ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

INDIAN CYBER POSTURE: IMPLICATIONS FOR PAKISTAN

By
Aamna Rafiq
Research Associate

Edited by
Najam Rafique

October 2, 2019

Indian Cyber Posture (ICP) is predominantly centered on the integration of cyberspace with other domains at the operational level rather than handling it as a discrete realm. The *Joint Doctrine for Indian Armed Forces 2017* includes cyberspace in the core definition of national territory together with land, air, aerospace and maritime. This "Integrated Military Power Principle" (IMPP) has led to the inclusion of cyberspace at doctrinal, force structure, institutional, political, economic, diplomatic, logistics and human resource development levels, but preserves the "decentralization, of command and decision-making" at the same time.[1]

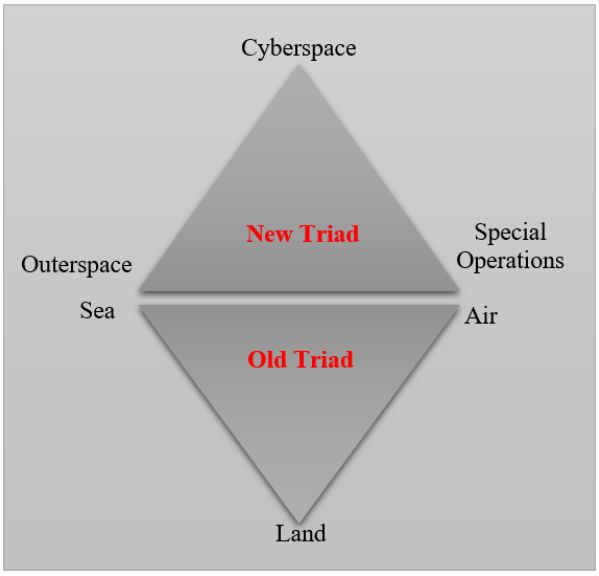
There are two fundamental drivers of this approach.

First, and the most interesting aspect is how New Delhi defines cyberpower. According to the Indian Ministry of Defense, it refers to acquiring vital information and the development of critical infrastructure imperative for growing e-commerce and establishment of global business linkages, but simultaneously denying all these to an adversary in order to maintain a competitive advantage "in the globalized world economy."[2] The objective is to establish a secure economy and financial support for the technological modernization of military force structure.

[1] Government of India. Ministry of Defense. *Joint Doctrine Indian Armed Forces*. New Delhi: Headquarters Integrated Defense Staff (2017): 3, 40.
[2] Ibid., 26.

Second, India has declared cyberspace, notably in terms of information warfare, as the backbone of the military operations at strategic level.[3] While defining the spectrum of conflict, New Delhi laid a special emphasis on fifth generation or hybrid warfare and acknowledged cyber warfare as its essential component. It also acknowledged cyber warfare conducted by state-sponsored non-state actors as an effective tool of creating chaos and violence. The objective is to destroy the adversary`s free and secure access to cyberspace in the operational environment by utilizing the various "instruments of national power" which ultimately require synergy. India is determined to establish a *Cyber Force Structure* (CFS) which could help it win cyber wars. India is also aspiring to wage *Network Centric Wars (NCW)* to exploit computers, surveillance and intelligence systems, Command and Control System (C2S), and information technology infrastructures.[4]

The roots of ICP can be traced back to the *Indian Army Doctrine 2004*[5] famously known as the *Cold Start Doctrine* which included hacking of Commercial Cloud Services (C2S), national aviation, banks, power-generation and other revenue-generating computer-based industries in addition to the destruction of the electromagnetic spectrum and psychological warfare. A decade ago, ICP was just ideation, but today, India is taking practical steps to transform this ideation into a future reality. To achieve maximum strategic advantages, India has added a "new triad" to its military force posture consisting of *Cyberspace, Special Operations* and *Outer Space*. These are the new domains where India is preparing to fight future wars in addition to the traditional triad composed of *Land, Air,* and *Sea*. Cyberspace and Outer Space will maintain the information flow necessary for accomplishing strategic objective through special operations.[6] The recent Balakot crisis in February 2019 was a perfect test case for this new triad. During the crisis, India allegedly conducted a special



Source: Joint Doctrine Indian Armed Forces, 2017.

[3] Ibid., 3.
[4] Ibid., 13, 49.
[5] Government of India, Ministry of Defense. *Indian Army Doctrine 2004*. New Delhi: Headquarters Integrated Defence Staff, last modified October 4, 2004, https://www.files.ethz.ch/isn/157030/India%202004.pdf
[6] Government of India. Ministry of Defense. *Joint Doctrine Indian Armed Forces*. New Delhi: Headquarters Integrated Defense Staff (2017): 48 – 49.

operation on the false pretext of the Pulwama terrorist attack, after which India used cyberspace, especially the social media platforms to malign the image of Pakistan through information warfare.

The *Joint Doctrine for Indian Armed Forces 2017* also outlined the establishment of three crucial agencies or tri-service commands namely: Defense Cyber Agency (DCA), Defense Space Agency (DSA), and Special Operations Division (SOD). Prime Minister Narendra Modi gave approval for the establishment of these three agencies during the "Combined Commander`s Conference" in September, 2018. These three agencies will be fully operational at the end of 2019. Rear Admiral Mohit Gupta will serve as the first head of DCA.[7] DCA is fundamentally an up-gradation of *Defense Information Assurance and Research Agency* (DIARA) which was previously established to facilitate the Ministry of Defense and the Indian Armed Forces for their information operations in cyberspace.[8] DIARA was also responsible for the monitoring of the Indian cyberspace at a meta-data level which will work in close collaboration with the *Defense Communication Network (DCN)*.The National Cyber Coordination Centre (NC3) is already working under the Ministry of Information for effective civil-military coordination in cyberspace. India is likely to finalize its new Cyber Policy in the first quarter of 2020 to replace its Cyber Policy of 2013.[9]

To further strengthen its escalating posture in cyberspace, India is increasing its collaboration with other countries and international organizations. In the course of the last five years, India has signed 39 multilateral agreements and 54 Memorandums of Understandings (MOUs) on cyberspace with various counties. New Delhi has also established cyber frameworks with 10 countries including China, Australia, Egypt, Japan, Malaysia, Russia, Singapore, Mongolia, United Kingdom and United States of America. These frameworks are focused on mutual collaboration in the areas of cybercrime mitigation, e-governance, intelligence sharing, Computer Emergency Response Teams (CERT) and technical training.[10] On August 22, 2019, India`s Ministry of Electronics and Information Technology signed a significant agreement of cooperation in cyberspace with the Estonian Information System

---

7 "India Set to Get Defence Cyber Agency…," *NDTV*, last modified April 30, 2019, https://www.ndtv.com/india-news/india-set-to-get-defence-cyber-agency-to-fight-pak-chinese-hackers-2030798.

8 Rajat Pandit, "Agencies take shape for special operations, space, cyber war," *Times of India*, https://timesofindia.indiatimes.com/india/india-begins-setting-up-new-tri-service-agencies-to-handle-special-operations-space-and-cyberspace/articleshow/69346012.cms.

9 Kritti Bhalla, "India to Get National Cybersecurity Policy By January 2020," *Inc 42*, last modified August 29, 2019, https://inc42.com/buzz/india-to-get-national-cybersecurity-policy-by-january/.

10 Leilah Elmokadem, "Mapping of India's Cyber Security-Related Bilateral Agreements," *The Centre for Internet and Society, India*, accessed August 25, 2019, https://cis-india.org/internet-governance/files/CyberSecurityAgreements_Infographic_04.pdf.

Authority (RIA).[11]The third edition of the Indo-French Cyber Dialogue was also held on June 20, 2019.[12]Apparently all these collaborations seem normal, but in reality these could prove to be extremely threatening for Pakistan because of two major reasons.

Firstly, the dual-use nature of cyber technologies will allow New Delhi to divert them from e-governance, e-commerce and communication sector to the technological modernization of military force structure. Secondly, a close inspection of these agreements, MOUs and frameworks especially with France, Japan, Indonesia and Russia show a consistent pattern of pairing cyberspace with the Outer Space technologies, Artificial Intelligence (AI), intelligence sharing, violent extremism and terrorism. This indicates India`s determination for robust operationalization of its new triad. This also indicates that cyberspace will be the next potential domain of conflict after Kashmir and water dispute. Any cybercrime at domestic level could be rapidly transformed into a cyber-crisis between the two nuclear powers. This threat is further validated by the Indian insistence on the application of Article 51 of United Nations Charter on cyberspace. India along with US-led block of Western countries is strongly advocating for the right of individual and collective self-defense in case of an armed attack in cyberspace.

This is a matter of serious concern because there is no understanding or Confidence Building Mechanism (CBMs) in place for cyberspace between India and Pakistan. Both countries are at a different level of technological advancement with a different set of laws, strategies and policies in cyberspace. How both states will develop an understanding of cyber-threshold? What infrastructures should be considered as critical in cyberspace? What will be the parameters to determine that cyber-attack actually happened, especially in the absence of reliable attribution mechanisms? These issues will further complicate the regional dynamics and produce destabilizing effects on strategic stability of South Asia. Under the pretext of international security in cyberspace, India is looking for the window of opportunity to use cyber-attacks as a justification for its military adventurism and interventionist policies.

It's high time for Pakistan to develop counter-force, as well as counter-value cyber capabilities. Despite rapid digitalization and technological modernization, Pakistan should always retain a human element in the management of its critical infrastructures, especially banking systems, C2S, and power generation plants. The security and military establishment must take effective measures for

[11] "Estonia's RIA concludes agreement on enhancement of cyber-security with India," *The Baltic Times,* last modified August 22, 2019, https://www.baltictimes.com/estonia_s_ria_concludes_agreement_on_enhancement_of_cyber-security_with_india/.

[12] "Indo-French Roadmap on Cyber security and Digital Technology," Prime Minister`s Office, India, last Modified August 22, 2019, https://www.pmindia.gov.in/en/news_updates/indo-french-road-map-on-cyber-security-and-digital-technology/.

the establishment of tri-service cyber command and enhance its international collaborations in cyberspace.