SPOTLIGHT
ON REGIONAL AFFAIRS

October 2025, Vol.43, No.10 (2)

Emerging Military Doctrine of Pakistan: From Battlefield to Cyberspace

Alina Fayaz*

Introduction

The evolving nature of war has blurred the lines between traditional and non - traditional conflicts. The traditional arena of warfare, i.e., land, sea and air has expanded to outer space, becoming the new and threatening frontier within the digital revolution. Unlike conventional battlefields, cyberspace is transnational, borderless and is mostly invisible, working by means of codes, networks, and information systems.[1] Both state and non-state actors are competing in cyberspace to gain influence, dominance, and strategic advantage without necessarily engaging in a physical conflict.

For Pakistan, cyberspace is not a marginal component of its national security, it is instead a key element in its developing military doctrine. Although the traditional deterrence and the nuclear potential have traditionally characterised the strategic position of Pakistan, the emergence of cyber threats have necessitated the directional changes within the military doctrine.[2] Cyberattacks have the capacity to cripple communication networks, sabotage infrastructure, halt economic activity, and subvert institutional legitimacy, which cannot be addressed by nuclear deterrence.[3] Pakistan has struggled to balance sovereignty in cyberspace and positioning itself in the regional landscape characterised by hybrid warfare and long-term hostility, especially with India.

This article discusses the incorporation of cyber capabilities in national security doctrine of Pakistan, followed by an analysis of some of the hybrid threats and examples of cyber-enabled campaigns. The last section sheds light on the analytical levels of deterrence, leadership and indigenous capacity-building to conclude with considerations into the future.

Cyber Frontier of Pakistan's Military Domain

The introduction of the cyber space into the Pakistan's military domain is a paradigmatic change in the strategic culture. The traditional nuclear deterrence system has embraced cyber deterrence based on the consideration of digital and informational fields in hybrid warfare that has a direct impact on strategic stability.[4]

Various institutional reforms have been incorporated within the armed forces structures of Pakistan to inculcate cyber preparedness, expressing the deliberate effort to establish cyber capabilities as a foundation of national defense. One such instance is the expansion of operations within the Signals Directorate of Pakistan Army to include cyber operations, in which it can protect communications and Command and Control (C2) systems.[5] Similarly, special wings have been formed within the Pakistan Navy and Air Force with emphasis on information warfare in addition to protection of cyber space and electronic warfare.[6]

The regiments of training also become more integrated as readiness exercises now readily include the use of simulated cyberattacks, red-team exercises, and combined exercises in electronic warfare.[7] To improve real-time monitoring and incident analysis and instantaneous counteractions to cyber incursions and disinformation campaigns Rapid Response Teams (RRTs) at institutions, such as the Inter-Services Public Relations (ISPR) are developing.[8]

In addition to the Military's preparedness, the National Cyber Security Policy (NCSP) 2021 is also serving as a unifying policy on cybersecurity at the policy level that brings civilian and military purposes of cybersecurity together.[9] It focuses on

* Alina Fayaz is working as Assistant Research Officer with the Cybersecurity Program at the Institute of Regional Studies (IRS), Islamabad.

securing critical information infrastructure, developing local technological capabilities, enhancing intelligence sharing and providing a whole-of-nation defense posture. The comprehensive policy brings together military, civilian, research, academic and technical entities together ensuring that there is no fragmented response and coordination between sectors is institutionalised, reflecting global trends of evolving doctrines.

Regional and Global Context

The cyber doctrine of Pakistan cannot be separated from the regional context. The competition with India is one of the main drivers of the cyber militarisation. Nonetheless, the wider trends in the world, including the US and China cyber wars and the application of hybrid warfare by Russia influence the perception of Pakistan as well. Regionally, South Asian cyber governance is not well institutionalised due to structural lacking. Therefore, it is a challenge for Pakistan to protect itself from the hostile cyberspace and promote collaborative mechanisms and international norms. Both state and non-state actors pose never-ending threats highlighting the criticality of cyber integration as component of overall hybrid warfare that may include a combination of cyber operations, disinformation, psychological campaigns, and propaganda. This section explores the threats posed by both state and non-state actors below:

State-Sponsored Threats

In the evolving landscape of regional cybersecurity dynamics, certain states have adopted increasingly assertive postures in cyberspace. Among these, India has emerged as the most actively and strategically engaged state in conducting cyber operations against Pakistan. Government websites have been targeted by DDoS attacks; military officers have been the victims of spear-phishing and attempts to break into defense networks have been reported. Apart from these direct attacks, disinformation campaigns have been launched as well, posing similar threats. In a report published by EU Disinfo Lab, the Indian Chronicle (2020) uncovered a vast network of fake NGOs and media houses that were being used to damage Pakistan's image globally and influence decisions in places like EU and UN.[10]

Use of disinformation by India to spread fake news and false information during Pulwama attack and the subsequent Balakot airstrikes to influence global opinion is a clear example of hybrid warfare. In reaction, Pakistan used digital forensics; evidence based diplomatic briefing and coordinated communication strategies revealing the complex interplay of interplay of the traditional, informational, and cyber worlds during national crisis. Similarly, the APT groups had carried out long term sabotage and espionage operations on the defense and energy sectors in Pakistan that they claimed had the state sponsorship.[11] These cyber-attacks demonstrated the weakness of the dual-use infrastructure (which is used both in the civilian context and in the military context). It also needed countermeasures in the form of hardened encryption, air-gapped technology and strengthened incident-response measures.

Non-State Actor Threats

Cyberspace has been used by extremist groups in a manner that has led to the groups' recruiting, propaganda and disruption. In 2022, organised government sites were hacked by non-state actors, which defined the exploitation of vulnerability. Civil-military synergy is required as the mitigation response of the Pakistan was based on the cooperation of the military cyber units and the National Cyber Emergency Response Team (CERT).

All this indicates how multidimensional cyber threats are to the Pakistan's security environment. They divulge that answers to the effective doctrine should be above the reactive defense to proactive measures based on resilience, intelligence, and credible deterrence.

Pakistan requires a comprehensive policy framework that fosters collaboration between government institutions and private sector entities to effectively address cyber-related threats. Additionally, engaging in regional partnerships for cyber intelligence sharing will strengthen Pakistan's capacity to respond proactively and enhance its overall cybersecurity posture.

Pakistan needs a strong plan to bring government and private companies to deal with cyber related threats. Pakistan should start working with other countries to share information related to cyber-attacks that can strengthen Pakistan's stance to respond better and stay safe from cyberattacks.

Analytical Dimensions of Cyber Integration

There are both challenges and opportunities of cyber capabilities in doctrine incorporation and a tri-dimensional analysis is needed in the analysis of deterrence, leadership analysis, and indigenous capacity-building. In today's evolving security landscape, reliance on nuclear weapons alone is no longer sufficient for ensuring Pakistan's national security. The traditional concept of nuclear deterrence falls short in addressing the complex ad emerging threats of the modern era, particularly in the cyber domain.

Although nuclear capability has been historically the heart of national defense, the very nature of cyber warfare, namely its anonymity, scalability and deniability, makes the logic of conventional deterrence less efficient. This is unlike nuclear threats where the traditional defense mechanisms can prevent the attack, but cyber-attack can slip through systemic vulnerabilities without any evident attribution, which makes retaliation less credible. Therefore, Pakistan needs to redefine its strategic policy to incorporate cyber deterrence with its nuclear posture. It will need to take a two-pronged strategy, one of deterrence by denial which involves ensuring robust digital infrastructures so that the adversaries cannot achieve their goals; and deterrence by punishment whereby they will use credible threats of retaliatory cyber attacks, uncovering of malicious operations, or even using diplomatic means. It is only under a balanced and integrated framework that Pakistan would be able to come up with a feasible cyber deterrence system which would help prevent the threats of being exploited by the technologically advanced enemies.

Cyber Warfare Leadership Problems

As stressed by Sun Tzu, the ultimate excellence is to conquer the opponent without fighting. The pinnacle of this maxim is cyber warfare, which provides the option to counterattack without using kinetic force. This demands that military leaders should integrate traditional attributes of command with technical expertise in IT systems, network security and digital forensics.

Francesca Spidaleri maintains that cyber defense requires interdisciplinary skills as a field-computer science and engineering are essential; however, international law, behavior psychology, and political science are also essential.[12] Pakistan therefore needs new breed of cyber-strategic leaders who would be able to cross technical and strategic world. Devoid of such leaders, institutional reforms are either stalled or mismanaged.

Indigenous Capacity Building

Dependence on external technologies poses supply-chain threats and the back door risks. To achieve true sovereignty in the cyberspace, Pakistan needs to develop local encryption system, secure communication systems and domestic cyber-defense systems. The collaboration with universities focuses on research and development, and the development of the skilled staff pipeline are crucial to long-term resilience. At present, gaps persist. The level of protection of civilian infrastructure is still low, inter-agency coordination tends to be disjointed, and the involvement of the private sector is limited. These weaknesses will be resolved to decide whether the cyber doctrine can be transformed into the policy rhetoric as it will be operational reality in Pakistan.

Combined Warfare and Information Operations

Another aspect of cyber integration is in information warfare. The doctrine of Pakistan is slowly considering information campaigns as the most important part of national security. Disinformation, propaganda, and perception management are components of hybrid tactics used against Pakistan, which was witnessed on Pulwama-Balakot and Indian Chronicle. The reactions of

Pakistan include laws like the Prevention of Electronic Crimes Act (PECA), international diplomatic attempts to unveil disinformation at the international conferences.

However, this does not eliminate the tension between the rights of civil liberties and the information that is controlled by the state. Excessive attention to control of information can lead to erosion of popular confidence and there is the necessity of balance between security considerations and democracy.

Conclusion

The traditional security domain faced a radical shift due to the incorporation of cyberspace into the military doctrine of Pakistan. The strategic path towards institutionalisation of cyber power is based on the understanding that digital war will not only be waged using kinetic weapons, but also codes, algorithms, and disinformation. The inclusion of cyber capabilities has transformed the doctrine towards proactive deterrence; however, certain issues still exist. These include weak civilian infrastructures, constant antagonism by their rivals in the region, anonymity of cyber threats, and lack of proper foreign technology are all weaknesses. Therefore, long term investment in domestic capabilities, inter-disciplinary leadership and civil military partnerships is necessary for appropriate cyber integration. To shape the trajectory of its future security, it is important for Pakistan to align its military doctrine with the cyber developments. Strategically, cyberspace has the potential to serve not just as a sphere of defense, but also as a source of power, stability, and deterrence, all of which are critical to maintaining sovereignty and regional security.

Notes and References

1 Zeeshan Faisal, "Cyber Warfare and International Security: A New Geopolitical Frontier," *the Critical Review of Social Sciences Studies* 3, no. 2 (19 April 2025): 513–27, https://doi.org/10.59075/k9cbhz04.

2 Timothy D. Hoyt, "Pakistani Nuclear Doctrine and the Dangers of Strategic Myopia," *Asian Survey* 41, no. 6 (November 2001): 956–77, https://doi.org/10.1525/as.2001.41.6.956.

3 Shahrukh Khan, "Cyber Security Challenges in Pakistan: An Assessment," Science Diplomacy Perspective 1, no. 1 (10 March 2022): 78–89, https://www.researchgate.net/publication/360256123_Cyber_Security_Challenges_in_Pakistan_An_Assessment.

4 Melika Mohammadi, "The Cyber Challenges to Nuclear Deterrence: Evaluating Pakistan´s Nuclear Deterrence in a Digital Era, 2024, https://nmbu.brage.unit.no/nmbu-xmlui/bitstream/handle/11250/3156410/no.nmbu%3Awiseflow%3A7083314%3A59113065.pdf?sequence=1&isAllowed=y.

5 Hassan Feroz and Khan, "Nuclear Command, Control and COMMUNICATIONS (NC3): The Case of Pakistan Technology for Global Security Special Report," 2019, https://securityandtechnology.org/wp-content/uploads/2020/07/khan_pakistan_nc3_IST_special_report.pdf.

6 Baqir Sajjad Syed, "Situationer: PAF's Cyber-Space Blitz Humbles IAF," *Dawn,* May 15, 2025, https://www.dawn.com/news/1911123.

7 Cristian Chindruş and Constantin-Florin Căruntu, "Enhancing Cybersecurity Readiness through the Red and Blue Team Competition," *Buletinul Institutului Politehnic Din Iaşi. Secţia Electrotehnică. Energetică. Electronică* 69, no. 2 (June 1, 2023): 35–56, https://doi.org/10.2478/bipie-2023-0008.

8 Gadi Eshed, "The Rapid Response Security Teams (RRSTs) on the Front Lines of Counterterrorism - ICT," *ICT*, 9 April 2025, https://ict.org.il/rapid-response-security-teams-on-the-front-lines-of-ct/.

9 Aamna Rafiq and Malik Mustafa, "THE NATIONAL CYBER SECURITY POLICY of PAKISTAN 2021," 2021, https://issi.org.pk/wp-content/uploads/2021/10/IB_Aamna_Oct_15_2021.pdf.

10 Bilal Kuchay, "EU NGO Report Uncovers Indian Disinformation Campaign," *Al Jazeera,* 2020, https://www.aljazeera.com/news/2020/12/11/eu-ngo-report-uncovers-a-15-year-disinformation-campaign.

11 " Subject -9vber Securitv Advisorv -Cvber Attacks Asainst Pakistan Bv *Sidewinder ApT Group (Advisorv No. 54),*" https://cabinet.gov.pk/SiteImage/Misc/files/NTISB%20Advisories/2022/54-Advisory-No-54-2022.pdf.

12 Francesca Spidalieri and Jennifer McArdle, "The Role of Cybersecurity Education in US Service Academies," *The Cyber Defense Review* 1, no. 1 (2016): 141–64, https://doi.org/10.2307/26267304.