SEQRITE

Cyber Threat Landscape Analysis:

India-Pakistan Conflict Dynamics

PoV Document

www.seqrite.com

Table of Contents

Introduction 01

Spotlight: APT36 – The Digital Operative of Pakistani Espionage 02

Motivations and Ideologies 03

APT36 and the Pahalgam Scenario: The Tipping Point 04

Why They Attack: Motivations and Messaging 05

Who’s Fighting: Hacktivist Groups and Alliances 06

The View from the Top: Strategic Implications 07

From Hacktivism to Hybrid Warfare 08

Application Layer Attacks: An Overlooked Vector 11

Countermeasures and Responses 16

Conclusion 19

Introduction

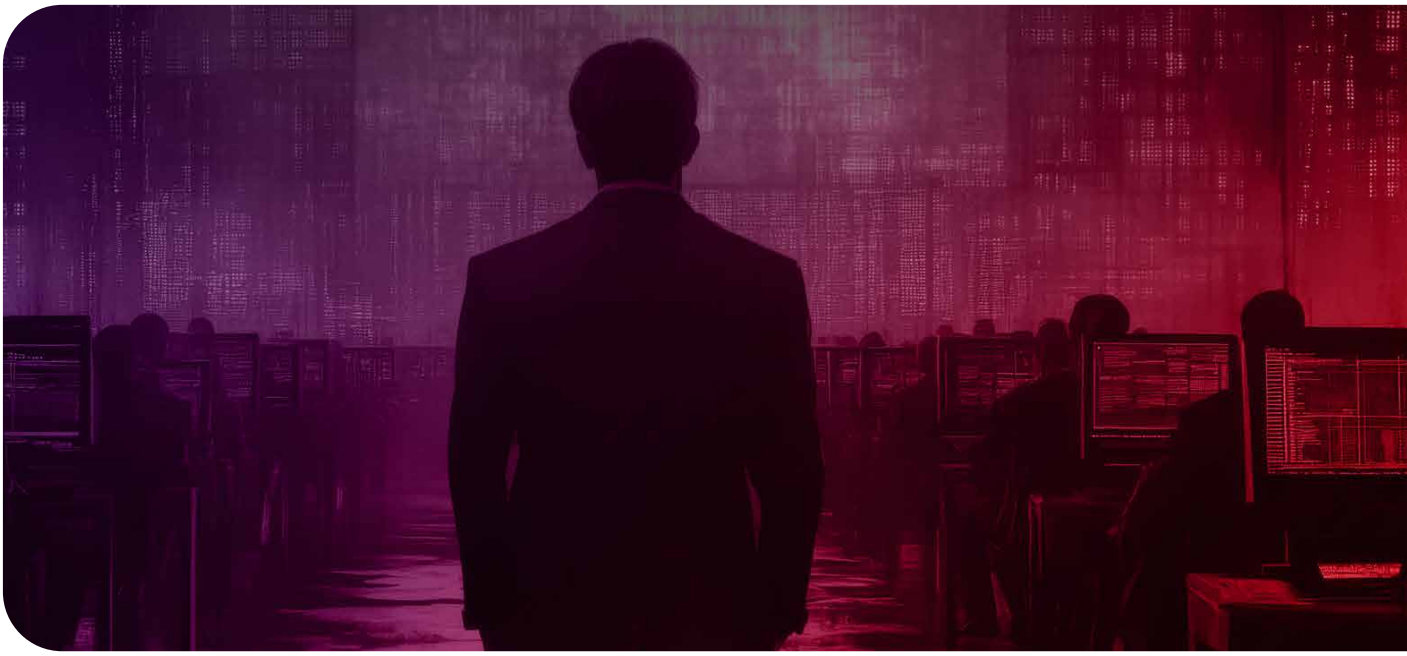
The advent of hacktivism and cyber-espionage has profoundly altered traditional conflict paradigms, especially in India-Pakistan relations. Hacktivist groups – informal collectives engaging in politically motivated cyber-attacks – and nation-state-aligned threat actors such as Transparent Tribe (APT36) play pivotal roles in shaping the digital battlefield. These operations blend cybercrime, geopolitical signaling, and social manipulation, making cyber warfare a central feature in contemporary conflicts between these two nuclear-armed neighbors. The world of conflict has expanded. It's no longer just about borders and bombs – today, cyber-attacks are as strategic as missile strikes.

This report presents a comprehensive researcher’s perspective on the evolving cyber threat landscape in the India-Pakistan conflict. It analyzes key actors, tactics, and hybrid warfare strategies while highlighting the implications of cyber operations for regional security and public perception.

Emergence and Evolution of Hacktivism

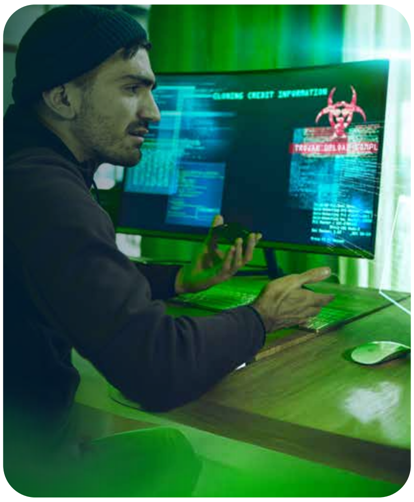
Cyber-warfare between India and Pakistan surfaced in the early 2000s, beginning with unsophisticated tactics such as website defacements led by groups like the Pakistan Cyber Army (PCA) and the Indian Cyber Army (ICA). Over the years, these operations evolved into state-aligned campaigns involving spear-phishing, data exfiltration, and disinformation warfare.

APT groups like APT36 (Transparent Tribe) emerged in the 2010s, using advanced malware such as Crimson RAT for espionage against Indian defense and government targets. In parallel, Indian threat actors like Patchwork countered with their espionage campaigns, albeit with different operational sophistication.



Spotlight: APT36 – The Digital Operative of Pakistani Espionage

APT36, also known as **Transparent Tribe, Mythic Leopard, or ProjectM, is Pakistan's most notorious Advanced Persistent Threat group.**



History and Tactics:

- **First active around 2013,** with sustained campaigns against Indian defense personnel and government entities.
- Primarily **spear-phishing:** fake government notices, military conference invites, and educational documents to lure victims.
- Notorious for **Crimson RAT, CapraRAT,** and recent Android surveillance tools.
- Masquerades behind educational platforms (learnfromhomenew[.]com), video conferencing apps, or fake recruitment forms.

Shift Toward Hybrid Warfare (2024–2025):

Historically focused on **espionage**, APT36 began **blurring lines between cyberwarfare and hacktivism:**

- Supported or coordinated campaigns with hacktivist allies (e.g., "Team Crack Codes", "Cyber Legion PK").
- Leveraged breach-style narratives destabilize **public perception,** not just steal information.

Motivations and Ideologies

APT36, also known as **Transparent Tribe, Mythic Leopard, or ProjectM, is Pakistan's most notorious Advanced Persistent Threat group.**

Political and Social Motivations:

The ambition to gather strategic intelligence or disrupt adversarial narratives is at the core of most cyber operations. Hacktivist forum members frequently voice strong discontent over governance failures, social injustices, and deeply rooted political or religious conflicts, often framing these grievances as catalysts for their actions. These ideologies fuel defacements, leaks, and targeted disinformation efforts, especially during real-world escalations like the **Pahalgam attack** and **Operation Sindoor.**

APT36 and the Pahalgam Scenario: The Tipping Point

On **April 22, 2025,** after the **terrorist ambush in Pahalgam,** resulting in casualties among Indian security personnel, the conflict spilled over into cyberspace.

APT36's Role in the Pahalgam Campaign:

Within hours, threat intelligence teams detected a sophisticated spear-phishing wave targeting:

- Indian journalists
- Defense personnel
- Telecom and tech sector employees

Key Indicators:

- **Malicious Excel & PowerPoint files** titled:
    - PAHALGAM SIDE FIGURED NUMBERS.xlam
    - Details of Pahalgam Martyr Report.ppam
- **Lure theme:** Intelligence updates, soldier lists, or public announcements.
- **Hosting domains** like:
    - pahalgamattack[.]com
    - operationpahalgam[.]info
    - **Shortened links via Bitly and Cuttly** to evade filters (e.g., bit[.]ly/alertpahalgam2025)
- **Payloads:** Embedded malware resembling Crimson RAT variants, likely customized for lateral movement in defense-related networks.

Why It Was Strategic:

- APT36 used Pahalgam as a "triggering event" – taking a real-world tragedy and turning it into a cyber intelligence operation + misinformation war.

Goals:

- **Harvest credentials** from defense & policy circles
- **Undermine trust** in Indian infrastructure by releasing fake "leaked" lists
- **Amplify outrage** through Telegram and X (Twitter) using doctored images and documents

This was **not just a phishing campaign – it was a cyber-psychological attack** wrapped in a digital flag of protest.

Why They Attack: Motivations and Messaging

Hackers aren't just trying to break into systems – they're trying to send messages, sway minds, or gather critical secrets. Their goals are:

Strategic Intelligence:

Espionage on defense, elections, and infrastructure.

Digital Retaliation:

Attacks responding to real-world events (like Pahalgam).

Perception Warfare:

Creating confusion, fear, and mistrust through misinformation.

Ideological Statements

Website defacements, slogans, leaks as forms of protest.

Who's Fighting: Hacktivist Groups and Alliances

This isn't a fight between just two countries. Dozens of groups – some organized, some opportunistic – have entered the fray.

Pro-Pakistan Groups (53 active)

- Kingsman
- Crack Codes
- Team White Cyber
- 7 Princes Lotus
- Cyber Volk
- Team Insane Pakistan

Pro-India Groups (18 active)

- N3XU5
- OneSec
- Red Eagle India
- SilentOne
- Kunthu Cyber Extractors
- INDIAN CYBER FORCE
- INDIAN CYBER MAFIA

They often **collaborate across borders** – from **Turkey, Indonesia, Algeria, Morocco, and Bangladesh** – creating a transnational network of ideological cyber warriors.

The View from the Top: Strategic Implications

APT36's evolution proves one thing: **espionage, influence, and perception operations are merging.**

Strategists must now prepare for:

- **Blended threat actors** who are part spy, part troll, part cyber warrior.
- **Nation-state proxies** (like hacktivist collectives) act as informal soldiers.
- **Active narrative management** to counter digital misinformation.

The Pahalgam operation wasn't a one-off. It was a **spark that lit a cyber fire.** Weeks later came **Operation Sindoor,** another wave of phishing and data leakage campaigns – this time piggybacking on Indian counter-insurgency actions in Kashmir.

APT36 (and its associates) used:

- **Lures themed around funeral processions, intelligence leaks, ceasefire documents**
- New domains like operationsindoor2025[.]in, tricolordocs[.]org
- Telegram disinformation via cloned handles of Indian journalists

The goal was clear: twist every national security event into a psychological disruption tool in cyber space.

From Hacktivism to Hybrid Warfare

APT36 has now evolved into a more dangerous hybrid threat actor, simultaneously acting as a state-sponsored spy, an ideological soldier, and a cyber instructor to the hacktivist underworld.

It no longer merely focuses on exfiltrating documents but aims to infiltrate the national psyche. It molds narratives, transforms PDFs into weapons, and wields hashtags like airstrikes.

As of May 2025:

- APT36 has **infrastructure alliances.**
- It's believed to supply tools, malware, and OSINT to groups like Crack Codes, Cyber Legion PK, and Kingsman
- It spoofs Indian media websites, uses fake bylines, and pushes manipulated news to stir conflict

It is now the maestro of digital manipulation, orchestrating cyber noise while hiding in signal.

The Misinformation Campaign Unfolds

Leading up to and following the attack, misinformation and propaganda were spread across social media, expertly manipulated by bot-farms linked to APT36. These campaigns falsely claimed the destruction of military infrastructure, spread fake news of casualties, and fabricated dramatic reports about drone strikes, missile launches, and military setbacks.

Key misinformation examples included:

- A viral claim about the Indian government advising citizens to turn off mobile location services, later debunked by the PIB Fact Check team.
- Fabricated videos of explosions at major infrastructure sites in India, like a fake explosion at Adani Port in Gujarat.
- False claims about the downing of Indian fighter jets, heavily amplified through fake accounts imitating legitimate news outlets like "Clash Report."
- The spreading of doctored footage from 2024, falsely attributed as a missile strike on New Delhi Airport.

These falsehoods weren't just isolated incidents but part of a well-orchestrated campaign designed to confuse, create fear, and influence public perception. The fake news had psychological and tactical implications, diverting attention from the real geopolitical moves happening on the ground.

The Connection to the Pahalgam Attack

The tipping point came when satellite imagery sourced from **US-based Maxar Technologies** revealed a surge in **high-resolution image orders for the Pahalgam region** in the weeks leading up to the April 2025 terrorist ambush. Multiple image requests were made between February 2 and 22, 2025, raising alarms about possible **pre-attack reconnaissance via commercial satellite feeds.**

While **Maxar Technologies has publicly denied that Business Systems International Pvt Ltd (BSI)** – a Pakistani geospatial firm – placed any of these specific orders for Pahalgam, the incident drew scrutiny due to BSI's prior history and Maxar's broader presence in conflict zones. Maxar's satellite outputs have been extensively used during high-stakes geopolitical crises, including the **Israel-Hamas conflict** and the **Russia-Ukraine war,** leading to renewed debate over the **accessibility and accountability of commercial satellite intelligence.**

BSI itself remains controversial; its founder had previously been convicted for exporting sensitive equipment to Pakistan's nuclear agency, suggesting the firm's potential as a proxy for strategic surveillance. Although no direct evidence currently ties BSI to the Pahalgam imaging orders, the **timing and pattern of requests** has heightened concerns about the **misuse of satellite data by third-party intermediaries** for military or terrorist planning.

The Dark Web Explodes – 8th May to 11th May 2025

The battle moved beyond email. On **May 8th,** reports of **dark web leaks** tied to APT36's operations began to surface. The **threat actor** claimed to sell **access** to sensitive Indian entities, including the **Election Commission of India (ECI)** and **Kulgaon Badlapur Municipal Council.** The data included **highly sensitive records** – a goldmine for disinformation campaigns aimed at destabilizing Indian democratic institutions.

By **May 9th,** a new leak appeared, this time involving **ExportersIndia.com.** APT36 claimed to have **shell access to the platform's backend,** exposing the personal details of **12.7 million users.** Such data could fuel a **multifaceted disinformation campaign** targeting Indian businesses and political figures.

But that was not all. On **May 11th**, a series of **APT36's phishing domains** surfaced, targeting Indian government entities with URLs like:

- hxxp://www.sindoor[.]website/
- www.sindoor[.]world
- www.sindoor[.]airforce

APT36 wasn't just running phishing operations – it was running **information warfare operations.**

The india.db Leak – 11th May 2025

On **May 11th**, an account named **“Cyber_Bapu”** leaked **sensitive documents** associated with the **Sindh police**. Another adversary named “Cyber_Berkkut” also leaked documents that allegedly contained **classified details** on Indian PsyOps operations, specifically **covert military strategies, narrative control,** and **cross-border activities** related to Kashmir.

These images – consisting of defaced government websites, leaked login pages, and screenshots of internal dashboards – were circulated across public forums, signaling an escalation in cyber disruption tactics.

Escalation – 12th May 2025

On May 12, 2025, the cyber conflict intensified with the circulation of a leaked document – allegedly from the Pakistan Air Force (PAF) – on Telegram channels associated with pro-India cyber actors. The document claimed that Indian Air Force strikes on Bholari Airbase, conducted during Operation Sindoor, caused significant infrastructure damage and resulted in 52 casualties among PAF personnel.

Note: Individuals linked to AnonSec were reportedly arrested concerning cyber operations related to Operation Sindoor. However, no official disclosures about their identities or affiliations have been made public.

Expanded Threat Assessment:

The Operation Sindoor campaign largely centered around phishing, DDoS, website defacement, and application layer attacks – relatively inexpensive tactics

Application Layer Attacks: An Overlooked Vector

While volumetric attacks at the network layer grab headlines, **Application Layer (Layer 7) attacks** are often overlooked yet can be significantly more disruptive and precise. These attacks target the **logic and functionality of web applications,** rather than attempting to flood bandwidth or network infrastructure.

Key Techniques Used

- **Web Defacement Attacks:** Hacktivist groups and politically motivated actors commonly exploit weak CMS setups or outdated plugins to alter website content, spreading misinformation or propaganda. Defacements are low-skill but high-impact tactics used to undermine public trust in institutions.
- **SQL Injection & Other Injection Attacks:** SQL injection allows attackers to manipulate backend databases through vulnerable input fields. In recent campaigns, such methods have been used to extract sensitive citizen records, login credentials, and government data.
- **Cross-Site Scripting (XSS):** Reflected and stored XSS attacks have been used to redirect users to phishing pages or silently capture session tokens, enabling further compromise of user accounts and admin portals.
- **Credential Stuffing & Authentication Abuse:** Credential stuffing attacks leverage breached data to target public portals with weak authentication mechanisms. This technique helped actors access restricted services without triggering traditional intrusion alerts.
- **Application Layer DDoS (HTTP Floods):** These attacks were launched against login portals, government dashboards (e.g., NIC, GSTN, GeM), and citizen-facing services. By exploiting HTTP/HTTPS protocols (e.g., GET/POST floods, slowloris), attackers were able to:
    - Exhaust server threads and memory.
    - Deny legitimate user access.
    - Bypass network-layer DDoS protections, as the traffic often appears legitimate.

Why These Attacks Matter

Unlike traditional DDoS attacks that rely on volume, **application-layer attacks are stealthier and require fewer resources,** making them **harder to detect and mitigate.** Their effectiveness indicates:

- A **deliberate targeting strategy.**
- Awareness of **specific application weaknesses.**
- Use of **open-source or basic tooling** paired with reconnaissance to cause maximum disruption.

Limited Attack Scope: Focus on Defacement, DDoS, and Phishing Over Ransomware or Data-Wipers

There are several likely reasons for the absence of more destructive attack vectors:

- Limited Capability and Infrastructure: Hacktivist groups involved (e.g., AnonSec, Team Insane Pakistan, Sylhet Gang-SG) often operate with minimal resources, relying on publicly available tools rather than custom malware. Many are decentralized and lack persistent access to advanced infrastructure like command-and-control panels or encrypted loaders.
- Low-Cost, High-Impact Strategy: The focus was on symbolic disruption rather than long-term damage or financial gain. Public defacements, credential leaks, and site outages generate media buzz and public anxiety without requiring sophisticated tooling.
- Coordination Without Integration: The campaign appeared coordinated but not deeply integrated. Hacktivists and APTs like APT36 may have shared narrative goals, but operational execution remained distinct, with hacktivists supporting through disruptive noise.

Intent to Signal, Not Destroy: These actors aimed to assert presence in the cyber conflict arena, leveraging national crises like Pahalgam to project influence, particularly through Telegram and social media hashtags like #OperationSindoor.

Hacktivist Tactics: Simplicity, Symbolism, and Visibility Over Sophistication: Most modern hacktivist groups tend to focus on low-effort, high-visibility attacks like DDoS and website defacement rather than advanced techniques such as ransomware or complex malware operations. This is mainly due to their limited technical capabilities and access to plug-and-play tools that make simple attacks easy to execute. Since their motives are often ideological rather than financial, they aim for short-term impact and media attention rather than long-term infiltration or monetary gain. Additionally, advanced attacks require significant resources, stealth, and infrastructure – something many hacktivist groups lack due to budget and logistical constraints. They also seek to minimize the risk of attribution and legal consequences, avoiding actions that could classify them as cybercriminals rather than activists. As a result, they prioritize quick, symbolic actions over technically complex or prolonged campaigns.tion.

Reconnaissance Activity and Indicators of Pre-Attack Mapping

Indicators suggest a phase of technical reconnaissance likely occurred before or alongside DDoS and phishing deployments:

- **Botnet-Based Probing:** High-volume automated scans were observed targeting login panels, form endpoints, and APIs of Indian public sector and defense-linked websites. These scans appeared coordinated, suggesting using botnets for service fingerprinting (e.g., identifying CMS, tech stack, and open ports).
- **Open Service Enumeration:** Attackers likely used search engines like Shodan or Census and web crawlers to map public-facing Indian government domains, SSL misconfigurations, open FTP, and unauthenticated APIs were likely flagged as potential vectors.
- **Recon Embedded in DDoS Campaigns:** Some DDoS activity probed application logic, mimicking typical user behaviors – this suggests Layer 7 DDoS was dual-purpose, serving both disruption and information gathering.
- **OSINT Use:** Similar to the campaign against pahalgamattack[.]com, evidence suggests that OSINT tools were used to discover forgotten or misconfigured subdomains – an essential recon technique for hacktivist playbooks.
- **Dark Web Activity (Late April – Early May):**

  Telegram channels like GhostSec_SouthAsia and darknet markets like OnionLeaks[.]net hosted chatter about Indian infrastructure, login dumps, and mentions of tools tailored to Indian government domains. No hard evidence of weaponized zero-days existed, but recon scripts, DDoS kits, and India-specific results were actively shared. Conversations suggested repackaging old malware families like Crimson RAT using newer delivery vectors (e.g., OneNote phishing, MSI payloads).

  The authenticity of both documents remains unverified, yet their release played into a broader psychological warfare narrative, strategically timed to exploit public fear and damage military credibility on both sides. This reflects a classic APT36 tactic – leveraging real-world geopolitical events to inject false or semi-true narratives into public discourse.

  ⓘ Analyst Note: These campaigns mirror prior APT36 tactics documented by SentinelLabs, often combining leaked content with forged military memos to stir unrest.

  As these documents proliferated through social media and cybercriminal channels, one conclusion became apparent: **Pahalgam was no longer just a physical battleground – it had become the launchpad of a full-scale cyber influence campaign.**

References

1. **SentinelLabs** – Transparent Tribe (APT36) | Pakistan-Aligned Threat Actor Expands Interest in Indian Education Sector
2. **Check Point Research** – The Evolution of Transparent Tribe's New Malware

A New Dimension to Geopolitical Struggles

Geopolitical actions continued to unfold in parallel with cyber activities. Reports confirmed that Pakistan's armed forces had established substantial defensive fortifications near Kasur, a region historically tied to terror groups such as Lashkar-e-Tayyaba. These fortifications, captured through satellite footage, hinted at an escalation in preparedness for a potential conflict to counter any Indian military advance.

At the same time, Pakistani authorities began to act against those spreading misinformation on their soil. In Lahore, multiple arrests were made, including an officer from a federal agency, under the PECA Act for spreading false information.

The Real-time Impact: Drone Attacks and Escalation

By May 2025, a concerning shift was observed in cyber threats targeting India's border infrastructure. Drone deployments, once limited to reconnaissance or isolated kinetic actions, are now being leveraged as components of **sophisticated cyber-physical campaigns**. Incidents along the India-Pakistan border – including aerial surveillance over civilian areas such as Ferozepur – coincided with targeted cyber intrusions into **CCTV networks, municipal alert systems, and digital infrastructure,** highlighting a growing focus on coordinated disruption of critical services.

This marks the emergence of **integrated hybrid attacks,** where physical systems are used not for direct conflict but to mask or amplify cyber operations. These drone sightings increasingly appear to be distractions – tools to test perimeter responses. At the same time, malware quietly infiltrates backend systems, creating a **false sense of urgency or system overload** to support silent digital incursions.

A more alarming trend is the **collaboration between state-aligned adversaries and cybercriminal ecosystems,** particularly **ransomware groups** from Eastern Europe and the Middle East. Intelligence reports and dark web chatter suggest the development of A**I-assisted malware,** capable of evading traditional detection systems by autonomously adjusting behaviors. These tools are often modular, deployed through toolkits sold in **cybercrime-as-a-service (CaaS)** marketplaces, and enhanced through partnerships with hacktivist groups that provide ideological cover or local targeting expertise.

Furthermore, **adversaries are now adopting machine learning (ML) algorithms** to **scan networks, identify unpatched vulnerabilities, and prioritize high-value targets** such as SCADA systems, defense logistics, and satellite-linked communication platforms.

In recent months, **Middle Eastern hacktivist groups** have reportedly joined forces with South Asian collectives to launch **multi-vector cyber assaults** that blend DDoS attacks, defacements, ransomware payloads, and psychological operations. These campaigns often coincide with geopolitical flashpoints, using misinformation, fake alerts, and synthetic media to destabilize the information ecosystem and create **false public narratives.**

India has initiated **counter-drone protocols and cyber surveillance enhancements,** but the evolving threat landscape necessitates a strategic pivot. Cyber defense efforts must now focus on:

- **Real-time anomaly detection across physical-digital interfaces** (e.g., drones triggering firewall evasion attempts)
- **Threat intelligence fusion between government CERTs and private-sector SOCs**
- **Preemptive monitoring of CaaS forums and ransomware alliances**
- **Deception and honeypot networks to trap AI-driven malware during reconnaissance stages**

In this new paradigm, **cyber warfare is no longer about isolated hacks or singular breaches –** it's a convergence of automation, ideology, and organized cybercrime, operating at the intersection of disruption and deception.

The Role of Hacktivists: Operation Sindoor and Beyond

As cyber warfare and misinformation campaigns escalated, hacktivist groups like those aligned with Pakistan's military intelligence began to intensify their efforts. Hackers initiated various operations, most notably "Operation Sindoor," which falsely claimed retaliatory cyberattacks launched by Indian hackers in response to military actions.

These operations, spearheaded by cyber groups acting under the guise of nationalism, created a fog of uncertainty, with misattribution and fear-mongering tactics designed to stoke further conflict. Misinformation on platforms like Twitter and Telegram helped blur the lines between state-sponsored and independent hacker activities.

The Escalation of Military Cyber Operations

By May 12, 2025, another alarming development emerged: a covert operation – "Operation TRINETRA" – was uncovered. This operation involved staging a false flag terror attack, falsely implicating Pakistan's ISI and the Resistance Front (TRF), to leverage diplomatic support from the U.S. It also involved the use of PSYOPS and botnets to manipulate international perception of the conflict.

During all this, India launched deep airstrikes during "Operation Sindoor," targeting high-value sites inside Pakistan, including areas like Muridke and Bahawalpur. The success of these strikes marked a significant moment in the conflict, demonstrating India's growing ability to project power and influence through kinetic and cyber operations.

Countermeasures and Responses

The evolving threat landscape, underscored by Operation Sindoor and TRINETRA, reveals critical vulnerabilities in civilian and defense digital infrastructure. If left unchecked, such threats could escalate into national command systems, essential chains of supply, and disruptions of public trust. To counter these hybrid threats, India must implement a layered and proactive defense strategy:

- **Enhanced Monitoring of Battlefield Management Systems (BMS) and CCTV Infrastructure:** Given the high risk of surveillance and manipulation, critical operational systems must be continuously monitored and hardened against cyber intrusions.
- **Increased Surveillance and Real-time Threat Reporting:** Government and defense agencies must institutionalize centralized incident reporting frameworks that allow real-time detection, analysis, and response to ongoing cyberattacks.
- **Proactive Public Advisories and Vulnerability Alerts:** Frequent bulletins to organizations and critical sectors should warn of emerging threat vectors such as domain spoofing, spear-phishing, and disinformation campaigns.
- **Collaborative Intelligence Sharing:** Partnerships between government agencies, CERT-In, law enforcement, and private cybersecurity firms should be expanded to enable faster attribution, cross-platform data correlation, and disruption of threat actor infrastructure.
- **Public Awareness and Digital Hygiene Campaigns:** To reduce social engineering success rates, nationwide awareness initiatives are essential. These must target public and sensitive sector employees with training on phishing recognition, data protection, and misinformation identification.

Futuristic Threat Trajectory – What We Can Expect

- **Escalation of Hybrid Warfare:** The coordination of APTs + hacktivists may become standard operating doctrine, blending espionage with disruption. Future events (e.g., elections, border tensions, or terror attacks) could trigger coordinated digital offensives.
- **More Stealth, Less Noise:** As visibility increases, adversaries may move from DDoS/defacements to data exfiltration, supply chain compromise, and misinformation campaigns using deepfakes and AI-generated content.
- **Weaponization of Leaks:** Expect increased leak-based blackmail, especially against critical sectors (defense, telecom, healthcare) with documents selectively shared on Telegram/dark web to sow distrust.
- **Cross-Regional Coordination:** Future cyber offensives may involve informal collaborations among actors from Turkey, Bangladesh, Indonesia, or North Africa, aligned more by ideology than formal alliances.
- **Adversarial AI:** The rise of AI-powered threat actors introduces a new paradigm. Potential use cases include:
  - Automated phishing kits with context-aware bait.
  - AI-assisted vulnerability scanning to find zero-days faster.
  - Synthetic media generation (deepfakes) for disinformation.
  - Conversational malware using large language models to interact and socially engineer victims.

  As defenders adopt AI, attackers will too, setting the stage for an AI vs. AI arms race in cybersecurity.
- **Supply Chain Attacks:** Modern digital supply chains are deeply interconnected, making them attractive targets for attackers. Adversaries may poison open-source libraries, infiltrate third-party service providers, or exploit hardware and firmware to gain persistent access. Incidents like SolarWinds and 3CX demonstrate how a single compromise can cascade across thousands of downstream organizations.
- **Less dependency on Vulnerability Exploitation:** Rather than relying solely on zero-days, adversaries now exploit misconfigurations, weak credentials, and token theft, often targeting human trust through phishing, MFA fatigue, or impersonation. They also use living-off-the-land techniques with legitimate tools like PowerShell or RDP, favoring stealthy, persistent access over high-profile exploits – a shift toward “low noise, high return” intrusions.

Securing the Future – Strategic Recommendations

For Government & Critical Infrastructure:

- **XDR with Recon Detection:** Deploy detection mechanisms for early reconnaissance indicators (e.g., Shodan hits, unusual botnet pings, URLScan trails).
- **Application-Layer DDoS Mitigation:** Harden Layer 7 endpoints – especially login forms, search queries, citizen services – with rate limiting, CAPTCHAs, and web application firewalls.
- **Dark Web Monitoring:** Constant surveillance for chatter related to exploits, IOCs, domain impersonations, or leaked credentials.
- **Threat Simulation:** Regular purple team exercises simulating phishing + lateral movement based on real TTPs (e.g., Ares RAT and LOLBins).

For Private Sector & Individuals:

- **IT Hygiene –** hardened systems, up-to-date patches/security fixes, endpoint security solutions
- **Identity protection –** periodic user account reconciliations, applying the principles of segregation of duties and least required privileges, additional controls for privileged user accounts and service accounts etc
- **Credential Hygiene:** Enforce MFA, monitor for breached credentials, and educate users on phishing lures like .lnk or .ppam attachments.
- **Phishing Resilience:** Simulate spear phishing and OneNote/MSI lure campaigns in employee training.
- **Zero Trust Implementation:** Avoid implicit trust in internal systems – verify every connection.
- **Security Monitoring and Incident Response –** Intelligence-driven Security Operations

Conclusion

The Pahalgam incident and Operation Sindoor powerfully remind us of the complexities of modern warfare, where digital and physical battlegrounds are increasingly intertwined. The role of APT36 and hacktivist groups in shaping public perception, sowing discord, and supporting military operations reveals the high stakes of cyber warfare in regional conflicts.

As both nations continue to grapple with the consequences of their actions, the lessons learned from the Pahalgam attack and Operation Sindoor offer critical insights into the future of warfare. In the future, the lines between truth and misinformation and defense and offense will become increasingly difficult to discern.

About Seqrite

Seqrite is a leading enterprise cybersecurity solutions provider. With a focus on simplifying cybersecurity, Seqrite delivers comprehensive solutions and services through our patented, AI/ML-powered tech stack to protect businesses against the latest threats by securing devices, applications, networks, cloud, data, and identity. Seqrite is the Enterprise arm of the global cybersecurity brand, Quick Heal Technologies Limited, the only listed cybersecurity products and solutions company in India.

We are the first and only Indian company to have solidified India's position on the global map by collaborating with the Govt. of the USA on its NIST NCCoE's Data Classification project. We are differentiated by our easy-to-deploy, seamless-to-integrate comprehensive solutions providing the highest level of protection against emerging and sophisticated threats powered by state-of-the-art threat intelligence and playbooks backed by world-class service provided by best-in-class security experts at India's largest malware analysis lab – Seqrite Labs. We are the only Indian full-stack company aligned with CSMA architecture recommendations, offering award-winning Endpoint Protection, Enterprise Mobility Management, Zero Trust Network Access, and many more. Seqrite Data Privacy management solution enables organizations to stay fully compliant with the DPDP Act and global regulations.

Today, 30,000+ enterprises in more than 70 countries trust Seqrite with their cybersecurity needs. For more information, please visit: www.seqrite.com

SEQRITE

Solitaire Business Hub, Office No. 7010 C & D, 7th Floor,
Viman Nagar, Pune - 411014, India. www.seqrite.com