indian subcontinent has always emanated from the northwest. India was artificially divided into India and Pakistan which itself involved seismic human processes of migration, partition and assimilation. Thus, the relatively continuous transition from Central Asia to the subcontinent has been impeded by man-made disputed and porous boundaries. Some analysts even state that like the post-Westphalia period in Europe, the process of fixed boundaries and state making is still to unfold in the region. In other words, the states are still evolving. Historically, invaders often treated the areas around the Hindu Kush as a base camp to invade the subcontinent. Although overrunning invasions and foreign control are fanciful in 21st century India, it still goes a long way to explain why Indian

8. Ibid.

decision-makers are extremely sensitive to developments in the Af-Pak region. The current Pakistani belligerence in the region affects both American and Indian strategy. It is important to impress upon the Punjabi dominated Pakistan Army that covert support of the Taliban might radicalise southeast Afghanistan and the Northwest Frontier Province (NWFP) on either side of the Durand Line, thus, uniting the Pashtuns under a radical leadership and, in turn, antagonising the comparatively moderate Pakistani provinces of Punjab and Sindh. This would jeopardise Afghan and Pakistani state building efforts in a major way. Free and fair elections in both Afghanistan and Pakistan and a departure from Pakistani insistence on Afghan strategic depth and covert warfare against India are critical to the stabilisation of the Indian northwest. Only a stable northwest can bring India into a fair bilateral negotiation about Kashmir. Pakistan, by continuing its present strategy, is playing into the trap of what Sumit Ganguly calls the *jihad* paradox. Pakistan is employing non-state actors to fight its adversaries because the state is relatively weak compared to the adversaries but the continued employment of such non-state actors is, in turn, further weakening the state-making process in both Pakistan and Afghanistan. Pakistan needs to transcend the paradox by more state control, institution-building and more diplomatic forms of national strategy. The nuclear parity between India and Pakistan should, in the words of Kenneth Waltz, lead to nuclear stability rather than covert activities by either government under the nuclear threshold. The land contiguity, sea connectivity and proximity can transform the economic and trade relationship but the same geography can lead to brinkmanship, higher stakes and extremely small margin of error. India, on its part, needs to understand that beyond a certain point, geographical limitations will restrict its ability to influence events in Afghanistan and Pakistan and, therefore, it needs to maintain a development and diplomatic footprint in the two countries and invest in quarantine strategies of homeland security and American alliance.

The US strategy in the subcontinent needs most seriously to take geography into account. America is transitioning to the phase where its grand strategy will operate on limited resources, flexibility, rebalancing and

alliance building. The Asia pivot suggests that America will look to extricate itself from the Middle East quagmire, barring traditional allies, and prioritise the Asia-Pacific. Here, it will look to delegate certain responsibilities to the allies, with American sea power being projected in alliance with the Japanese and Indian Navies.

The Chinese strategy is obviously cognisant of this. The Chinese naval presence in Gwadar is a game changer. With an allied Pakistan which could be coerced to facilitate a stable transit to Afghanistan, China will have increased access to the Persian Gulf and Central Asia along with the planned Silk Route all the way to Turkey. Indian presence in Chabahar port is critical to our counter calculations. This might involve some tricky give and take between the US and India on the issue of the alliance structure and strategy on the two vital geo-political areas of the Persian Gulf and Asia-Pacific. America is focussed on continuing as an influential Asian power while India's core interest lies in domination of the arc of the Indian Ocean across East and West. A port in northeast Africa could be another strategic asset for both India and China in projection into the Middle East. An India-China relationship has been set back by a festering border dispute with topography and capabilities in favour of the Chinese side, leading to a competitive relationship, in geo-political terms. Robert Kaplan, alluding to the Sino-Indian relationship states that "India could emerge as the global pivot state supreme, tilting on some issues toward the United States and on others toward China. "If you accept the notion that the most important bilateral relationship of the 21st century will be that between the United States and China, then India[9] – because of the size of its population and economy – emerges as the weathervane of international politics. The more turbulent Central Asia and South Asia become politically, the less of a chance there is to develop those pipelines, thus, slowing the emergence of the Indian Ocean as the premier strategic region. The growing dominance of China will lead the citizens of India – particularly its ruling economic classes – to become increasingly frustrated with the inefficiencies of their own tumultuous

9. http://www.foreignaffairs.com/discussions/interviews/qa-with-robert-kaplan-on-geopolitics-in-the-indian-ocean?page=show

democratic system. I am not talking here of a desire for authoritarianism but for more efficient and less corrupt governance. Competition with China could be the catalyst for the Indian government to perform better than it does. Precisely because there will be points of tension in the Indian-Chinese relationship, India must do all that it can to seek out points of agreement with China in order to stabilise relations. Merely seeking cooperative economic agreements with other countries along the rimland of the Indian Ocean will strengthen India's strategic position vis-à-vis China.

An average Chinese seems to prioritise order and an average Indian prioritises individuality and freedom.

While the South China Sea and East Asia Sea are undoubtedly Chinese areas of influence with America continuing to be muscled out by an assertive Chinese Navy, future American strategy involves nimble-footed flexible patrolling from areas like Guam and other American owned islands in the region and quick intervention in the event of Chinese action against an ally. This is in coordination with other navies of the region which can quickly come together to form a coercive fleet in the event of a crisis. The credibility of the American military machine remains intact. America is still the preponderant military power with a core competiveness of high-tech disruptive warfare. Despite the draining wars in West Asia, military expenditure still doesn't form the major chunk of the debt with issues like health care still dominating domestic politics. The US, thus, is realigning its strategy while still retaining credible capability of deterrence and swift, selective intervention in any part of the globe.

Chinese-American geo-politics will decide the future of the international system. China and the US are both continental powers with natural harbours and long coastlines. China's proximity to the Eurasian landmass and Spykman's rimland gives it exceptional strategic assets of power projection similar to the US in the Western hemisphere. The Chinese have somewhat succeeded in homogenising the geography of the Chinese state with a few exceptions of Tibet and Taiwan. That is because, as the Indian strategist Air Commodore Jasjit Singh opined, an average Chinese seems to

The nature of Chinese power would ultimately decide the direction but it would have to follow the classical balance of power logic.

prioritise order and an average Indian prioritises individuality and freedom. It remains to be seen what the Chinese response to the greater assertion of the latter would be. China has a rich civilisational platform at the Yellow and Yangtze river basins from where the Chinese people flourished. In that sense, it is a similar to the civilisational history of the subcontinent which too flourished in isolation for centuries before foreign dominance. Hence, China is a civilisational state and its geo-political strategy is planned in the long term. Time is defined in a much broader sense in the Chinese lexicon. Historically, the Chinese leadership has centralised and emphasised authoritarian control to maintain order but with greater growth and stability, China needs to reinvent itself politically. With greater interaction with the neighbourhood and the world, geography is forcing structural changes in Chinese society. The urbanisation, the export driven growth stagnation, the different systems of Hong Kong and Macau, the stand-offs with East Asian neighbours, and the rising inequality in different regions have resulted in new challenges for the leadership which the Chinese Communist Party (CCP) has coped with so far but it is still an ongoing challenge. In fact, even if the CCP fails and the extreme event of democratisation takes place, a democratic China might become an even more dynamic economic power, so the Indian strategy should be primarily governed by geo-political factors. There is an adage in geo-politics: "A world balanced is a world free". Thus, whatever be the result of internal and human processes in China, other nations should also look to check it geo-politically. Therefore, the US will look to either balance or bandwagon China in a regional arrangement which would make it unfavourable for China to be disruptive or revisionist. Structural regimes like the Shanghai Cooperation Organisation (SCO), Asia-Pacific Economic Cooperation (APEC), Association of Southeast Asian Nations (ASEAN) plus and Pacific community, inclusive or exclusive of China, are possible outcomes. The nature of Chinese power would ultimately decide the direction but it would have to follow the classical balance of power

logic. Due to the proximity of China to the countries and in the absence of institutionalisation, unlike the North Atlantic Treaty Organisation (NATO), countries would look to balance China with US help. Although the US will continue to decline in relative terms, it is the process of its decline which is crucial to the US. A smooth transition, similar to Britain's rather than a systemic collapse like the Soviet Union's, is what the US is aiming for. The timeline may be variable but the geo-political logic suggests that no hegemony can be perpetual but the transitions can be disruptive, gradual or variant. Space is always contested among nations but strategy and nature of engagement decide the eventual pay-offs and outcomes.

CONCLUSION

In conclusion, this paper was an attempt in contextualising the geo-political puzzle before India. India, with its burgeoning demographics and huge economy, needs to focus on wealth creation and political stabilisation through proper redistribution and respect for civil liberties to first homogenise its own geography. It has a diversity of ethnicities, central location in the Eurasian continent, crippling energy dependency on the northwest and secure lanes of communication, proximity to a continental power, an outward global outlook of the citizenry, command of the English language, huge investments in education and infrastructure, nascent manufacturing in spite of rich endowment of natural resources, economic and political reforms which respect the decentralised nature of Indian geography along with central direction and strategy formulation. Effective implementation and promulgation of Acts like the Land Reforms Bill, GST, Foreign Direct Investment (FDI), Forest Rights Act, Judicial Accountability Bill, Ombudsman Bill, Social Safety net legislation, etc., sustenance of the services economy and continuing progressive use of Information and Communication Technology (ICT) and Research and Development (R&D) are critical factors to equip ourselves for the geo-political challenge. These strong fundamentals will both influence and enable our central leadership and armed forces to strategise cogently for the geo-political challenge ahead. The alliance choices, the force structure, the investment in defence

imports and indigenous defence production are directly linked to the factors mentioned above. In my analyses, an alliance with the US, hedging behind the US to delay confrontation with China while increasing trade and staying sensitive to China's Tibet concerns, diplomatic mechanisms and avoiding conflagration on the Chinese border for another 10-15 years, domination of energy routes through the Indian Ocean and quarantining the northwest frontier are the core challenges of the Indian geo-political strategy.

The probable grand strategy dealing with these respective core geo-political challenges could have the following elements:

- A strategic treaty with the US with proper institutionalisation of mutual trust to impress upon them the Indian security stakes in a stable Afghanistan, similar to theirs in the Persian Gulf (a *quid pro quo* to that effect can be considered).
- Investment in disruptive air and sea power technologies.
- More clear yet independent strategic choices perhaps in coordination with US policy in the Asia-Pacific and the Persian Gulf.
- Steering clear of the radical human processes on either side of the Durand Line while maintaining a developmental footprint; no political or military overtures to transform Af-Pak or engage the region without action; and institutional assurances on terrorism and employing economic levers in the short-term across the geo-political region.

Finally, I revert to two central ideas of geo-politics and classical realism which could steer the Indian grand strategy: "There is a Limit to Human Will" and "A World Balanced is a World Free".

CYBER WARFARE AND NATIONAL SECURITY

E. DILIPRAJ

INTRODUCTION

In the wake of the 21st century, the cyber world began to spread its roots deep into the society and penetrated the lives of the people so much so that the internet became an indispensable part of the citizens' life, thus upgrading them to the status of 'netizens'. Moreover, technology in cyber space gained dynamism, increasing the population of netizens. This became possible in the cyber space not because all the citizens became technically sound but also because the cyber technology became more user friendly. Nevertheless, the height of the 'liberty to express' was readily available in the cyber space by virtue of the very low level of restrictions and legal barriers applied by the governments of the countries in the cyber space.

The cyber space began to grow in terms of information and also in the population of users with the passage of time. The users of the cyber space ranged from children looking for information for school assignments to business tycoons seeking profits; from the governments' e-governance services for the public to terrorists/non-state actors using it for their online communications and covert operations. As a result, in due course, this unregulated cyber space became a mine of information worth billions, thus, opening up a battleground for the netizens to acquire such vast information

Mr **E. Dilipraj** is a Research Associate at Centre for Air Power Studies, New Delhi.

Citizens of a country who were unable to express their hatred and fight against a rival state brazenly, found cyber space a suitable option.

and also to sabotage the same to fulfil their own motives. The important feature of this battle was that it did not require an army to fight it—an individual, capable of writing a few lines of codes and with a minimal level of expertise in cyber technology, could wage a war against a country.

This form of battle among the netizens in the cyber space is referred to by various terms like cyber crime, cyber war and cyber terrorism, depending on the nature of the perpetrators and the consequences. This also became the preferred form of the fight of the public against their perceived enemies ranging from an individual to a government due to the following reasons: the low level of restrictions and legal barriers, the anonymity and no casualties, and, most importantly, the indispensability of minimal resources and the need of infinitesimal people with little expertise. Almost all the countries of the world faced this challenge in their respective cyber space on a regular basis and it was more often experienced in the networks of rival states. In addition, citizens of a country who were unable to express their hatred and fight against a rival state brazenly, found cyber space a suitable option to vent their anger and hatred as it provided them a natural outlet and anonymity, along with the weapon of technology. In this regard, no country of the world was an exception in this cyber hate contest, including India and Pakistan.

India and Pakistan: The South Asian neighbours have fought three major conventional wars ever since their birth in 1947, until the end of the 20th century – in 1947-48, 1965 and 1971, and a smaller war in 1999. At the end of the 20th century, the tension between the two nations increased to its highest level, as both countries achieved the status of 'nuclear weapon states' after successfully conducting nuclear explosive tests for military purposes, one after the other. Although nuclear deterrence and other international pressures prevented these two countries from getting into another major war in the later scenarios, the hatred for each other in the minds of their citizens has only got aggravated. This hatred deepened when

the state sponsored terrorism from Pakistan became the highest national security threat for India from the 1990s and the Indian armed forces were busy retaliating against it. The people were waiting for an opportunity to express their anger and hatred towards each other.

Actions of people in the cyber world against any network belonging to someone else are referred to as cyber attacks.

THE ICE BREAKER

As mentioned earlier, the world of cyber space advanced rapidly but with almost no regulations, resulting in vulnerability to the use of technological luxuries for immoral and anti-social purposes. As a result, this became the voluntary medium for the people to express their views and emotions to their targeted audience all over the world and they started using it for this purpose. These actions of people in the cyber world against any network belonging to someone else are referred to as cyber attacks and these started spreading all over the world with the number of incidents increasing over a period of time. They reached India on June 3, 1998, when the Indian website owned by the Bhabha Atomic Research Centre (BARC) came under a cyber attack by a group called 'milw0rm'. The attack was caused by breaching into the website of BARC and defacing the same. It was also found that the attackers had downloaded five megabytes of e-mails and data from the database.[1]The attackers claimed in their message in the defaced website that the attack was in response to the testing of nuclear weapons by India on May 11 and 13, 1998. The defaced website of BARC had a message from the hackers as follows:

> Nuclear Tests in India. This page has been hacked in protest of a nuclear race between India, Pakistan and China. It is the world's concern that such actions must be put to an end since nobody wants yet another world war. I hope you understand that our intentions were good, thus, no damage has been done to this system. No files have been copied or deleted, and

1. http://ces.iisc.ernet.in/hpg/envis/doc98html/miscbarc69.html, as accessed on September 3, 2012, 11:30 am

main file has been just renamed. Stop the Nuclear Race! We Don't Want a Nuclear Holocaust.[2]

At first, it was believed that these attacks were from Pakistani hackers backed by the Inter-Services Intelligence (ISI) but later, after a thorough investigation, it was revealed that hackers were individuals who only had contacts among themselves through the internet, were operating under their pseudonyms and belonged to different nations. The group consisted of teenagers who went by the aliases of JR, Keystroke, ExtreemUK, savec0re, and VeNoMouS[3]. VeNoMouS, 18, hailed from New Zealand, ExtreemUK and JR, both 15, from England, Keystroke, 16, from the US, and Savec0re, 17, from Russia.[4]

Although, the first major cyber attack faced by an important Indian website was not by Pakistani hackers, the initial blame on them which came as the immediate response from the Indian side clearly exhibits the level of suspicion due to the distrust in the minds of the people. However, the attack on the website was proved to be not an act of the Pakistani hackers. This incident was the ice-breaking one which cleared the way for future cyber attacks between these two countries' netizens. After this incident, in the year 1999, there were four attacks on Indian cyber networks that were recorded and the investigations revealed that these were carried out from Pakistan. This count increased drastically to 72 in the year 2000, and there were also reports confirming seven attacks in 1999 and 18 attacks in 2000 on the Pakistani networks conducted from India.[5] Thus, a mutual cyber hatred contest began without much fanfare in the cables between the netizens of India and Pakistan.

This saga of the cyber hatred contest continued even in the 21st century where the first half of 2001 witnessed 150 incidents of defacing of websites on the Indian side; they also took place the Pakistani side but in comparatively

2. http://www.youtube.com/watch?v=XcL9EqUbg4Y, as accessed on 3/09/2012, 11:45 am
3. William C. Boni & Gerald L. Kovacich, *I-way Robbery* (UK: Butterworth-Heinemann, 1999), p. 142.
4. "India: Sahara India Mass Communication," *Rashtriya Sahara*, 1996.
5. Iftikhar Alam, "Pakistan India Cyber War Begins", *The Nation*, December 5, 2010.

fewer numbers[6]. Such cyber hatred attacks on both sides kept increasing every year and the victims of these cyber skirmishes were the key websites of both countries. Mr. Munawwar Iqbal, President of the Pakistan Computer Association (PCA) once stated in an interview:

> As per my information, there are two groups of hackers from both countries: one is called the Indian Cyber Army and the other is known as the Pakistan Cyber Army. Both are in competition to hack each other's websites. It is totally illegal, and should be stopped in the greater regional and international interest, as well as that of both countries' people. [7]

In the meantime, many new hacking groups started emerging and displaying their skills in the networks. Of these, one of the most notorious and dangerous groups originated from Pakistan – this was the Z Company Hackers Crew (ZHC) which has a record of attacking 1,846 Indian websites, both government and civilian.[8] There are also other hackers groups like Pakistani Hackers Club (PHC) whose founder is claimed to be from Karachi, and the G-Force, which is believed to be consisting of eight members, is from Lahore.[9]

On the Indian side also, there was the emergence of many groups of which H2O or the Hindustan Hackers Organisation[10] is famous among the cyber hacking community and another group called TEAM NUTS that did a record hacking and defacement of 57 commercial sites in Pakistan in one day in 2010.[11]

THE SPILLOVER EFFECT

As the cyber contest was nurtured on hatred and anger, growing day by day among the private hackers groups of India and Pakistan, it led to an increase

6. Alamzeb Khan, "Pakistan Cyber Warfare and Internet Hacking", January 17, 2012, URL: http://www.simple-talk.com/opinion/opinion-pieces/pakistan-cyber-warfare-and-internet-hacking/
7. Ibid.
8. http://www.hackread.com/read/hackread/3289
9. Alam, n. 5.
10. Ibid.
11. http://thehackernews.com/2010/12/57-pakistani-websites-hacked-by-team.html

in the number of cyber attacks exchanged between them. Although this became a daily affair of the private hackers of both countries, it remained unrecognised and was not considered a threat to national security by either the Indian or Pakistani government. But the spillover effect of this cyber contest soon came into the limelight.

As the various cyber hacking groups in both countries were waiting on a standby mode for an opportunity to sabotage the other in a massive way, the D-Day finally arrived on November 26, 2010, the second anniversary of the 26/11 Mumbai terror attacks. On this day, the members of the Indian Cyber Army (ICA) launched an all out attack on 870[12] Pakistani websites out of which 34 were crucial government websites belonging to the Pakistan Navy, Maritime Security Agency, Foreign Ministry, the Chief Minister of Sind, etc. The ICA spokesperson stated, "Our objective of launching cyber attacks was to pay our homage to the martyrs of 26/11," on the website called Hacker Regiment.

This act of the ICA instigated the hacker groups in Pakistan, and their most powerful group called Pakistan Cyber Army retaliated with a similar all out attack on December 3, 2010, on the 39th anniversary of the 1971 Indo-Pak war by attacking 270 [13] Indian websites of which the worst affected was the website of the Central Bureau of Investigation (CBI) which remained offline for almost one month after the attack before being revoked with great difficulty. The entire software had to be tested and revalidated again before making it available online. It was later identified by the Department of Information Technology that the hackers who attacked the CBI website were based in Peshawar and they had used an Indian Air Force website as a back gate to enter into the CBI website which shared the same database and this became a major security lapse.[14] The hacked CBI website had a message saying:

> This attempt is in response to the Pakistani websites hacked by 'Indian Cyber Army'. We told you before too... we are sleeping but not dead..

12. Sandeep Unnithan, " Inside the Indo Pak Cyber Wars", *India Today*, March 18, 2011.
13. Ibid
14. Khan, n. 6.

> Remember PCA (Pakistan Cyber Army)! back off kids or we will smoke your d00rs off like we did before.. let's see what your investigating agency, so-called CBI can do for you or for us! Haha.. one more attempt from your side.. We got your every website lying around here like its our local server! Buahahaha...so we would like to say to your 31337 hackers and your 31337 NIC team go and read some more books... you guys are seriously bunch of script_kiddies!..you know nothing rite now..got r00t access to NTC server? Wtf mass defacements...how about something like this...a planned attack! Haha...btw we got r00t to your NIC too :P.. Your filtering sucks... have fun! And DO NOT DISTURB... we got better things to do.. :D.. stop complaining about Pakistani websites security.. secure your own ass first..thats what intelligent people do!..lol..tata.:D.[15]

In retaliation, the ICA attacked and defaced the website of the Oil and Natural Gas Regulatory Agency (ONGA)[16], the Pakistani counterpart of the Oil and Natural Gas Commission (ONGC) of India on December 4, 2010. The defaced website of ONGA had the following message: "You Have Been Hacked by the INDIAN CYBER ARMY This Is a Retaliation of Hacking 'CBI."[17]

Pakistani government sources claimed that the attacks on 870 of their websites on November 26, 2010, were planned and executed by India's technical intelligence agency called the National Technical Research Organisation (NTRO) by hiring hackers for their offensive cyber operations which was never proved. Similarly, India also accused Pakistan's ISI for the attack on December 3, 2010, on 270 of its websites and, most importantly, the website of the CBI, which was the most affected. India also claimed that the ISI had recruited hackers for waging a cyber war against India.

These attacks carried out by the Indian and Pakistani hacker groups on each other's cyber networks during the months of November and December 2010, are considered to be among the major cyber attacks that have ever taken place between any two countries of the world without

15. www.cbi.gov.in/index.php, accessed on December 3, 2010.
16. Alam, n. 5.
17. www.Hackerreginet.com

their governments' support. Nevertheless, these attacks are seen only as a prelude to a much bigger contest in the cyber space between India and Pakistan in the future.

However, these attacks carried out by the private hacking groups of both India and Pakistan succeeded in catching the attention of the governments. Immediately after the attacks, a multi-level meeting was called by Mr. Sachin Pilot, India's Minister of State for Communication and Information Technology, from the various agencies like CBI, NTRO and National Informatics Centre (NIC) to discuss the issue[18]. Although the hacking saga faded away after the government's intervention, the hacking groups of both countries now claim to have easier access to the other's cyber networks. "We still own many servers of Pakistan and are prepared to respond to any attack from the PCA or any other Pakistani hacker group," says 'Disfigure' a hacker from the ICA[19].

Although many small cyber skirmishes and cyber attacks took place after the major cyber clash between the hackers of India and Pakistan, they were not considered harmful until the situation became intense again on January 26, 2012, when India geared up to celebrate its 63nd Republic Day. An India-based hacker group called 'Jaguar Hacker' defaced 21 Pakistani websites and posted a message saying: "Nothing Personal But It's Just That Today Is Our Republic Day.. :)).Don't worry nothing has been deleted... Just Index page renamed (*sic*)."[20]

In retaliation to this, the famous hacking group from Pakistan, Z Company Hacking Crew hacked some 400 websites of India and posted:

> You claim to be the largest democracy in the world but when it comes to Kashmir and Kashmiri people, you tend to forget all your democratic principles. You kill our fathers, our brothers, shoot down teenagers point blank and detain them under draconian laws like PSA without even giving them a fair trial, you rape our sisters and mothers. After years of atrocities

18. Unnithan, n. 12.
19. http://www.civilspedia.com/2010/12/indiaica-pakistanpca-cyber-army-warfare.html, as accessed on 13/09/2012, 14:20 pm
20. http://www.mid-day.com/news/2012/jan/280112-Indo-Pak-cyber-war-on-Jan-26.htm

> and oppression we say that we will Rise and Rise Again ... Until Lambs become Lions !!!(*sic*).[21]

WHY DOES THIS MATTER SO MUCH?

The cyber attacks between India and Pakistan (by the various hacking groups of these countries) were not a surprise for the cyber technology management groups as they encounter such activities regularly. According to a report from the Computer Emergency Response Team of India (CERT-IN), it has an account of around 3,600[22] Indian websites that were hacked in the first half of the year 2010, which amounts to approximately 20 hacking instances per day. There are also reports of 774 government websites that have been hacked in the last five years. In spite of all these reports, it is unfortunate to know from many independent cyber security observers in India that despite regular reports of hacking incidents, the government organisations have not been vigilant enough to take the necessary steps to improve any sort of security to the Indian cyber networks. It has been reported after an audit that out of about 7,000 Indian government websites, only 3,192 have been audited for Information Technology (IT) security, while 3,556 others are being audited. Yash Kadakia, head of Security Brigade, a government-empanelled security auditor says,

> According to our data, about half the government websites are vulnerable to cyber attacks. Most of the government websites do not have proper security checks in place.[23]

The same kind of lethargy prevails on the Pakistani side in securing their cyber infrastructures. When asked about the steps taken for management of security to the Pakistani cyber networks, a senior official in the Electronic Government Directorate (EGD), the agency officially responsible for monitoring the hacking saga in Pakistan said,

21. Ibid.
22. "India and Pakistan in Cyber Warfare", *Al Jazeera*, December 4, 2010.
23. Piyali Mandal, "Half the Govt Websites in India are Prone to Cyber Attacks", *Business Standard*, January 6, 2013.

> The government has so far secured only 33 websites belonging to government ministries and departments, out of thousands of official government websites. And there is no system that can't be hacked. You can break any kind of lock, and the same is the case with hacking websites. The government never demonstrates seriousness in dealing with the hacking problem, which poses a constant threat to all state and privately-run websites.[24]

While aggression is the only tactic followed by the hacker groups in both countries, on the contrary, the security providers for the cyber space have always been lacking in vigilance to provide security to their country's cyber networks and infrastructures. Sunil Abraham, Executive Director of the Bangalore-based Centre for Internet and Society, said during an interview to 'Al Jazeera,' "The Indian government has a very low level of cyber awareness and cyber security. We don't take cyber security as seriously as the rest of the world".

The problem of cyber attacks by the hacking groups would not be a big problem if it stopped with the hacking and defacing of websites. But, in reality, it moves on to the next stages. The same people who carry out hacking and website defacing jobs may get involved in cyber espionage and data mining against their enemies. These people may also volunteer their expert services to the terrorist organisations in return for money and other forms of remuneration. According to a cyber security professional working with one of India's intelligence agencies,

> We once sat down to check the Delhi [internet] Backbone. We found thousands of systems compromised. All were government systems, Research and Analysis Wing, Intelligence Bureau, Military Intelligence... we don't realise how much damage has already happened.[25]

24. Khan, n. 6.
25. Pierre Mario Fitter, "Stuxnet Attack Wakes India Up to Threat to Critical Infrastructure", *India Today*, September 5, 2012.

The lack of awareness and the lethargic approach in monitoring and providing security to the cyber networks by India led to thousands of compromised computers across the country. The infection ranges from small Viruses, Botnets[26] to that of Stuxnet[27] level malwares which can hamper the total operations of the network connected to the compromised computer. It has been observed that out of the 10,000 Stuxnet infected Indian computers, 15 were located at critical infrastructure facilities. These included the Gujarat and Haryana Electricity Boards and an ONGC offshore oil rig. Though Stuxnet reached the networks of these infrastructures, thankfully, it did not activate itself on them. In other words, India was only a few flawed lines of code away from having its power and oil sectors crippled.[28]

The list of new malwares goes on – Stuxnet, Flame[29], Duqu[30], etc – and many more are in the process of coding; their abilities to operate as cyber weapons are incredible and, at the same time, unbearable, if not protected against properly. Assuming that the hacker groups get access such malwares, then the situation would become extremely dangerous for the national security as it is equivalent to terrorists getting access to nuclear weapons. While talking about the same, Mr. Sachin Pilot, Minister of State for Communications and Information Technology said:

26. The term bot is short for robot. Criminals distribute malicious software (also known as malware) that can turn your computer into a bot (also known as a zombie). When this occurs, your computer can perform automated tasks over the internet, without you knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a botnet.
27. It is believed that Stuxnet was jointly programmed by the US and Israeli intelligence as part of a project called Olympic Games in order to sabotage Iranian nuclear facilities. It spread from computer to computer, hunting down the exact one that controlled Nantanz's centrifuges and caused big damage to it. It was reported that around 2,000 centrifuges in the Nantanz facility were damaged due to this Stuxnet attack. But a flaw in Stuxnet's code caused it to spread further than planned, infecting more than one lakh other machines worldwide.
28. Fitter, n. 25.
29. Flame is a modular computer malware discovered in 2012 that attacks computers running the Microsoft Windows operating system. The programme is being used for targeted cyber espionage in the Middle Eastern countries.
30. Duqu is a computer worm discovered on September 1, 2011, thought to be related to the Stuxnet worm. The Laboratory of Cryptography and System Security of the Budapest University of Technology and Economics in Hungary discovered the threat, analysed the malware, and wrote a 60-page report naming the threat Duqu. Duqu got its name from the prefix "~DQ" it gives to the names of files it creates.

> The entire economies of some countries have been paralysed by viruses from across the border. We have to make ourselves more resilient. Power, telecom, defence, these areas are on top of our agenda.[31]

A careful study of the series of hacking on one another's websites and networks by the private hacking groups of India and Pakistan would reveal a basic fact that something which started as a small act of hate has now taken on a much different shape in the form of personal revenge, economic profits, a race to show off technical supremacy, and anti-national propaganda.

This was very much evident from one unwanted event that disturbed the internal security of India in August 2012. The Indian government was alerted by the exodus after thousands of people from the northeast gathered at railway stations in various cities all over the country after being threatened by the rounds of SMS and violent morphed pictures that were being circulated on more than 100 websites. The SMS threatened the northeastern people living in various cities in India of a targeted attack on them, asking them to go back to their homeland, whereas the pictures circulated on the internet were images of some violent bloodshed. Out of the various SMS that were in circulation, one said:

> It is a request to everyone to call back their relatives, sons and daughters in Bangalore as soon as possible. Last night, four northeastern guys were killed by Muslims in Bangalore (two Manipuri, two Nepali). Two Nepali girls were kidnapped from Brigade Road. The reports say that from August 20, marking Ramzan, after 2 pm, they are going to attack every north-eastern person. The riot started because of the situation in Assam.[32]

Another SMS said:

> Many northeast students staying in Pune were beaten up by miscreants believed to be Muslims following the Assam riots. Heard that it is happening

31. Ibid.
32. "TRAI Tracking Panic-Spreading SMS"; *The New Indian Express,* August 17, 2012.

> in Muslim areas like Mumbai, Andhra Pradesh, Bangalore. At Neelasandra, two boys were killed and one near passport office.[33]

The Government of India reacted soon on this matter and a 43-page report was prepared by intelligence agencies along with the National Technical Research Organisation (NTRO) and India Computer Emergency Response Team (CERT-IN) which traced several doctored images to Pakistan. The origins of these morphed images were later traced back in specific to Lahore, Rawalpindi and other Pakistani cities by the Indian intelligence agencies. "From all available forensic evidence, we are fairly convinced that all those postings came from Pakistan," said an official of NTRO.

Another senior official who has been involved in India's Pakistan watch for several years said,

> It has been happening for several months now. This is a low cost, very effective way of destabilising us. They don't need to send terrorists and explosives to create mayhem. Internet has been a very effective platform for instigating communal divisions in India. They also have a multiplier effect, first resulting in anger and hatred, then riots and, finally, many taking to terrorism.

This act of unnecessary involvement by Pakistan-based elements is seen as cyber terrorism and cyber psychological warfare against India to cause internal security disturbance and eventually to create a huge crisis in the country. This incident which created major turmoil in the internal security of the country is the biggest example of the adverse effects of wrong use of cyber technology.

WHAT COULD BE DONE?

Any anti-social element, be it an individual or a hacking group, and whatever may be its motive, would certainly need a lot of time to study, analyse

33. Ibid.

There is also a need to increase the number of cyber security experts and IT security auditors, in which the country is facing a crisis at present.

and make the required arrangements in order to penetrate the existing security system. If such elements can spend so much time and effort to plan and carry out an attack, why cannot a country like India, which claims to have a pool of talent in the IT sector, make an attempt to secure its networks and websites with the available talent? This would be possible only when there is political will to address the issue, which India is lacking but the consoling fact is that realisation is now slowly dawning. Also, India's legal system needs to be upgraded towards enhanced cyber laws as its present form is still dwelling on the IT Act 2000, IT Amendment Bill 2006 and IT Amendment Bill 2008 which are unable to cover all forms of the problem in a field which is racing ahead every single day. Finally, there is also a need to increase the number of cyber security experts and IT security auditors, in which the country is facing a crisis at present. Currently, the number of IT security auditors stands at 60 in India.[34] J. Satyanarayana, the Information Technology Secretary of India stated, "We need five lakh professionals to protect our cyber space. We only have a small fraction of this"[35]

For India, it is not only Pakistan that challenges its security in the cyber front but there is always the Red Giant Cyber Dragon – China – above India, which has more a advanced and organised form of cyber army, with which it challenges even the United States through cyber espionage operations like 'Titan Rain'[36]. It is believed that the Chinese cyber warfare policy is based on the 6th century B.C. Chinese strategist Sun Tzu regarding, "the art of fighting without fighting". There have already been instances between India and China where officials in the Indian government have alleged that attacks on Indian government networks, such as that on the Indian National Security Council, have originated in China. According to the Indian government, Chinese hackers are experts in operating Botnets. Fears of Chinese cyber espionage have resulted in the blocking of deals with Chinese telecoms, like

34. Mandal, n. 23.
35. Unnithan, n. 12.
36. Nathan Thornburgh, "Inside the Chinese Hack Attack", *TIME,* August 25, 2005.

Huawei, due to their ties with the Chinese military.[37] India's intelligence agencies have warned about Huawei's penetration into the Indian telecom. Their worst fear is that the Chinese firm could be a Trojan horse, meant to infiltrate India's network in peace-time and disable it through remote 'kill switches' in war-time, through hidden 'trapdoors' and malicious programmes that could then open a channel back to its designers.[38] In 2010, the cyber attacks on the computers of India's National Security Adviser's (NSA's) office, Indian Air Force and Indian Navy are suspected to have originated from China. In each case, it opened up several small windows through which classified documents and presentations were whisked away.

At this juncture, Pakistan's affiliation towards China is an important factor and this affiliation can become deadly for India if they join hands in the future for cyber offensive operations against India. In order to avoid such extreme situations, the Indian government should take quick measures to identify the real people behind these hacking sagas on the Indian side and rehabilitate those who are deserving, and recruit them into its cyber security infrastructures. As most of the hackers are teenagers, this act of converting the 'Black Hat Hackers' into 'White Hat Hackers' would be the right step for the government to get its hands on them and mould them. This will not only give a future to these youngsters but will also create a strong cyber security culture in the country. Also, India is fortunate to have pool of talent in the private IT sector which can be fruitful if used in the proper way. The experts of cyber security in the private sector can be invited to train the government cyber security professionals and can help in conducting security drills from time to time in the government and other cyber networks of the country. Extremely efficient and reliable government cyber security civilian professionals can, in turn, be used to train the defence cyber security personnel so that not only the security of the networks is updated but also it helps in a broader perspective of national interest in the years to come with regard to both national and cyber security.

37. Indrani Bagchi, "China Mounts Cyber Attacks on Indian Sites", *The Times of India*, May 5, 2008.
38. Unnithan, n. 12.

THE AFGHANISTAN REFUGEE CRISIS: IMPLICATIONS FOR PAKISTAN AND IRAN

RHEA ABRAHAM

Migration has been a regular concept in the history of Afghanistan where nomads roamed the land in search of basic necessities, while parents sent their young sons to trading centres for business and employment. Also, internal dislocation among families during conflicts and tribal feuds has been a major cause of migration. At the beginning of the 1960s, rural-urban migration became predominant in and around Afghanistan with the need for development and better living standards forcing locals to migrate internally and externally. Over the years, Pashtuns as the major ethnic group, spread out in large numbers, and other ethnic groups such as the Hazaras crossed into Pakistan for trade and transit. Large scale labour migration of Afghans into Iran also took place regularly, culminating in an exchange of cultural, religious and ethnic migratory routes.

However, post the 1970s, with the Saur Revolution and the subsequent entry of the Soviets into Afghanistan, this seasonal migration soon gave way to the world's largest population displacement, creating a pool of refugees, both inside Afghanistan and on to other neighbouring countries. Post the 2001 US' war on terrorism, these Afghan refugees have been assisted through various programmes to return to their homeland.

Ms **Rhea Abraham** is a Associate Fellow at the Centre for Air Power Studies, New Delhi.

Refugee law as a study remains a separate part of international law that deals with customary law, norms and legal instruments.

However, the prevailing challenges in Afghanistan, the incomplete repatriation procedures, and the unwillingness of the Afghan migrants to return and face an unsteady future, led to massive strain on neighbouring countries like Iran and Pakistan that continue to host a large number of Afghan refugees in their territories.

THE CONCEPT OF MIGRATION

Migration as a social phenomenon in the history of international relations has formed the basic pattern for human evolution and settlement in different parts of the world. The concept, termed as the movement of people from one place to another, caused by the political, social and economic environment, can be categorised mainly as permanent, forced, voluntary or temporary migration. With the onset of globalisation, migration has become an international concern requiring countries to come together and legislate on policies of migration that may directly or indirectly influence their territory and people. A subset of law studies has also emerged encompassing a separate international migration law focussing on intercontinental and interstate migration, including the understanding of refugees. The main elements of international migration law have come to cover several areas such as: the duty of states to accept returning residents, human rights, human trafficking, migrant smuggling, and the obligation to provide consular access to non-residents, and specific areas subject to international agreements such as labour migration.[1] However, international migration law restricts the traditional authority of states and national law on migration.

In this context, refugee law as a study remains a separate part of international law that deals with customary law, norms and legal instruments. The main refugee law under the United Nations Convention on the Status of Refugees (also known as the 1951 Refugees' Convention) defines refugees in the context of international law and defines the rights

1. "International Migration Law", in *Essentials of Migration Management* (International Organisation for Migration: Geneva, Switzerland), http://www.rcmvs.org/documentos/IOM_EMM/v1/V1S06_CM.pdf

of those who are granted asylum by the state. According to the convention, a refugee is defined as,

> A person who, owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable, or, owing to such fear, is unwilling, to avail himself of the protection of that country; or who, not having a nationality and being outside the country of his former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling, to return to it.[2]

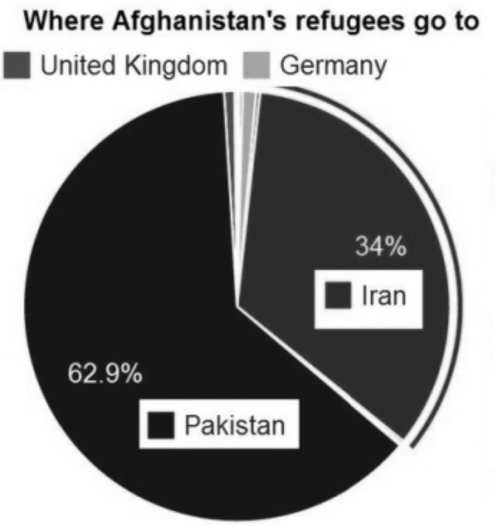
There are 147 signatories to the convention which has been ratified by all under the 1967 protocol. All states privy to the convention need to necessarily abide by it and cooperate with the United Nations High Commissioner for Refugees (UNHCR) in regard to external and internal refugees. The refugees cannot be punished by the states they enter if their life is at stake in their home country. Also, if they are able to provide details to the state authorities, they cannot be imposed with penalties under the refugees' right to be protected against forcible return.

REFUGEES FROM AFGHANISTAN

War has been the greatest enemy for Afghans who have witnessed injustice and instability in the region with the increasing number of conflicts that have been fought on their soil. For years, Afghan refugees have been displaced due to fear of persecution for reasons of race, religion, nationality, armed conflict, and political opinion. In the last ten years, around 5.7 million refugees have been voluntarily repatriated to Afghanistan, mainly assisted by the UNHCR. Despite this, 2.7 million Afghans continue to live in exile in neighbouring countries with the number of refugees returning being recorded low since 2011. [3]

2. "Convention and Protocol Relating to the Status of Refugees", http://www.unhcr.org/3b66c2aa10.html
3. "Afghanistan: What now for Refugees", Asia Report, no.175, August 2009, www.crisisgroup.org/.../asia/...asia/afghanistan/175_afghanistan___what..

Fig 1: Percentage of Afghan Refugees in Host Countries[4]



The first phase of Afghan migration took place soon after the military coup in 1978 against the Daoud government, which was carried out by the Afghan Marxist political group, the People's Democratic Party of Afghanistan (PDPA). With increasing tensions in the region, the Soviet Union, to prevent a political fragmentation in the region, entered Afghanistan in 1979. This presence soon instigated the US and its allies to project the invasion as a threat to the stability of the region and they offered financial and military support to the Afghan fighters, the Mujahideen, to help remove the Soviets from the country. The war in Afghanistan created large scale instability in the region, forcing the Afghans to migrate to neighbouring countries such as Pakistan and Iran. The spread of violence throughout the country, and the recent changes in landownership, social practices and marriage customs along with the changing leadership, forced many to abandon their homeland.[5] The majority of these refugees were Pashtuns who were mainly peasants, farmers, small landowners and clergy,

4. "Where Afghanistan's Refugees go to", http://www.intellectualtakeout.org/library/chart-graph/where-afghanistans-refugees-go
5. Leila Jazayery, "The Migration–Development Nexus: Afghanistan Case Study", *International Migration*, vol. 40, no. 5, pp. 231-254, Special Issue 2, 2002, http://onlinelibrary.wiley.com/doi/10.1111/1468-2435.00218/abstract

who felt that their traditional and cultural existence was being threatened. The second phase of Afghan mass migration occurred simultaneously with the withdrawal of the Soviet troops, beginning in 1986 till 1989. The withdrawal was caused by an increase in the internal power struggle of the Mujahideen groups which, in turn, created two parallel migration movements.[6] With the installation of Najibullah, the United Nations (UN) decided to help out. Repatriation and reconstruction efforts were initiated by the UNHCR through 'Operation Salam' which aimed to create the conditions for the refugees' return, including mine clearance, health programmes, rehabilitation of essential infrastructure and provision of services such as health and education.[7] However, the programme was fraught with financial, logistical, political and security problems, with limited UN access to assistance in Pakistan and Iran. While many Afghan refugees were encouraged to return, others preferred to stay outside due to the growing unrest. These refugees were mainly urban business professionals (Dari-Persian speaking) who were compelled to leave as they were considered to be Communist supporters by the warlords. Many settled in Nasir Bagh Camp in Pakistan's Peshawar province.[8] However, ethnic and linguistic differences between the Pashtun and Dari speaking refugees soon gave rise to tensions in the camps. By 1993, the rate of return declined considerably. The subsequent fight for the control of Kabul and Kandahar resulted in the destruction of the cities and displacement of around 100,000 Kabulis.[9] Many of those who had recently returned to Afghanistan, after 13 years in exile, were once again forced to return to Pakistan or Iran.[10]

The third phase of Afghan mass migration occurred after the Taliban took power in 1996. During the Taliban era, there was support from the Pashtun refugees who decided to return in large numbers, feeling a sense

6. Ibid.
7. Rudiger Schoch, "Afghan Refugees in Pakistan During the 1980s: Cold War Politics and Registration Practice ", UNHCR New Issues in Refugee Research, no. 157, 2008, www.unhcr.org/4868daad2.html.
8. Susanne Schmeidl, "Security Dilemmas: Long-term Implications of the Afghan Refugee Crisis", *Third World Quarterly*, vol. 23, no.1, pp. 7-29, 2002, www.jstor.org/stable/3993574
9. "Afghan Refugees in Pakistan: Push Comes to Shove", Human Rights Commission of Pakistan, April2009,www.humansecuritygateway.com/showRecord.php?RecordId=32538
10. Teresa Poppelwell, " Afghanistan", http://www.forcedmigration.org/research-resources/expert-guides/afghanistan/fmo006.pdf

of security with the coming of the Taliban. However, the introduction of a repressive regime, with political instability and economic challenges, soon led to a drought that created widespread food and water shortages throughout the 1990s. A number of people were compelled to migrate under such circumstances and these were mainly non-Muslim religious minorities and Shia Muslims, who felt threatened under the Wahhabi Taliban regime. As famine and diseases spread, many were forced to migrate to Pakistan and Iran. [11]Also, the taking over of Mazar- e-Sharif by the Taliban in 1996 resulted in a large number of Afghans, mainly Tajiks, fleeing due to the fear of ethnic cleansing by the Taliban. During this period, an estimated 2 million Afghan refugees fled to Pakistan and about 1.5 million were forced to migrate to Iran. Others migrated to other countries in South Asia, West Asia, North America, and Europe. The fourth phase of Afghan mass migration took place with the US global war on terrorism in 2001, which increased socio-economic and political instabilities that generated large outflows of Afghan refugees. By 2001, 900,000 Afghans were internally displaced due to intense fighting in the region.[12] It is interesting to note that even after the ousting of the Taliban in 2001, not too many refugees returned to Afghanistan. However, the tripartite agreement signed among the Pakistan, Afghanistan and UNHCR and similarly with Iran in 2002, facilitated the return of around 1.5 million refugees to Afghanistan.[13]

Table 1: UN Index for Afghan Refugees in Iran and Pakistan[14]

Type	Country	Total
Unregistered Afghans	Iran	1.4 million
	Pakistan	1 million
Registered Afghans	Iran	1 million
	Pakistan	1.9 million

11. S. G. Khattak, "Insecurity: Afghan Refugees and Politics in Pakistan", *Critical Asian Studies*, vol. 35, 2003, pp. 195–208, criticalasianstudies.org/issues/vol35/no2/in-security.html
12. http://afghanistan101.blogspot.in/2012_07_01_archive.html
13. n. 11.
14. "2013 UNHCR Country Operations Profile – Afghanistan", http://www.unhcr.org/cgi-bin/texis/vtx/page?page=49e486eb6&submit=GO

AFGHAN REFUGEES IN PAKISTAN

The vast majority of Afghan families in Pakistan arrived in the first years of the refugee crisis. Also, due to traditional migratory routes, a number of Afghans who were present in the Northwest Frontier Province (NWFP) in Pakistan were second and third generation Afghan migrants.[15] The Afghan refugees in Pakistan, mainly from southern and eastern Afghanistan, comprised Sunni Pashtuns (82 percent) who found it easier to migrate to places that were housing other Pashtun ethnic communities while other ethnic groups such as Sunni Tajiks (8 percent), Shia Hazaras (2 percent) and Sunni Balochis (1.7 percent) migrated in small numbers.

History

Afghan refugees came to Pakistan in various phases, starting with the Panjshir revolt in 1979, when a large number of Afghan dissidents, mainly Tajiks and Hazaras, who were opposed to Prime Minister Daoud's policies, fled to Pakistan.[16] The second was the arrival of Afghan refugees with the onset of the Soviet invasion into Afghanistan. Around 100,000 refugees, mainly from the eastern regions of Afghanistan like Konar, Paktia and Nangarhar, entered Pakistan.[17] As resistance against the Communist regime of Babrak Karmal started to increase, most people fled to Pakistan where relief operations were being initiated in 1979. A cash allowance was provided to a limited number of registered refugees by Pakistan, but employment as a choice of the refugees themselves was restricted.[18]

The migrating Pashtun refugees preferred Peshawar as they could easily enter the local markets and also obtain Pakistani identity cards and, therefore, they settled in parts of the Federally Administered Tribal Areas

15. "Afghan Refugees: Current Status and Future Prospects", CRS Report for Congress, January 2007, www.fas.org/sgp/crs/row/RL33851.pdf
16. "Afghan Refugees", Refugee Studies Programme, March 1989, repository.forcedmigration.org/pdf/?pid=fmo:5680
17. Anthony H. Cordesman, "The Afghanistan/Pakistan War at the End of 2011", CSIS Report, 2011, csis.org/publication/afghanistan-pakistan-war-ahe-end-2011
18. n. 16

Afghan refugees who were willingly to fight against the Soviets were provided arms, training and financial support by Pakistan.

(FATA), Balochistan and NWFP.[19] In Quetta, they were, however, put under tribal security. On the other hand, the Hazara refugees took sanctuary under the Hazara leaders in Quetta and a number of Ismaili refugees went to Karachi. The invasion of the Soviets in 1979 and the subsequent entry of refugees into Pakistan provided legitimacy to Pakistan under Gen Zia-ul Haq to intervene in the regional security related decision-making. Although Pakistan did not sign the Geneva Convention or any other international convention related to refugees, it clearly recognised the Afghans as refugees, a move that was not entirely based on humanitarian reasons. Rather, the Pakistan government's decision was a move to gain international military, economic, and diplomatic status. Most importantly, those Afghan refugees who were willingly to fight against the Soviets were provided arms, training and financial support by Pakistan, which was further facilitated by the United States and other Muslim countries like Saudi Arabia.

Initially, the Afghan refugees could register as refugees only if they resided in the NWFP and Balochistan province. Registration provided the Afghan refugees access to basic necessities and material aid.[20] In the beginning, the Pakistan government tried to contain the refugee population in areas where there was cultural affinity between the Afghans and the Pakistani Pashtun population. However, as mentioned earlier, the presence of the other ethnic migrants such as the Hazaras, Tajiks, and Uzbeks fuelled the ethnic divide with the people of the NWFP and Balochistan. Most refugees were employed in construction sites by private companies and Afghans who went abroad from Kabul sent remittances to their families in Pakistan. Afghans opened restaurants in Peshawar and Quetta, as Afghan cuisine and carpets became famous.

19. " Afghans in Pakistan: Broadening the Focus", Briefing Paper of the Afghanistan Research and Evaluation Unit, Collective for Social Science Research, January 2006, www.areu.org.af/.../602E-Broadening%20the%20Focus-BP-web.pdf
20. n. 11

Through education and intermarriages, a large number of Afghans learned Urdu.

After the Soviet withdrawal in 1989, a large number of refugees tried to return to Afghanistan. However the attempt failed in 1992, with the ongoing conflicts between the Mujahideen, mainly the Hizb-e-Islami, Jamiat-e-Islami, and Hizb-e-Wahdat, destabilising the region of Kabul.[21] The Government of Pakistan also played covertly into the situation by fuelling the conflict through the supply of arms and money. By the time the Taliban took control of Afghanistan in 1996, there was a rapid decline in the international aid to Afghanistan and the food shortage forced many to once again flee the country into Pakistan. With the increasing flow of refugees, after 2001, the Pakistan government decided to close its border with Afghanistan and refused to admit new Afghan refugees. In 2002, the Pakistan government closed a number of camps in the NWFP, including Nasir Bagh, Jalozai, and Kacha Gahri, and also issued eviction orders to the residents in these camps.[22] In 2004, other camps in South Waziristan were closed and in 2005, the remaining camps in FATA and two camps in Balochistan were also closed. The closure of these camps effectively displaced many Afghan refugees and also led to violence between the Pakistani officials and Afghans in the region.

Status of Refugees

As a part of the migration, the Afghan refugees in Pakistan resided in settlements or compounded areas called 'villages' which were easier for administration and identification, and provided the refugees with basic amenities.[23] The refugees were not allowed to buy land and property or get involved in Pakistani politics but were allowed to form their own political organisations. Relief operations that took place during the early periods were government funded, managed and amended in 1984 to

21. Shah Mohmand, " The Saga of Afghan Refugees in Pakistan", MEI-FRS, February 2010, www.refugeecooperation.org/publications/Afghanistan/06_mohmand.php
22. "Closed Door policy: Afghan Refugees in Pakistan and Iran", *Human Rights Watch*, vol. 14, no. 2, February 2002, www.hrw.org/reports/2002/pakistan/
23. n. 19

By 2006, more than 2.8 million Afghan refugees had returned from Pakistan, under a UNHCR-assisted voluntary repatriation programme.

introduce self-reliance activities for the refugees.[24] Separate organisations called 'commissionerates' were established in Peshawar and Quetta to administer the refugees assistance, including registration, settlement in camps and provision of basic amenities. These were further organised into six departments: health, relief, registrar, security, budget and finance.[25] International agencies such as the UNHCR and the World Food Programme were instrumental in organising the refugees in Pakistan. It is interesting to note that many of the Afghan refugees who settled in Pakistan had social networks, kinship and economic contacts existent in the country, which helped ease their transition further. A large majority of refugees was employed as casual wage labourers and the refugees in Karachi largely engaged in business and trade. The refugees were largely dependent on aid money to supplement their low incomes due to their incomplete primary education. Even today, Afghan refugees in Pakistan do not have access to formal employment and a large proportion is made up of children and youth, under the age of 18 (around 1.7 million).

In 2006, the Pakistani government began a registration campaign through which around one million Afghans were registered and provided with official identification (Proof of Registration cards) which would enable them to remain in Pakistan for an initial period of three years, which was, however, extended till 2012.[26] The UNHCR and Pakistan agreed in 2009, to allow around 1.7 million refugees to reside in Pakistan. By 2006, more than 2.8 million Afghan refugees had returned from Pakistan, under a UNHCR-assisted voluntary repatriation programme. Unfortunately, with increasing security threats in Pakistan including unemployment and poverty, the validation of refugee identification is to end by July 2013, when the right

24. n. 16
25. n. 21
26. "Midnight Deadline Looms for Afghan Refugees", *The Newcastle Herald*, June 18, 2013, http://www.theherald.com.au/story/1580159/midnight-deadline-looms-for-afghan-refugees/?cs=5

of all Afghan refugees to live in Pakistan will be taken away and forcible deportation will be conducted by the Pakistani officials.

Security

It has been understood that the influx of Afghan refugees into Pakistan has increased the pollution and traffic in the country. Refugees have also replaced locals for lower wages and thereby affecting the employment rates in the country. After 9/11, the attitude of the locals towards the Afghan refugees changed considerably as they wanted the Afghans to return to their homeland due to decreasing living spaces. The refugee camps have also been termed as safe havens for terrorist recruitment, training and accommodation and thereby, the protection by Pakistani officials has decreased with random interrogation forcing the refugees to return on a large scale. The Taliban have been able to easily penetrate the Pashtun dominated camps and blend in with the refugees, making any detection by officials difficult. Most importantly, information on refugees in the FATA region is restricted mainly as UNHCR officials are not allowed into these tribal zones, which poses a problem for the complete repatriation of the Afghan refugees. However, as part of the ongoing repatriation from Pakistan, mainly with the expiry of the Proof of Registration cards, returnees are being given repatriation assistance of $117 per person, as well as a travel allowance of between $10 and $40.[27] Around 89,000 refugees returned to Afghanistan from Pakistan last year due to the strict measures.

Also, with the overall level of international funding for refugees having decreased, the economic burden on Pakistan has increased significantly. The government has claimed that the country does not have adequate infrastructure to support the remaining Afghan refugees and also prevent any further infiltration of terrorism and non-state actors into Pakistan. In 2006, the Pakistani government closed 32 camps as they were represented as a risk to its national security. The refugees were forced to move to alternative camps or to return to Afghanistan, with a number of camps being closed in Balochistan, despite increasing protests.

27. n. 23.

AFGHAN REFUGEES IN IRAN

Thirty years of war in Afghanistan has left Iran with a large urban refugee population in the world. More are than 1 million Afghans are registered as refugees in Iran, which is also home to another 1.5 million illegal Afghan migrants.[28] More than 1.6 million Afghans have returned from Iran since April 2002, but the pace reduced significantly in 2006, with only around 5,000 returning due to lack of a better standard of living in Afghanistan.[29] In 2007, with increasing security threats in the region, Iran forced the Afghans to go back to Afghanistan, separating many families and raising concerns of a humanitarian crisis which came under criticism by the UNHCR. Furthermore, Iran has been forcibly repatriating illegal immigrants, which is also a cause of concern for many refugees in the current context.

History

During the Soviet invasion of 1979, thousands of Afghans fled to Iran with its open door policy of championing Islamic brotherhood, which, however, denied the refugees dignified work and initially termed them as violent criminals and drug dealers. During the 1990s, under President Akbar Hashemi Rafsanjani, the government sought to naturalise them.[30] Since then, the Afghan refugees, termed as 'involuntary religious' migrants (Mohajerin), have lived among the locals, and have been permitted to work in the Iranian labour market, primarily in the construction, agricultural and general manual sectors. It is to be noted that even prior to the Soviet invasion, it was a tradition in many regions of Afghanistan to send young villagers to Iran as migrant workers from remote areas such as Afghanistan's central highlands comprising the Bamian and Daikundi provinces.

Afghans share a common language (Persian speakers) and a similar culture with the Iranians, and, hence, have more easily integrated into

28. "2013 UNHCR Country Operations Profile - Islamic Republic of Iran", http://www.unhcr.org/cgi-bin/texis/vtx/page?page=49e486f96&submit=GO
29. Mohammad Jalal Abbasi-Shavazi et al, "Return to Afghanistan? A Study of Afghans Living in Mashhad", AREU, 2005, http://www.areu.org.af/Uploads/EditionPdfs/527E-Afghans%20Living%20in%20Mashad-CS-web.pdf
30. Bruce Koepke, "The Situation of Afghans in the Islamic Republic of Iran Nine Years After the Overthrow of the Taliban Regime in Afghanistan", MEI-FRS, February 2011, www.refugeecooperation.org/publications/Afghanistan/03_koepke.php

the Iranian society. The ethnic and sectarian composition of Iran's Afghan refugee population is diverse and includes the majority (40.47 percent) ethnic Shia Hazaras, 22.07 percent Sunni Tajiks, 8.8 percent Sunni Pashtuns, 3.1 percent Sunni Balochis, and 2.5 percent Sunni Uzbeks. Over the years, Iran has sought to integrate the Afghan refugees into the society. They were given permission to work in designated occupations, provided access to free health, education and food subsidies. However, the state did not provide assistance for housing, thereby forcing the refugees to congregate together, creating spontaneous settlements along the border between Iran and Afghanistan, close to Herat's urban areas.[31] These Afghan colonies were located in geographical areas that have a high demand for manual labour, particularly in the fields of agriculture, construction, brick-making, and stone-cutting. Also, around 25,000 Afghans have been accommodated in refugee camps.[32] Iran's Afghan refugee population comprises mainly Pashtuns from the neighbouring province of Farah in western Afghanistan, who adhere to conservative social and cultural practices similar to those of the host country. Therefore, the decision to repatriate depends primarily on the initiative of their tribal leaders.

Status of Refugees

Under the Iranian Refugee Proceedings, an individual is recognised as a refugee if he is: (1) crossing the border into Iranian soil; (2) a foreign national submitting a request to receive refugee status from Iran and enter Iranian soil; (3) a foreign national residing inside Iran submitting a request for receiving refugee status. Further, for the request to be processed by the refugee committee, the requesting party must have the following qualifications: (a) should be subject to one of the reasons prescribed in Article 1 of the Convention Relating to the Status of the Refugee and have a clean background; (b) should have not committed war crimes, or crimes against humanity or severe violation of public rights; (c) should have gone through the proper process of becoming a refugee; (d) should give a guarantee to

31. n. 10.
32. n. 34.

Iran is now host to second and third generation Afghans who speak authentic Farsi dialects.

abide by internal Iranian laws for the duration of his/her residency in Iran. Upon issuance of the refugee status by the refugee committee, the individual is also issued a refugee card and prescribed a place of residence.

While consistently cooperating with the UNHCR, the Iranian government has preferred to manage its refugee population via its Ministry of Interior's Bureau of Aliens and Foreign Immigrants Affairs (BAFIA), together with some government-approved non-governmental organisations and minimal international support or interference. Over the last decade, the Iranian government has regularly registered its refugee population. An initial identification and registration exercise of the refugees was carried out in 2000, followed by frequent registration exercises in 2003, known as Amayesh. This process of sequential registrations has enabled BAFIA to provide refugees with adequate assistance and to monitor emerging trends, including the growth rate of the Afghan refugee population. Renewable registration cards are issued by BAFIA once an Afghan refugee re-registers and pays the necessary registration fees and municipality taxes.

With more than three decades having elapsed, Iran is now host to second and third generation Afghans who speak authentic Farsi dialects. The Iranian government estimates that the Afghans living in Tehran in large numbers are primarily single men originating from areas in Afghanistan with high unemployment. While most come to Iran for a short stay of one to two years, many travel between the two countries over longer periods of time. Iran continues to provide educational opportunities to Afghan refugee students up to pre-university level. Until 2005, Afghan refugees had the option to enrol in either Iranian schools or in Afghan-run private schools, which also admitted undocumented Afghans. While not approved by the Iranian government, these Afghan-run schools were registered with the Afghan Embassy in Tehran. However, following a decree issued by President Mahmud Ahmadinejad in 2009, all Afghan children, including undocumented Afghans, have been permitted to enrol in Iranian schools

once their family has registered with BAFIA and paid the school fees. According to the Iranian government, since this decree, 60,000 undocumented Afghan children have availed of this opportunity to attend school. In addition to these pre-university students, Afghan theology students are also studying in Iran.

The majority of refugees in Iran are concentrated in urban areas around the country and only around 5 per cent live in camps.

The voluntary repatriation programme which began in 2002, under the tripartite agreement facilitated the return of refugees from Iran. Some received assistance, which included transportation to the border, small cash grants and assistance packages, while others returned unassisted.[33] In addition to UNHCR-assisted voluntary repatriations of refugees, undocumented Afghans are allowed to return spontaneously to Afghanistan each year. By applying for an exit *Laissez-Passer* from the Afghan Embassy or Consulate in Mashad, undocumented Afghans have the opportunity to return to Afghanistan, via self-funded transport to the Afghan border, without being penalised by Iran's disciplinary forces. According to the Afghan Embassy in Tehran, on average between 600 and 1,000 single Afghans apply for a *Laissez-Passer* every day.[34]

Unlike in Pakistan, where many Afghans live in refugee camps, the majority of refugees in Iran are concentrated in urban areas around the country and only around 5 per cent live in camps. However, in the current scenario, Iran's worsening economic crisis and government policies have prompted a number of Afghans to return home or migrate further to Turkey and Greece.

Challenges to Security

With the mass inflow post 2001 seeming to threaten internal stability, the Iranian government announced residential restrictions, including in those provinces where Afghan nationals were living in large numbers. This meant that those who had been living in a place for years had to relocate to another

33. Ritendra Tamang "Afghan Forced Migration: Reaffirmation,Redefinition, and the Politics of Aid", *Asian Social Science,* vol. 5, no. 1, January, 2009
34. Abbasi-Shavazi et al, n. 29.

approved location. Fourteen provinces of Iran, including the provinces of Lorestan, East Azerbaijan, North Khorasan, Sistan and Balochistan, Western Azerbaijan, and Kurdistan as well as the islands of Kish, Gheshm and Abu Musa, have been designated as off limits for the Afghans with restrictions on other cities approved for Afghan residency. Even along Iran's major border with Afghanistan in the province of Sistan and Balochistan, trespassing Afghans are arrested. Furthermore, many of the restrictions, such as in Yazd, Fars and Isfahan province, create employment problems for the Afghans, as well as for the agriculture sector in which they are employed.

The illegal presence of Afghans in Iran places an additional financial burden on the Iranian government. It has been estimated that every Afghan living in Iran, whether a refugee or an illegal migrant worker, costs the Iranian government a minimum of two dollars a day.[35] In addition, the Iranian government claims that illegal Afghans pose threats to its national security, especially by becoming victims to insurgents and narco-traffickers near the Afghan border.

Many Afghans who cross the Afghan border illegally attempt to evade Iran's disciplinary forces by using the services of human smugglers. In this regard, the Iranian government has been trying to regularise the entry of Afghan workers and provide them work and labour permits. The BAFIA has stepped up random inspections of building firms and factories, threatening to shut down those that employ undocumented workers. The government also announced that marriages between illegal migrants and Iranians would not be recognised and illegal immigrants would not qualify for refugee status. Children of an illegal immigrant thereby have no legal status, barring them from education and health care.[36] Iranian law prevents Afghan nationals who do not have a valid passport, visa and work permit from holding governmental jobs, buying or selling land, enjoying socialised governmental health care, opening a bank account, registering a cell phone, or any other activity that requires official registration. Afghans without an

35. n. 30.

36. "Go Back Home: As Iran's Economy Slides, Afghan Refugees are Being Penalised", *The Economist*, February 16, 2013, http://www.economist.com/news/middle-east-and-africa/21571935-irans-economy-slides-afghan-refugees-are-being-penalised-go-back-home

Iranian citizenship, even those who fled to Iran 30 years ago, including children born to Afghan families inside of Iran, are still considered foreign nationals and do not enjoy any citizenship rights. Ironically, a large number of the workforce comprises Afghan migrants who, due to their low wages, are allowed to work but, on the other hand, due to their inability to follow up on their legal rights, are simultaneously abused by the Iranian construction managers.[37]

CONCLUSION

The Afghan refugee crisis has been one of the largest humanitarian interventions in the world. The UNHCR has been extremely instrumental in the assistance, refuge and repatriation of Afghan refugees in Iran and Pakistan, mainly through administered refugee camps. Over the years, funds from other countries have been collected by the UNHCR to the tune of $1,000 for the cost of each repatriation. During the civil wars in Afghanistan, around 234,000 refugees took asylum in different parts of the world, including Germany, Austria, Netherlands and Denmark. Also, the refugees preferred to migrate either to Iran or Pakistan based on ethnicity, religious sect and political affiliation as a major factor. The 2011 industrialised country asylum data noted that there was a 30 percent increase in applications from Afghans from 2010 to 2011, primarily towards Germany and Turkey, reflecting the unwillingness of the Afghan refugees to return and the eagerness of those still residing there to continue to do so.[38]

A number of reasons underlie the limited repatriation of Afghan refugees to their homeland. These can be understood as the following:

- Many Afghans have no land to return to in Afghanistan. While assistance is available from the Afghan government for eligible landless Afghans, these transfers would require legal assistance to clarify complex land titles.
- There are only few employment opportunities for the returnees in Afghanistan, restricted mainly to rural areas such as agriculture.
- The deteriorating security environment in Afghanistan does not

37. "Iran: An Afghan Free Zone?", Justice for Iran, June 2012, http://justiceforiran.org/wp-content/uploads/2012/06/Iran-anAfghanFreeZone-layout-Final.pdf
38. "Afghan Refugees", http://costsofwar.org/article/afghan-refugees

encourage sustainable repatriation, with an increasing number of mines in, and flow of armaments into, the country.

- Living conditions in Iran and Pakistan continue to be considerably better, with access to basic health care, education, employment and affordable housing in a secure environment.
- There are human rights violations, ethnic rivalries, low basic health care and malnourishment in the country with economic vulnerability and insecurity. Also, assistance is provided predominantly in Kabul and other main cities, with few activities in the rural areas.

The Afghan government's slow process of allocating land to migrants has certainly been a key factor in discouraging refugees from returning. In the case of Afghan refugees in Iran, factors such as the acculturation of the refugees to an Iranian lifestyle, with many of the benefits of an advanced modern society, and the complexity of political, ethnic, tribal, and sectarian adherence in Afghanistan have made the repatriation process redundant. For many, the idea of returning to rural areas in Afghanistan which offer extremely basic infrastructure, social services and employment opportunities, is difficult. In addition, Iranian-educated graduates are frequently exposed to varying degrees of prejudice upon their return to Afghanistan and thereby many younger Afghans prefer to remain in Iran primarily for its greater economic opportunities. However, attempts to encourage Afghan university graduates to voluntarily repatriate are being introduced such as the IOM (International Organisation for Migration) programme, funded by the Japanese government, which is aimed at facilitating the return of more than 100 skilled Afghans from Iran to Afghanistan's public and private sectors.

With instability continuing in Afghanistan, the migration of Afghan refugees to towns and cities in Pakistan and Iran remains a major issue for the stability and security of the region and the host countries. In the current context, land disputes between locals and migrants could lead to future conflicts in the region; and there has been a rise in poverty, population, unemployment and criminality among the neighbours, and other developmental challenges. Unchecked cross-border activities continue to

increase fears of non-distinction between insurgents and migrants, thereby giving more leverage to Pakistan and Iran to intervene, leading to massive informal repatriation. Also, the refugees have become political tools in the hands of both Iran and Pakistan and are being used by both countries to negotiate political, social and economic benefits with regard to Afghanistan and the international security environment. For example, in 2007, the Iranian government enforced a mass deportation of undocumented Afghans through its disciplinary forces because of the lack of any security measures imposed by the Afghan government on the joint border. This sudden influx of a large number of deported Afghans not only strained the capacity of the Afghan Ministry of Refugees and Repatriation, but had political repercussions, with the Afghan Parliament issuing a vote of no-confidence against the Ministers of Refugees and Repatriation and Foreign Affairs.

Secondly, it is important to note that the limitation in the definition of refugees by the UNHCR and other state bodies has been creating issues for the legality of the rights of the Afghan refugees and their existence in the host country, mainly due to the differences in approach.[39] This, in turn, has allowed exploitation of the illegal migrants or undocumented refugees and forced repatriation by the state bodies, which continues to remain an issue of threat in the region. Also, the migrants who are not repatriated properly under legal jurisdiction are liable to become victims at the hands of drug and arms cartels through smuggling, trafficking and consumption, thereby adding to the instability in the region. Also, Pakistan being a non-signatory to the 1951 convention, is a major obstacle in finding a sustainable solution to the refugee problem from Afghanistan. Afghan refugees in Pakistan, prior to being officially registered, have complained of extortion and detention by official forces as there is no provision or law under the Pakistani Constitution for the protection of refugees and, therefore, even their movements are heavily curtailed or monitored.

In view of the complexity of the crisis and the challenge to the stability of the region, an international conference in Geneva in May 2012 brought

39. Personal interaction with Harsheth Virk, Regional Adviser (HIV/AIDS),UNODC on June 19, 2013.

Keeping in mind the economic insecurities of the Afghan refugees in India to find jobs, long-term visas are being issued since June 2012 to help them find formal employment in the host country.

Afghanistan, Iran and Pakistan under the auspices of the UNHCR to endorse a Solutions Strategy for Afghan Refugees, which aimed to pursue voluntary repatriation, sustainable reintegration and assistance to host countries. As for India, the issue of the Afghan refugees remains a less likely threat because of the low number of refugees in India (around 25,000) who have come to the country for educational, economic and medical facilities and have, in turn, taken back a large contribution to their home country. Also, keeping in mind the economic insecurities of the Afghan refugees in India to find jobs, long-term visas are being issued since June 2012 to help them find formal employment in the host country. However, with the withdrawal of the US forces in 2014 and the changing regional dynamics, there is a possibility of complete instability in Afghanistan and an even bigger influx of refugees into countries of South Asia, including India. To control any future crisis, countries like India need to engage regionally with all the weaker sections of Afghan society, mainly the refugees and the internally displaced persons. Most importantly, India should lead the initiative and help countries like Iran to have a clear policy and implementation programme for asylum seekers and refugees, in order to engage them economically and prepare for a crisis situation in the region.

RESEARCH FELLOWSHIPS – 2014-2016

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 1,000 words must be sent to **Director, Centre for Air Power Studies, P-284, Arjan Path, Subroto Park, New Delhi-110 010** not later than **March 31, 2014** 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 electronically, 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.

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	Overseas
☐ Rs. 275/- per copy	☐ US $ 35 per copy
☐ Rs. 1100/- per annum (4 Issues)	☐ 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 t**o: KW Publishers Pvt. Ltd., 4676/21, Ansari Road, Daryaganj New Delhi 110 002 T: +91.11.23263498 / 43528107 E: knowledgeworld@vsnl.net W: www.kwpub.com**

AIR POWER Journal

SUBSCRIPTION FORM

In India	Overseas
☐ Rs. 275/- per copy	☐ US $ 35 per copy
☐ Rs. 1100/- per annum (4 Issues)	☐ 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 t**o: KW Publishers Pvt. Ltd., 4676/21, Ansari Road, Daryaganj New Delhi 110 002 T: +91.11.23263498 / 43528107 E: knowledgeworld@vsnl.net W: www.kwpub.com**