Pahalgam attack: Code of war - India and Pakistan take their battle to the (web)front

Synopsis Following the Pahalgam terror attack, India and Pakistan's tensions have escalated into cyberspace, marked by intensified cyberattacks from both sides. Pakistan-sponsored hacker groups target Indian military websites and databases, employing tactics like website defacement and phishing malware.

It’s no longer just bullets and bombs—today, the battlefield stretches into cyberspace. Following the Pahalgam terror attack, tensions between India and Pakistan have sharply shifted into the digital realm, where hacker groups have launched a series of high-stakes cyberattacks. These digital offensives come alongside India’s clearance of Dhruv helicopters for Army and Air Force use and a strong maritime posture by the Indian Navy, which has issued a firing alert in the northern Arabian Sea amid ongoing Pakistani naval drills.

Pakistan-sponsored hacker groups have significantly increased their efforts to breach Indian military websites and databases, focusing particularly on sites linked to schools and veterans, ET reported. In the latest wave of attacks, websites like Army Public School Nagrota, Sunjuwan, and the Army Institute of Hotel Management were targeted, with defaced pages mocking the victims of the Pahalgam incident.

Meanwhile, pro-India hacktivist group ‘India Cyber Force’ also claimed to have hacked Pakistani government and private sector databases of Euro Oil, AJK Supreme Court, University of Balochistan, Wada Call Agency and Sindh Police.

On April 22, a terrorist attack in Pahalgam, Kashmir, left 26 tourists dead, with terrorists linked to Pakistan responsible. In swift retaliation, India took action on April 23, announcing the suspension of the Indus Waters Treaty, closing the Attari border in Punjab, and downgrading diplomatic ties with Pakistan. Pakistan retaliated by shutting its airspace to Indian flights, halting trade, and rejecting India’s move on the water treaty, warning it would be seen as an "act of war."

The cyber warfare According to ET sources, at least two cyberattack groups, ‘Cyber Group HOAX1337’ and ‘National Cyber Crew’, have been actively targeting Indian military-linked sites, launching repeated attempts to infiltrate these high-security domains. "These attacks have focused on websites linked to children, veterans, and civilians," sources revealed, highlighting that the aim is to provoke India's military and test its restraint.

These cyberattacks are just one piece of a broader strategy by Pakistan, which has long leveraged digital warfare alongside terrorism and information campaigns. The continued ceasefire violations along the Line of Control (LoC) suggest this persistent provocation.

Report & Update Regarding Pahalgam Terror Attack', has been flagged by Indian cybersecurity experts. The document, linked to phishing domains that mimic official Indian government websites, is believed to be part of a larger scheme to compromise sensitive information.

India vs Pakistan on the cyber front
Experts predict that the cyberattacks will intensify, with Vishal Salvi, CEO of Quick Heal Technologies, highlighting a sharp escalation in Pakistan-backed cyber campaigns targeting Indian defence and critical infrastructure. His firm's recent investigations revealed that hacker group APT36 (also known as Transparent Tribe) has been deploying advanced malware like CrimsonRAT and MeshAgent through sophisticated phishing attacks. "These cyber strikes coincide with rising DDoS surges and website defacements, all aimed at destabilizing public trust," Salvi told ET earlier.

"Every major flashpoint now triggers coordinated digital offensives aimed at undermining a country's critical infrastructure." The digital battlefield is evolving quickly, and both sides are adapting to evade detection and cause maximum disruption. This escalation is not limited to government and military targets. Dhiraj Gupta, cofounder of mFilterIt, a fraud detection agency, revealed that social media bots and malicious ads have been increasingly used to shape narratives and spread chaos. mFilterIt reported a 10-15% rise in malicious ad placements on OTT platforms over the past week, with 70% of its clients affected by misleading ads.

India Vs Pakistan on the naval front
As India and Pakistan continue to experience heightened tensions along the Line of Control (LoC), the Indian Navy has issued a NavArea alert, warning ships to stay clear of a designated firing zone in the northern Arabian Sea. The alert, effective until May 3, comes amid Pakistan's naval drills in the region.

The Indian Navy has marked the area, about 80-85 nautical miles from Pakistani training zones, as dangerous for navigation due to ongoing firing exercises, signaling India's readiness to assert its maritime presence. India Vs Pakistan on the aerial front The Indian government has cleared the resumption of operations for the Army and Air Force versions of the Advanced Light Helicopter Dhruv after the entire fleet of over 330 helicopters was grounded in January. While the Army, Air Force, and Coast Guard variants are now cleared to fly, the naval version remains grounded.