CENTRE FOR AEROSPACE POWER AND STRATEGIC STUDIES

In Focus

New Delhi

CAPSS In Focus: 08/2026

12 February 2026

Strategic Dilemma of Contemporary Cyber Warfare: Evidence-based Analysis and Imperatives for India

Ms Gowri R
Research Associate, Centre for Aerospace Power and Strategic Studies

Source: Created by the Author using AI

Keywords: Cyber Incidents, Armed Conflict, Cyberspace, Geopolitical, Strategic Effects

From Deterrence to Persistent Engagement

The dawn of the digital age has brought about a profound transformation in the nature of conflict, security, and the rule-based international order. The deepening inter-connections of societies, economies, and militaries have made cyberspace a domain of strategic competition, which challenges the traditional security paradigms. Cyber weapons, in the form of malicious code and sophisticated cyber operations, now stand alongside conventional and nuclear arms as a decisive instrument of statecraft, capable of shaping the destinies of nations, conflicts, and the stability of the global system.[1] Cyber warfare operates in a borderless, instantaneous, and accessible domain, involving a wide array of actors, from major powers and rogue States to non-state groups and even individuals.[2] This democratisation of capabilities has blurred the lines between war and peace, offence and defence, and state and non-state actors, creating a landscape of persistent, low-level competition.

With the heightened contemporary geopolitical tensions, such as armed conflicts, changing alliances, or economic sanctions, states and non-state actors increasingly turn to cyberspace as a priority domain for competition, disruption, and influence. Geopolitical uncertainties are increasing the incidences of cyber operations, as states employ them to gain strategic advantage, signal retaliation, and reduce adversary's capabilities while avoiding overt military escalation. The ambiguity and uncertainty surrounding cyber operations also reduce attribution, making it difficult to identify responsible actors and implement proportional responses, thereby encouraging actors to take more aggressive actions in cyberspace. Importantly, the cyberattacks have emerged as one of the top five geopolitical risks of 2025 targeting Critical Information Infrastructure (CII), government and private sector networks.[3]

Cyberspace is a sociotechnical environment defined by interconnectedness and potential for exploitation [4] Traditional concepts of deterrence and coercion, central to the nuclear and conventional strategic paradigms, are shifting with the growing cyber environment. The logic of security in cyberspace is determined by continuous operations; states must persistently set and reset the conditions of security in their favour, anticipating and countering the actions of adversaries in a domain where the boundaries of engagement are fluid, and the costs of entry are minimal.[5] Cyberspace has renewed interest as a military instrument of statecraft with strategic foresight. This necessitates a focused review of cyber incidents associated with armed conflicts and engagements from the previous year, with particular emphasis on the use of the cyber domain to achieve strategic advantages. The emerging strategic imperatives shall reinforce India's cyberspace capabilities towards developing a resilient and credible cyber power.

Cyber Escalation in Armed Conflicts since 2025

Throughout the Russia-Ukraine conflict since 2022, Cyber operations have played an important role. In 2025, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP Ukraine) developed its cyber capabilities through the detection of cyberattacks, the acquisition of necessary instruments (network monitors), and raising awareness to the general public with the help of the North Atlantic Trade Organisation (NATO), the European Union (EU), and the United States (US). The Computer Emergency Response Team of Ukraine (CERT-UA) has processed 6,000 cyber incidents in 2025 targeting Ukraine's government, defence, and critical infrastructure sectors, as the nation continues to face sustained attacks.[6] The operational activities targeting sophisticated and technical capabilities demonstrate that Russia has institutionalised cyber warfare as a primary instrument of statecraft, coordinated across the Foreign Intelligence Service (SVR), Federal Security Service (FSB), and Main Intelligence Directorate (GRU). Russian state sponsored actors such as APT 28, APT 29, KillNet, NoName056(16) and others use Artificial Intelligence (AI) tools such as ChatGPT and large language models (LLMs) to scale up the attacks, using polymorphic techniques to frequently change the signature, use of legitimate cloud services such as telegram and one drive to create Command and Control (C2) channels, development of Industrial Control Systems (ICS) specific malware to disrupt Operational Technology (OT) architecture, and deliver malware to the targeted individuals, and use of sophisticated tools to erase the logs and stop incident response.[7] The FSB-linked Gamaredon's evolution from crude phishing campaign to sophisticated zero-day exploitation, Cloudflare-based C2 obfuscation, and data exfiltration within 30 to 50 minutes necessitates equally agile defensive postures from organisations and national security entities.[8] Russian hackers demonstrated their cyber prowess in space systems by telecasting the Victory Day parade to Ukrainian viewers, extending the war in all domains.[9] Ukrainian cyber defence has been fortified with the support of the West, which has helped significantly helped in countering the Russian cyber offensive campaigns. Russo-Ukraine conflict in the cyber domain has reiterated that cyber defence is more difficult than cyber offence, contrary to the conventional paradigm of defence-offence balance. This can be mitigated only through the proliferation of emerging and innovative employment of technologies in the conduct of operations.

In May 2025, the Pahalgam Terror Attack led to conflict between India and Pakistan. Parallel to military escalations, cyberattacks were prevalent in both India's and Pakistan's cyberspace.[10] Pakistan targeted the government officials by sending spear phishing emails with malware attached to it. The Distributed Denial of Service (DDoS) attack, defacement of websites, and social media handles were observed on both sides. A coalition of cyberspace hacktivist collectives was employed to obtain strategic effect coupled with perception management. Both India and Pakistan have recognised cyber as a domain of warfare with a significant increase in capabilities. However, during

the conflict, both sides refrained from declaring evidence for coordinated cyber operations for the conduct of operations in other domains.

In June 2025, Israel and Iran escalated cyber warfare in parallel with kinetic conflict. Israel crippled Iranian financial systems, and hacktivist group Predatory Sparrow reportedly stole USD 90 million from Nobitex, Iran's largest cryptocurrency exchange.[11]

Israel's Unit 8200 carries out defensive and offensive cyber operations in its defence infrastructure. Israel has conceptualised a cyber-Iron Dome with effective cyber intelligence, defensive and offensive operations following Operation Protective Edge in 2014.[12] The Predatory Sparrow, an Israeli-based hacktivist group likely state-sponsored, is known for its cyber-attack on gas stations, steel manufacturing plants, and railway stations of Iran. Iran responded with a 700 per cent surge in cyberattacks targeting Israeli networks.[13] Iran's cyber offensive operations are carried out through the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS). APT 42, APT 34, and Muddy Water, which are among Iran's state-sponsored APT groups conducting cyber espionage through social engineering, cloud compromise, PowerShell, public exploits, Domain Naming System (DNS) tunnelling, and supply chain attacks.[14] Iranian state and non-state actor attacks also target countries allied to Israel. These attacks show deterrence and coercion effects in the systems. Technologically superior Israel was counterbalanced through Iranian cyber response. Cyber deterrence is possible even with limited capabilities, with a credible response coupled with the intent and communication of offensive actions coordinated in other domains.

In July 2025, the conflict between Thailand and Cambodia over the border dispute resulted in military clashes accompanied by cyberattacks, including DDoS and website defacement attacks.[15] Persistent cyberattacks are expected to continue as the disputes remain unresolved. Beyond these, cyber operations have become a geopolitical competition across the globe. North Korea's Lazarus Group has demonstrated its cyber capabilities and generated revenue through a large-scale cryptocurrency exchange breach.[16] China's cyber threat actors, such as Volt Typhoon and Salt Typhoon, have maintained persistent access to US Critical infrastructure and multiple telecommunication networks, respectively.[17] Moreover, the Philippines has also faced more cyberattacks from China-linked threat actors amid the intensifying South China Sea territorial waters conflict. This implies that persistence of cyber operations during peacetime is equally significant to the actions and responses carried out before and during the war.

The Operation Absolute Resolve by the United States (US) carried out a multidomain operation on Venezuela involving cyber, electromagnetic, space, and air power. The cyberattack occurred on January 03, 2026, leading to a blackout or outage.[18] The cyber effects played as an

enabling factor for air power to accomplish the operation. Large-scale cyberattacks of this nature require planning and capabilities built over several preceding years. In March 2019, Venezuela reportedly suffered major blackouts in approximately 20 cities. The then-president of Venezuela, Nicolas Maduro, accused the US of a cyber and electromagnetic attack, which resulted in an outage and disruptions in telecommunications. However, this accusation was rejected by the US.[19] There is a possibility that the requisite cyber capacity has been further developed and executed now, before the current attack. This has revalidated that multidomain integration is vital in obtaining the strategic effects through cyberspace. Military effectiveness is dependent on operational readiness through planning considerations with foresight.

Conclusion

The recent trends observed in conflicts from the year 2025 underscore the importance of cyberspace as a persistent domain of contest rather than a supporting role. The growth of critical national infrastructure, along with rapid digitisation and volatile geopolitical situations, demands a proactive cyber strategy. Evidence-based analysis of the cyber incidents indicates profound use by the great cyber powers to derive strategic effects to shape the conduct of their own operations. Cyberattacks predominantly targeted CII, leveraging the system vulnerabilities of OT to retain the operational advantage in other domains. While the lesser cyber powers are limited to operational effects to support their narrative in the cognitive domain. This proves that the cyber threat landscape would remain proliferated with persistent threat vectors to gain a competitive edge through cyber espionage and weaponising vulnerabilities in future. The use of technologies such as AI-enhanced malware development, zero-day exploitation, and ICS-specific tools of threat actors has been normalised and continues to accelerate. The boundaries between state and non-state actors have reduced, with hacktivist proxies functioning as force multipliers that provide deniability while expanding operational reach.

Cyber resilience has to be recognised as a fundamental component of national security strategy. India should define and enforce OT/ICS-specific security guidelines for CII, including IT-OT segmentation, OT asset inventories and incident exercises. The investment in defensive capabilities, offensive deterrence options, international norms development, and cross-sector cooperation has to be developed. There should be communication and coordination among the National Critical Information Infrastructure Protection Centre (NCIIPC), CERT-In, Defence Cyber Agency (DCyA) and state police-level cyber groups, which may be achieved through the National Security Council Secretariat (NSCS) as a central body. The deficit in talent pool to carry out defensive and offensive operations in India should be bridged through upskilling of students, researchers and collaboration with private ethical hacker groups. It is necessary to build cyber awareness and establish cyber teams among all segments of the population.

Due to volatile geopolitical tensions, the use of cyber capabilities by great powers, advances in technology, and coordinated activities between state and non-state threat actors, the conflicts of 2025 proved that in future warfare, the physical and digital domains will be inseparable

Notes:

[1] Lucas Kello, *The Virtual Weapon and International Order* (New Haven and London: Yale University Press, 2017), p. 170.

[2] Ibid.

[3] "Top Geopolitical Risks of 2025," *S&P Global,* 2025, https://www.spglobal.com/en/research-insights/market-insights/geopolitical-risk Accessed on July 16, 2025.

[4] Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory* (New York: Oxford University Press, 2022), p. 149.

[5] Ibid., p 110.

[6] State Service of Special Communications and Information Protection of Ukraine, "CERT-UA Processed Nearly 6,000 Cyber Incidents in 2025: Hostile Attack Volume Rose by 37%," 2025, https://cip.gov.ua/en/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37. Accessed on January 28, 2026.

[7] "A Comparative Study of Russian Offensive Cyber Capabilities from 2022 to 2025," National Cyber Security Centre, 2025, p. https://www.nksc.lt/doc/rkgc/A_Comparative_Study_of_Russian_Cyber_Offensive_Capabilities_from_2022_to_2025.pdf. Accessed on January 29, 2026.

[8] Ibid.

[9] "Russia's Victory Day Beamed in Ukraine: Can Satellites Be Hacked and Could It Threaten National Security?," *Firstpost,* August 19, 2025, https://www.firstpost.com/world/russias-victory-day-beamed-in-ukraine-can-satellites-be-hacked-and-could-it-threaten-national-security-ws-e-13926137.html. Accessed on February 02, 2026.

[10] Gowri Ramakrishnan, "Cyber Warfare: Dual Operational Fronts in Contemporary India-Pakistan Conflicts," Centre for Aerospace Power and Strategic Studies, May 20, 2025, https://capssindia.org/cyber-warfare-dual-operational-fronts-in-contemporary-india-pakistan-conflicts/. Accessed on February 03, 2026.

[11] Kris Jackson, "The Unseen War: Cyber Warfare in the Shadow of Global Conflicts," *Cobalt,* July 08, 2025, https://www.cobalt.io/blog/the-unseen-war-cyber-warfare-in-the-shadow-of-global-conflicts. Accessed on July 14, 2025.

[12] Michael Raska, "Building a Cyber Iron Dome: Israel's Cyber Defensive Envelope," RSiS, October 02, 2014, https://www.files.ethz.ch/isn/184527/CO14192.pdf. Accessed on January 27, 2026.

[13] Kris Jackson, "The Unseen War: Cyber Warfare in the Shadow of Global Conflicts," *Cobalt,* July 08, 2025, https://www.cobalt.io/blog/the-unseen-war-cyber-warfare-in-the-shadow-of-global-conflicts. Accessed on July 14, 2025.

[14] Koushik Pal, "Part 2: The Iran-Israel Cyber Standoff - The State's Silent War," CloudSEK, June 19, 2025, https://www.cloudsek.com/blog/part-2-the-iran-israel-cyber-standoff---the-states-silent-war. Accessed on January 27, 2026.

[15] "Cross-Border Cyberattacks Surge as Thailand–Cambodia Tensions Escalate," *Cyber Defense Wire,* July 29, 2025, https://cyberdefensewire.com/cross-border-cyberattacks-surge-as-thailand-cambodia-tensions-escalate/, accessed on January 27, 2026.

[16] Adam Zarazinski and Bruno Faviero, "Swap Around and Find Out: The New Rules of International Digital Economic Warfare," *War on the Rocks*, August 15, 2025, https://warontherocks.com/2025/08/swap-around-and-find-out-the-new-rules-of-international-digital-economic-warfare/. Accessed on February 03, 2026.

[17] Erica Lonergan and Michael Poznansky, "A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats," *War on the Rocks,* February 25, 2025, https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/. Accessed on February 03, 2026.

[18] Louise Marie Hurel, "Layered Ambiguity: US Cyber Capabilities in the Raid to Extract Maduro from Venezuela," Royal United Services Institute (RUSI), January 14, 2026, https://www.rusi.org/explore-our-research/publications/commentary/layered-ambiguity-us-cyber-capabilities-raid-extract-maduro-venezuela. Accessed on January 27, 2026

[19] Ibid.