www.maritimeindia.org

Maritime Dimension of Hybrid Warfare – The Indian Context

Author: Gurpreet S Khurana*
Date: 28 December 2017

(This is a revised extract of chapter titled "India's Strategic Landscape, Hybrid Threats and Likely Operational Scenarios" jointly authored by Gurmeet Kanwal, Syed Ata Hasnain, Gurpreet S Khurana and Manmohan Bahadur, in Satish Kumar (ed.) India's National Security: Annual Review 2016-17 (Routledge India: December 2017)

Introduction

To address its maritime dimension, it is essential to comprehend the generic concept of 'hybrid war' and its nature, applied in the Indian context. First; it represents the innovative use of unconventional (non-military) means by the adversary to hurt India's national interests in a manner to be able to achieve its 'desired end-state'. It could also be used in conjunction with conventional means of warfighting, with the aim of disrupting India's warfighting processes at the national-strategic and military-strategic levels. At the higher level, it could target India's apex political decision-making or its national war-effort. At the latter level, it could seek to disrupt its military-operational planning; more specifically – in terms of 'Operational Art' – the 'lines of operation'.

Second; while the term 'hybrid war' has come into vogue in recent times, the concept is not new. Nonetheless, the increased employment of non-state groups by India's adversaries and the advent of new technologies – including the easy availability of Commercial Off-The-Shelf (COTS) equipment – over the past decades have enabled to enhance the potential of disruptive effects against India. In this context, it may be recalled how in November 2008, Pakistan-based terrorists specifically trained for sea-borne clandestine infiltration used advanced satellite-based navigational and communication gadgets and sophisticated weapons to wreak havoc in Mumbai.[1] When

used in conjunction with conventional warfighting, such 'hybrid' means could lead to palpable 'asymmetry' against the Indian military forces.

Third; traditionally, the various security agencies constituting India's national security apparatus have preferred to operate in their respective 'compartmentalized' domains – land, sea or air. However, in the contemporary context, the nature of relevant unconventional means and of the associated technologies enables hybrid threats to transcend all domains. Whatever hybrid means are brought and bear in the terrestrial domain, can also be employed in the maritime realm. Of course, the application of such means would differ, and would be based on the inherent nature of the ocean realm, and the role the seas play in meeting national interests.

Furthermore, the seamless nature of the maritime domain enables ready flow of threats and challenges from one area to another. For instance, maritime terrorism has grown and expanded over the years, operating from the sea and at sea, in both direct and indirect forms, necessitating increased focus on coastal and offshore security. It has also started taking an increasingly hybrid character, with possible blurring of lines between conventional and sub-conventional levels of conflict.[2]

Threat Scenarios

The maritime domain bears vital economic interests of a country. However, a predominant part of the oceans is not subject to national sovereignty, which makes it much easier for a hybrid threat to manifest. For instance, during an armed conflict, an adversary would usually attempt to disrupt India's strategic crude oil imports. The conventional practice is to achieve this through a naval blockade of Indian ports or distant interdiction of India-bound oil tankers. However, this would necessitate establishment of Sea Control. The adversary could avoid all this simply by employing a terrorist group to lay crude mines – even explosive-laden drums – in maritime choke-points like the Strait of Hormuz or Bab-el-Mandeb, wherefrom much of India's oil imports transit. The explosion of a single mine would be sufficient to disrupt shipping through the choke-point due to fear among shippers. The insecurity to shipping could be aggravated using information operations, including through social websites. Although this action would also impinge upon the interests of many other countries, the adversary could deny any linkage with the terrorists.

Another possible scenario could be the paralysis of India's sea trade through cyber-attacks. The increasing digitization of the shipping industry has made it highly vulnerable to such unconventional threats.[3] A determined adversary could hack into its port management information systems or even into the navigation, automation or external communication systems of Indian-flagged ships, leading to disruption of commercial transactions, eventually causing serious outcomes for the Indian economy.

The adversary could also employ terrorists to target India's offshore oil-platforms using bomb-laden fast boats. Identifying the threat in the open seas amidst rather dense shipping and fishing environment has always been a major challenge. After the November 2008 terrorist attacks in Mumbai, India has taken major strides towards enhancing Maritime Domain Awareness (MDA) through coastal surveillance measures and the establishment of the National Command Control Communications and Intelligence Network (NC3IN). However, the NC3IN could be disrupted by the sponsoring state through cyber attacks preceding the terrorist action. Such disruption could also precede a terrorist strike from seawards against India's critical littoral infrastructure like nuclear installations.

The adversary may also use unconventional means to disrupt India's satellite-based maritime communications and imagery services. This is more likely to be undertaken at crucial moments during or preceding an armed conflict; and using non-kinetic means, which encompasses an element of deniability. The satellites could be 'blinded' through cyber-attacks against the control stations, or even directly through Electro-Magnetic Pulse (EMP) weapons.

India's coastal infrastructure and assets are also susceptible to hybrid threats in the form of clandestine underwater attacks by terrorists trained in diving operations. It is well known that achieving even limited sub-surface MDA is extremely challenging. The recent advances in underwater technology – including robotics – achieved by India's adversaries, compounds the threat. India's major ports are more at risk since these are hubs of the nation's maritime-economic activity and represent soft targets. The impending growth of passenger and cruise shipping industry would only enhance the vulnerability of Indian ports, including that of cruise terminals and passenger vessels plying in India's island territories.

Another hybrid scenario could be the disruption of the Global Undersea Communication Cable Infrastructure (GUCCI), which runs across the Indian Ocean. Nearly all of India's major internet and telecommunications service providers use GUCCI, whose disruption could isolate India's cyberlink communication with the rest of the world. In December 2008, multiple accidental cable cuts in the Mediterranean Sea and the Persian Gulf resulted in a widespread loss of internet connectivity throughout the Middle East and South Asia. India lost 50 to 60 per cent of online connectivity while Egypt lost 70 per cent. Many feel that communication satellites can serve as redundancy in the event of a disruption of GUCCI, but this is not true since these satellites offer a limited bandwidth.[4]

Conclusion

Responding to 'hybrid' threats at sea is not an easy proposition, considering that the maritime domain is a predominantly international medium. The presence of a large number of neutrals in the vast and largely unregulated expanse of the oceans brings about two major challenges, viz. achieving MDA and formulation of effective Rules of Engagement (RoE).

Nonetheless, since 'hybrid' threats transcend land, sea and air domains, and even the capabilities of Indian military forces, the response to these threats necessitates a more holistic and synergistic national approach, with the defence forces firmly within the loop, even though not spearheading the response.

****

**Captain Gurpreet S Khurana, PhD, is Executive Director at National Maritime Foundation (NMF), New Delhi. The views expressed are his own and do not reflect the official policy or position of the NMF, the Indian Navy, or the Government of India. He can be reached at gurpreet.bulbul@gmail.com*

References

[1] 'Pakistan Navy frogmen trained Kasab, other terrorists: Headley', *The Times of India*, 19 July 2010, at http://timesofindia.indiatimes.com/india/Pakistan-Navy-frogmen-trained-Kasab-other-terrorists-Headley/articleshow/6187958.cms (Accessed 17 November 2016)

[2] 'Ensuring Secure Seas: Indian Maritime Security Strategy', Integrated Headquarters, Ministry of Defence (Navy), 2015, p.104

[3] Fiona Macdonald, 'Top 5 Facts About Cyber Attacks', *Ship Efficiency Review*, 8 April 2016, at http://www.shipefficiencyreview.com/top-5-facts-about-maritime-cyber-security/ (Accessed 11 November 2016)

[4] RJ Rapp, FS Gady, SS Parmar and KF Rauscher, 'India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure', *Strategic Analysis*, Vol 36(3), May-June 2012, pp.375-383.