COLLUSIVE AND HYBRID THREATS

On October 18, 2014, the Prime Minister Modi in the Combined Commanders' Conference said, *"Beyond the immediate, we are facing a future where security challenges will be less predictable; situations will evolve and change swiftly; and, technological changes will make responses more difficult to keep pace with. The threats may be known, but the enemy may be invisible. Domination of cyberspace will become increasingly important. Control of space may become as critical as that of land, air and sea. Full scale wars may become rare, but force will remain an instrument of deterrence and influencing behaviour, and the duration of conflicts will be shorter."*[1] This clear and categorical direction emanating from the Prime Minister himself, is indicative of future threats and challenges to national security. The security challenges for the nation can no longer be defined and definite, as these are likely to be hybrid, conducted in many battle spaces by multiple means driven by a collective ideology , plausibly without any direct attribution and without any physical military application of combat power ab-initio.

India's national aim is to " Transform India to a modern, prosperous and secure nation." India is a responsible, rising nation with regional and global aspirations. The largest democracy of the world, the second largest population at over 1.25 billion people, the fourth largest armed forces and the fourth largest economy are some of the many contributors to a comprehensive national power. However, India does have the longest disputed borders with it's neighbors, a continuing proxy war waged by Pakistan for over a quarter century now, insurgencies in the North East, though mostly sub-critical and an internal security Naxal problem in the hinterland. The region is also home to three of the world's nuclear armed nations.

1

The Afghanistan-Pakistan (AF-PAK) region and the middle East with ISIS domination are the two fault lines that directly impact the security of our nation. Given the multiplicity of threats to our national security across all domains, it is essential that a pragmatic assessment and continuous review of the threat be carried out to enable capability development and capacity enhancement to meet future security challenges.

The key question is “What is a hybrid threat?” Some strategic thinkers and military minds, believe that the threats remain constant and only acronyms and words have changed, that too merely an adaption of American concepts of warfighting. Under Grounds (UGs) to Insurgents to militants to anti-national elements (ANEs) and now to terrorists are the definitions assigned to groups and individuals who have taken up arms against the nation state in the sub-conventional domain in our context over the years. Nuclear war, conventional, limited and localised wars, irregular warfare, 4G wars and small wars, asymmetric warfare and proxy wars are real and present threats. In addition there is non contact warfare to include cyber, informational and the space domain. Does the hybrid threat encompass all or some of these warfare's in time and space? What are the similarities and differences in the methodology of both waging such warfares and seeking effective counter-warfare strategy to this multi-faceted and multidimensional threat. It is important to have a common understanding of the hybrid threat especially so in the Indian context to meet future challenges to India’s national security.

Though hybrid threats in some form or another have persisted in military history but the Israeli-Hezbollah War of 2006 demonstrated that the sophistication and lethality of non-state actors, along with their ability to persist within the modern state system, is a new occurrence. Hezbollah’s defiant resistance against the Israeli Defense Force in the summer of 2006 may be a classic example of a hybrid threat. The fusion of militia units,

specially trained fighters and the anti-tank guided-missile teams marks this case, as does Hezbollah's employment of modern information operations, signals intelligence, operational and tactical rockets, armed UAVs and deadly anti-ship cruise missiles. Hezbollah's leaders describe their forces as a cross between an army and a guerrilla force, and believe they have developed a new model.20

The Israel Defense Forces were stunned by Hezbollah's advanced battlefield tactics and weaponry, including the successful use of an advanced ground-to-ship missile and anti-tank weapons. The Israeli experience in Lebanon has become a textbook case of the kind of hybrid warfare that many defense analysts believe will be a defining feature of the future security environment.2

--Michèle A. Flournoy (U.S. Under Secretary of Defense for Policy) and Shawn Brimley

Conflict in Ukraine, Iraq and Syria during 2014 hasalso put renewed focus on so-called 'hybrid warfare', in which combatants employ a mix of military and non-military tactics to achieve their objectives. The mix of tactics employed by Russia in Ukraine, and by the Islamic State of Iraq and al-Sham (ISIS) in Iraq and Syria, has left the world uncertain as to how best to respond. While the methods used in the two theatres are by no means the same, both involve the simultaneous use of military and civil instruments, covert operations, information warfare and social media.

COUNTERING HYBRID THREATS: CHALLENGES FOR THE WEST

by Fortuna's Corner

November 23, 2014

In the backdrop of these present day conflicts which force strategic thinkers to foresee the likely shape and intensity of future wars, it is pertinent to try and define the Hybrid threat.

Hybrid warfare (HW) has many definitions. The more relevant to the Indian context are

Hybrid warfare is a military strategy that blends conventional warfare, irregular warfare and cyberwarfare. In addition, hybrid warfare is used to describe attacks by nuclear, biological and chemical weapons, improvised explosive devices and information warfare. This approach to conflicts is a potent, complex variation of warfare. By combining kinetic operations with subversive efforts, the aggressor intends to avoid attribution or retribution. Hybrid warfare can be used to describe the flexible and complex dynamics of the battlespace requiring a highly adaptable and resilient response. http://en.wikipedia.org/wiki/Hybrid_warfare

Robert M. Gates, U.S. Secretary of Defense simply defines hybrid warfare as “The categories of warfare are blurring and no longer fit into neat, tidy boxes. One can expect to see more tools and tactics of destruction -- from the sophisticated to the simple -- being employed simultaneously in hybrid and more complex forms of warfare.”

- Frank Hoffman article

In the Indian context, in addition to the hybrid threat, there looms the ever present danger of a collusive and/or collaborative threat from Pakistan and China. It is the application and exploitation of this threat by known adversaries which needs to be factored in a counter-strategy, and to enhance capacities and build capabilities.

Gen V P Malik former COAS of the Indian Army while delivering the 30 USI National Security Lecture on the Grand Design between China and Pakistan stated *"The possibility of a concerted twin strike in a grand design by China and Pakistan has very serious implications for India: nuclear, aerospace and maritime dimensions. It may also involve Bhutan, Nepal and Bangladesh. Such a venture would hurt China's global image severely. India would have diplomatic support of almost the entire world. This, to my mind, is the least likely manifestation. However, if it does occur, India could initially hold China in the North, and turn its attention and weight towards Pakistan. This probability will serve as a deterrent to the Pakistani participation. As India would be the main sufferer, it could legitimately hurt maritime interests of China and Pakistan in the Indian Ocean and even rescind its No First Use (NFU) of the nuclear doctrine to send warning signals to both countries."* In all these manifestations, China-Pakistan military collusion in the Karakoram Pass region can be considered as the most likely scenario. A similar theory though in much greater detail has been propagated by Pravin Sawhney in the cover story of the April issue of FORCE magazine. A collaborative threat by Pakistan and China though may seem farfetched but is plausible especially so if there is a perceived threat to the China - Pakistan Economic corridor (CPEC), as it passes through disputed territories.

30th USI National Security Lecture
A Comprehensive Response Strategy to a Collusive and Collaborative Threat from China and Pakistan*

The construct of a hybrid and collusive threat in the Indian security context is based on a few key certainties as under:-

- A more vigorous proxy war by Pakistan in Kashmir.
- Multiple and simultaneous attack on soft target major cities and/or religious places orchestrated by Pakistan based terrorist outfits.
- With the US drawdown from Afghanistan, India should be prepared for a shift in Pakistani controlled terrorist organizations from Afghanistan to J&K.
- Pakistan's pushing drugs into Punjab, is part of the plan and a considered hybrid threat
- A collusive or collaborative threat from both China and Pakistan. This is open to argument as China mindful of its national and economic interests is not likely to overtly either support or collaborate with Pakistan. However, in the event of the China threat, Pakistan will only be too willing to support it's all weather friend China and a collaborative threat from Pakistan would be imminent, as it takes on a mightier India preoccupied with China along the Northern Borders.
- A perceived threat by China to China-Pakistan economic corridor (CPEC)/ Karakoram highway (KKH) would lead to a collaborative threat from China and Pakistan. The plausibility of this collaborative threat to the disputed Siachen glacier and Aksai Chin is much more as it provides strategic depth to the CPEC. The CPEC effectively dominates Afghanistan, balances India and gives a much needed boost to a sagging Pakistan economy.
- China's one belt, one road and the Maritime silk route has major political, economic, strategic and security implications for India. As it

further strengthens Beijing's string of pearls strategy. China's exploitation of non-contact warfare capability in the cyberspace information wars, psychological warfare and electronic warfare.

- China's covert and overt support to Indian insurgent groups in the NE.

The Hybrid threat may manifest in many ways and spheres. It's a well established fact that the Chinese goods and parts are all pervasive and on account of low cost and easy access. Made in China parts can be easily embedded into government and military systems and subsystems specially so in the ICT which is a vital part of the C3I systems. These subsystems can be controlled to either function or dysfunction at the command of the owner which happens to be China.

Future conflicts will be a continuous, long drawn war conducted in many battle spaces by multiple means driven by collective ideas but without any direct attributability, by denial of physical military application of combat power and employing proxies for cyber warfare thus circumventing international laws and consequent sanctions.

Future conflicts will be complex. These are not likely to be large scale, conventional wars in the backdrop of a nuclear umbrella, neither a nuclear war leading to mass destruction nor a totally non-contact war in the cyberspace, and informational domain. So what is the likely shape of future conflicts.