IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

State-Sponsored Cyber Operations & Cyber Terrorism: Sectoral Targeting, Legal Challenges, and The Indian Perspective

Vidhan Dilip Gambhire[1], Ass. Prof. Sandhya Kaprawan[2]
Student, University Department of Information & Technology (M.Sc. Cybersecurity)[1]
Assistant Professor, University Department of Information & Technology (M.Sc. Cybersecurity)[2]
University of Mumbai, Mumbai, Maharashtra, India

Abstract: *The proliferation of digital technology has fundamentally altered national security paradigms, expanding threat vectors beyond traditional data breaches to encompass the targeting of critical infrastructure. This study analyzes the strategic escalation of cyber threats into sectoral targeting, specifically focusing on vulnerabilities within energy, finance, healthcare, and government systems. By examining state-sponsored operations and cyber terrorism through an India-centric lens, this paper conducts a qualitative analysis of high-profile incidents, including the 2020 Mumbai power outage, the 2022 AIIMS ransomware attack, the 2018 Cosmos Bank cyber heist, and the 2019 Kudankulam nuclear facility intrusion. Furthermore, it addresses the convergence of transnational organized crime and cybersecurity through an examination of hybrid threat networks operating from Myanmar. The research demonstrates the specific inadequacies of current legal frameworks namely the Information Technology Act 2000 and the Unlawful Activities (Prevention) Act in addressing the complexities of attribution and state-proxy engagements, concluding with targeted policy recommendations for strengthening national cyber defense and critical infrastructure resilience.*

Keywords: State-Sponsored Cyber Operations; Cyber Terrorism; Sectoral Targeting; Critical Infrastructure Security; Cyber Warfare; Attribution Challenges; India Cybersecurity; Advanced Persistent Threats (APT); Cyber Espionage; Industrial Control Systems (ICS); Legal Framework; IT Act 2000

I. INTRODUCTION

The proliferation of digital infrastructure has led to an increase in the importance of cyberspace as a critical dimension of modern warfare, often referred to as the fifth domain of warfare, in addition to land, sea, air, and space. Additionally, cyber warfare activities are no longer limited to data breaches or financial fraud but now involve critical infrastructure such as energy, finance, healthcare, and government sectors, which could potentially result in a wider impact. In cyberspace, threats are not only limited to data breaches but also directly threaten lives by compromising critical infrastructure.

Within this context, state-sponsored cyber warfare and cyber terrorism have emerged as major instruments of strategic influence. The terms state-sponsored cyber warfare and cyber terrorism refer to activities conducted or supported by nation-states to achieve political, military, or economic objectives, or activities using cyber means to cause disruption, terror, or damage to infrastructure in general.

The salient feature of the evolving cyber warfare landscape is the shift towards sectoral cyber warfare, wherein attackers target a particular domain to maximize impact. The recent Mumbai Power Outage (2020), AIIMS Delhi cyber attack (2022), Cosmos Bank cyber attack (2018), Kudankulam Nuclear Power Plant cyber attack (2019), and Myanmar-based cyber scam attack (2023-present) indicate a pattern of strategically targeting diverse sectors.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

From an Indian perspective, the implications of state-sponsored cyber warfare and cyber terrorism are an increase in exposure to multidimensional cyber threats owing to geopolitical tensions and international criminal organizations. At the same time, the growing complexity of cyber warfare activities poses a major challenge in terms of legal response. The difficulty in attributing state-sponsored cyber attacks and a lack of legal framework to address such threats serve as a major impediment in countermeasures.

The growing complexity of state-sponsored cyber warfare and cyber terrorism highlights a need for a more integrated and policy-centric approach to address evolving challenges in cyber security.

II. LITERATURE REVIEW

Scholarship surrounding cyber warfare historically anchors itself to the strategic maneuvers of established geopolitical powers, charting the evolution of state-funded collectives from opportunistic exploiters to architects of sustained, systemic disruption. Foundational doctrines most notably the *Tallinn Manual 2.0* [3] offer essential architectures for mapping international law onto digital conflicts, particularly regarding the friction points of state proxy accountability and the pervasive fog of attribution. Concurrently, institutional threat monitors like NATO's CCDCOE [3] and the UNODC [4] have extensively cataloged the escalating migration of these offensives toward critical infrastructure, tracking persistent breaches across power grids, financial switches, and medical databases.

Despite this robust global catalog, a pronounced geographical and legislative void persists. While emerging inquiries acknowledge the mutation of conventional cybercrime into "hybrid threats" scenarios where state tolerance overlaps with the logistical muscle of transnational criminal syndicates localized academic scrutiny remains surprisingly sparse. Specifically, contemporary literature fails to adequately superimpose these shifting operational paradigms onto India's unique domestic vulnerability matrix. There is a distinct lack of synthesis regarding how systemic sectoral targeting outpaces the jurisdictional boundaries of regional statutes, such as the Information Technology Act of 2000 [1]. This research intervenes directly in that academic blind spot, structurally analyzing the intersection of global proxy strategies, industrialized cybercrime, and localized infrastructural realities within the Indian subcontinent.

III. RESEARCH METHODOLOGY

To effectively deconstruct the evolving architecture of state-sponsored offensives and hybrid terror networks aimed at the Indian subcontinent, this research grounds itself in a qualitative, comparative case-study framework. Rather than relying on purely theoretical modeling, the investigative rigor here is driven by the synthesis of high-fidelity secondary intelligence. The data pool is constructed by dissecting open-source intelligence (OSINT) artifacts, parsing the operational narratives buried within government threat appraisals, analyzing forensic incident post-mortems[11], and critically interpreting current statutory architectures.

The analytical engine of this paper is a structured comparative matrix applied across distinct infrastructural pillars: energy grids, financial switches, medical logistics, and nuclear facilities[12]. Each infrastructural breach is systematically interrogated against a rigid set of operational variables: the specific nature of the targeted asset, the forensic footprint of the suspected proxy actor, the granular mechanics of the modus operandi, and the ultimate strategic fallout. To trace the tactical heartbeat of these intrusions, the Lockheed Martin Cyber Kill Chain is deployed not merely as a descriptive tool, but as an active analytical overlay. This allows the study to expose hidden structural symmetries—specifically detailing how disparate threat actors handle initial reconnaissance, establish deep network persistence, and ultimately execute their payloads.

Finally, the research shifts from forensic dissection to legislative critique. It juxtaposes these verified operational realities against the prevailing Indian statutory environment, aggressively interrogating the blind spots within current cyber legislation to forge actionable, policy-oriented countermeasures.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

IV. CONCEPTUAL FRAMEWORK

Typically, state-sponsored cyber operations can be grouped into three major strategic functions: espionage, sabotage, and influence operations. As mentioned above, these three functions often blur into each other.

Espionage refers to any unauthorized access or extraction of sensitive information without immediate disruption to the target systems. The objective of any cyber espionage is intelligence gathering for the long term. The operations often target government agencies or organizations with sensitive information. The SolarWinds attack is a classic example of a cyber espionage attack. In the attack, which occurred in 2020, hackers gained access to many different government agencies and corporate networks using compromised software updates.

On the other hand, sabotage refers to any cyber attack aimed at disrupting or destroying target systems. Sabotage often results in physical damage to the targeted systems. Sabotage is different from cyber espionage in that its objective is immediate disruption. The Stuxnet attack is a classic example of sabotage. In the attack, which occurred in 2010, hackers used malware targeting industrial control systems at Iranian nuclear plants. The attack resulted in physical damage to the centrifuges at the Iranian nuclear plant.

Influence operations refer to any cyber attack aimed at influencing perceptions or decision-making processes. Traditionally, these operations often target information or psychological operations. However, these operations often blur with disruption attacks aimed at creating panic or confusion. The WannaCry ransomware attack is an example of a disruption attack aimed at creating global panic. The attack occurred in 2017 and resulted in widespread disruption of healthcare services globally.

The three operations mentioned above demonstrate the evolution of cyber operations into an integrated whole aimed at influencing strategic operations.

V. SECTORAL TARGETING: CRITICAL INFRASTRUCTURE AND CASE-BASED ANALYSIS

The nature of cyber threats has evolved significantly, shifting from isolated data-centric attacks to targeted operations against critical infrastructure. Increasingly, such attacks are capable of disrupting essential services and, in certain contexts, posing direct risks to human life. This shift has led to the emergence of sectoral targeting, where adversaries strategically focus on specific domains to maximize disruption, economic impact, and geopolitical influence.

Energy Infrastructure: Power Grid Vulnerabilities

The energy infrastructure forms a basic aspect of national infrastructure wherein cyber attacks possess a potential to cause immediate large-scale disruption, which could be felt in multiple domains.

The 2020 Mumbai Power Outage can be cited as a salient example of vulnerabilities in power grid infrastructure.

Year: 2020.

Target: Power grid infrastructure (load dispatch centres and transmission systems).

Actor (Suspected): China-linked APT group (RedEcho).

Attack Type: Infrastructure intrusion / potential sabotage.

Incident Overview and Strategic Context:

The 2020 Mumbai Power Outage occurred in an environment of high geopolitical tension, which led to an analysis of potential strategic signaling via cyber attacks. Although the attribution of the attack remains disputed, assessments by threat intelligence agencies revealed malware associated with China-associated APT Groups in Indian Power Sector networks. This highlights how infrastructure can be used not only for disruption but also to demonstrate potential and intent.

Operational Methodology (Modus Operandi):

The attack pattern is typical of advanced persistent threats. The initial stages of the attack probably involved a mapping of grid systems, including vulnerable points of entry. The attackers would then gain entry into networks connecting

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

information technology systems with operational technology systems. Inadequate network segmentation would allow them to gain persistence. Possible scenarios for manipulating load dispatch systems would be initiated from this position, leading to disruptions in power transmission.

Impact and Consequences:

The impact of the attack is a blackout in a metropolitan area. A blackout is a widespread disruption affecting transportation, information technology, financial systems, and daily activities. The blackout is a direct consequence of a cyberattack on an energy sector organization. In this regard, disruptions in power transmission have a direct impact on services such as hospital services, which are critical to human life.

Observed Vulnerabilities and Security Gaps:

The attack on the grid system revealed several security gaps, primarily in information technology/operational technology segregation. The absence of adequate real-time monitoring of grid systems is a security gap. Inadequate intrusion detection systems would allow attackers to gain persistence, increasing the risks associated with undetected threats.

Financial Infrastructure: Cyber-Enabled Economic Operations

The financial sector forms a critical pillar of national stability, where cyber intrusions can lead not only to monetary loss but also to systemic disruption and erosion of public trust. In the context of state-sponsored cyber operations, financial institutions are increasingly targeted as instruments of economic warfare.

The Cosmos Bank cyberattack (2018) represents a significant case of coordinated cyber intrusion into India's banking infrastructure.

Year: 2018.

Target: ATM switch systems and SWIFT transaction infrastructure.

Actor (Suspected): North Korea-linked Lazarus Group.

Attack Type: Financial cyber operation / economic warfare.

Incident Overview and Strategic Context:

The Cosmos Bank incident involved a highly coordinated attack that enabled unauthorized withdrawals across multiple countries within a short time frame. The scale and synchronization of the operation suggested a well-resourced and organized threat actor. Such attacks are often linked to state-sponsored groups seeking to generate revenue to bypass economic sanctions, indicating a shift from traditional cybercrime toward state-driven financial operations.

Operational Methodology (Modus Operandi):

The attack followed a structured approach typical of advanced cyber operations. Attackers initially infiltrated the bank's internal network, likely through compromised credentials or vulnerable systems. This was followed by lateral movement to the ATM switch, which controls transaction authorization. By manipulating the switch, attackers were able to bypass authentication protocols and authorize fraudulent withdrawals. Simultaneously, unauthorized transactions were executed through the SWIFT network, enabling rapid transfer of funds across international accounts.

Impact and Consequences:

The attack resulted in losses exceeding ₹94 crore through coordinated ATM withdrawals and international fund transfers. Beyond financial damage, the incident exposed systemic vulnerabilities in banking infrastructure and highlighted the potential for large-scale disruption of financial systems. Such operations undermine trust in digital banking mechanisms and demonstrate how financial networks can be exploited for strategic economic gain.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

Observed Vulnerabilities and Security Gaps:

The incident revealed significant weaknesses in internal network security, particularly in access control mechanisms and monitoring of critical systems such as the ATM switch. Insufficient real-time anomaly detection allowed attackers to execute large-scale transactions without immediate detection. Additionally, gaps in SWIFT transaction monitoring and delayed response mechanisms contributed to the scale of the attack. These vulnerabilities underscore the need for stronger network segmentation, continuous monitoring, and enhanced transaction validation frameworks.

Healthcare Infrastructure: Cyber Terrorism and Human Impact

Healthcare infrastructures represent a part of critical infrastructures that is arguably among the most sensitive, where disruptions caused by cyber attacks have direct implications for human lives and well-being. Unlike most infrastructures, disruptions caused by cyber attacks in this sector are not limited to operational or financial consequences. Instead, they have direct implications for patient safety.

The cyber attack on AIIMS Delhi in 2022 is an exemplar of the vulnerability of healthcare infrastructures to targeted cyber attacks.

Year**:** 2022.

Target: Hospital information systems and patient databases.

Actor (Suspected): Foreign state-linked actors (China-linked entities suspected).

Attack Type: Ransomware / service disruption.

Incident Overview and Strategic Context:

The cyber attack on AIIMS Delhi triggered a disruption in services, affecting patient registration, diagnostic services, and medical record access. As a leading public healthcare institution in India, this attack underlines the systemic risks associated with digital dependency in critical infrastructures. The selection of healthcare infrastructures is part of a general trend in cyber attacks, which increasingly target infrastructures where disruptions are likely to have significant societal and psychological repercussions. In this regard, this attack reinforces concerns over cyber terrorism.

Operational Methodology (Modus Operandi):

The attack pattern is typical of ransomware-based cyber attacks on extensive institutional infrastructures. The attacks are likely to have started with a compromise of credentials or exploitation of vulnerable endpoints. Subsequently, the attackers exploited their accesses to deploy ransomware on critical databases, impairing their functionality, which resulted in restricted access to patient information systems.

Impact and Consequences:

The consequences of the cyber-attack include significant disruptions in the hospital's operations, which entailed delays in treatment and processing of patient records on a manual basis. The hospital also suspended critical operations due to the inability to access digital medical records. The case is a classic example of the consequences of cyber-attacks on healthcare infrastructure, which began with a technological disturbance but ultimately impacted human lives in a physical manner, similar to the trajectory of cyber threats on physical and social entities.

Observed Vulnerabilities and Security Gaps:

The cyber-attack on the hospital revealed various security risks and vulnerabilities related to endpoint security and the overall security posture of the hospital's network. The hospital did not have adequate real-time monitoring tools in place, which facilitated the rapid proliferation of the ransomware. The hospital also failed to implement a robust backup strategy for its centralized digital infrastructure.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

Nuclear and Critical Infrastructure: Strategic Espionage

The nuclear infrastructure is one of the critical infrastructures that is categorized under the most sensitive category. In this category, the intrusion is seen to have strategic and security implications in the long term. In comparison to the other critical infrastructures, the intrusion is seen to be focused on the acquisition of intelligence rather than the disruption of the infrastructure.

The Kudankulam Nuclear Power Plant intrusion in the year 2019 is a notable example of the critical infrastructure intrusion.

Year: 2019.

Target: Nuclear facility administrative network.

Actor (Suspected): North Korea-linked Lazarus Group (DTrack malware).

Attack Type: Espionage / data exfiltration.

Incident Overview and Strategic Context:

The identification of the DTrack malware in the Kudankulam Nuclear Power Plant raised significant concerns regarding the security of the infrastructure. Although the official announcements claimed that the infrastructure was not impacted, the presence of the malware in the administrative infrastructure indicates the potential for the acquisition of intelligence.

Operational Methodology (Modus Operandi):

The attack appears to be consistent with a targeted intrusion pattern, which is normally characteristic of an advanced persistent threat. The malware used for gaining initial access was most likely used in spear-phishing campaigns or via compromised endpoints. Once the malware gained access, it allowed for persistence and assisted in data collection. Although operational networks were isolated, unauthorized access to administrative systems could prove beneficial in gaining further insight into system architecture and operational processes.

Impact and Consequences:

Despite the limited immediate operational impacts, the breach has significant strategic implications. Access to internal systems can provide attackers with access to sensitive information that could be used for further attacks or intelligence gathering. Information gained includes details about the configurations of the systems and the organizational structure. The breach thus underscores the need for cybersecurity to extend beyond protecting operational systems to the supporting infrastructure within nuclear plants.

Observed Vulnerabilities and Security Gaps:

The breach exposed the vulnerabilities that exist in endpoint security measures, employee awareness, and segmentation of networks for both administrative and operational networks. Overreliance on administrative networks without effective monitoring measures increases the risks of attacks going undetected. Moreover, the breach exposed the inability of existing security measures to identify advanced persistent threats. To counter these risks, there is a need to strengthen access control measures, enhance monitoring measures, and employee awareness.

Government and Defence Systems: Espionage and Psychological

Government and defense systems are key targets within the cyber domain, where intrusions have the potential to impact national security, strategic planning, and military action. In comparison to other domains, cyber intrusions within this domain are primarily aimed at intelligence gathering, surveillance, and psychological warfare.

In recent years, several instances of cyber attacks against Indian defense personnel and government agencies have been reported, focusing on phishing and social engineering attacks.

Year: Ongoing (multiple incidents reported over time).

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

Target: Defence personnel, communication systems, and government databases.
Actor (Suspected): Pakistan-linked APT groups (e.g., APT36).
Attack Type: Espionage / social engineering.

Incident Overview and Strategic Context:
These operations are often conducted as part of broader intelligence-gathering efforts aimed at extracting sensitive information related to military activities and government functioning. The use of cyber means allows adversaries to conduct surveillance without direct confrontation, making such operations a key component of modern hybrid warfare strategies. The repeated targeting of defence personnel indicates a sustained and focused approach toward exploiting human and institutional vulnerabilities.

Operational Methodology (Modus Operandi):
The attack pattern typically begins with reconnaissance of potential targets, including identification of individuals through open-source information. This is followed by spear-phishing campaigns, impersonation tactics, or the use of malicious applications designed to appear legitimate. Once access is obtained, attackers may extract sensitive data, monitor communications, or attempt to escalate privileges within the network. These operations rely heavily on social engineering rather than purely technical exploitation.

Impact and Consequences:
The potential consequences of the attacks could be the exposure of confidential military information, the exposure of military strategies, and unauthorized access to confidential communication channels. Such attacks, no matter how limited they are, could have a significant effect on the security of the country. In addition, the attacks could contribute to psychological pressure on the institutions, thus affecting the decision-making processes.

Observed Vulnerabilities and Security Gaps:
The primary vulnerabilities in this sector arise from human factors, including susceptibility to phishing and inadequate cyber awareness. Weak access control practices, use of unsecured communication platforms, and lack of regular security training further increase risk. The absence of continuous monitoring and delayed detection mechanisms can allow attackers to maintain access for extended periods. Addressing these gaps requires a combination of technical safeguards and institutional discipline.

Hybrid Threats: Cybercrime and Human Trafficking
A new dimension of cyber threats is the convergence of cybercrime with transnational organized crime, including human trafficking, which has resulted in hybrid threat models beyond the scope of traditional cybersecurity paradigms. The cyber scam networks emanating from Myanmar (2023-present) are a notable example of such hybrid threat models, especially against Indian nationals.
Year: 2023–present.
Target: Global individuals (financial fraud victims) and trafficked individuals (forced operators).
Actor (Suspected): State-tolerated transnational criminal networks.
Attack Type: Cybercrime + human trafficking (hybrid threat).

Incident Overview and Strategic Context:
Several scholarly studies have documented the existence of organized scam compounds in certain regions of Myanmar, where individuals from different countries, including India, are lured under false pretenses of job opportunities to engage in cyber fraud activities. The organizational scale of such operations suggests a degree of tolerance or ineffective action from local authorities. The threat model, therefore, suggests a paradigm shift from traditional

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

cybercrime to a more organized, industrialized, and scaled-up version of cybercrime, possibly within a transnational criminal ecosystem.

Operational Methodology (Modus Operandi):

The process typically begins with recruitment through fraudulent online job offers, particularly targeting individuals seeking employment abroad. Victims are transported across borders and confined within controlled environments. Once inside, they are coerced into conducting cyber fraud activities such as investment scams, phishing campaigns, and social engineering operations targeting victims globally. These operations are managed centrally, with predefined scripts, technological infrastructure, and performance monitoring.

Impact and Consequences:

The consequences of such operations are multifaceted. First, they result in financial fraud on a large scale, affecting victims from different countries. Second, they involve grave violations of human rights, including forced labor and confinement of individuals from different countries. In the context of India, this is a dual threat, both from a cybersecurity threat vector and a consular dimension, considering that Indian nationals are exploited as part of such cybercrime ecosystems.

Observed Vulnerabilities and Security Gaps:

The continued existence of these networks points to weaknesses in cross-border law enforcement, immigration control, and the monitoring of fraudulent recruitment schemes. In addition, the use of encrypted communication platforms and the existence of a decentralized financial system make these operations difficult to detect. In order to address these vulnerabilities, there is a need for international cooperation and the integration of cybersecurity with other law enforcement strategies.

VI. STATE ACTORS AND STRATEGIC INTENT

It is important to understand that state-sponsored cyber activities are not conducted in a random manner but are closely associated with overarching national interests. In the current geopolitics of the world, cyberspace can be considered an operational domain in which nations seek to fulfill their intelligence, economic, and military agendas. In this regard, it can be argued that cyber activities are an extension of a country's foreign policy, which allows nations to achieve their strategic interests without engaging in a direct military conflict.

The cyber strategy of **China** reflects a long-term strategy in which critical infrastructure targeting plays a pivotal role. The activities of China-associated hacking groups reflect a strategy to gain persistent access to critical infrastructure sectors such as energy and telecommunications. Although such activities are not conducted to disrupt or destroy infrastructure, they are often conducted in a manner to pre-position potential activation in case of a geopolitical crisis. This strategy reflects a broader objective of strategic deterrence.

North Korea has established a cyber strategy in which financial activities play a central role. The cyberattacks conducted by North Korean hacking groups, such as those conducted on banking and cryptocurrency platforms, reflect a strategy to generate financial resources and evade economic sanctions.

The nature of **Pakistan's cyber activities** is mostly focused on defense and government organizations, with an emphasis on intelligence gathering and psychological warfare. Phishing and social engineering attacks on military personnel suggest a tactical approach with a focus on gathering sensitive information and affecting decision-making processes. These attacks are often linked with regional security issues.

In terms of nuclear infrastructure, cyber attacks are mostly focused on strategic intelligence gathering. Attacks on sensitive facilities suggest an attempt at gathering intelligence on the architecture, processes, and technological prowess of the targeted systems. These attacks are often stealthy and long-term strategic efforts rather than tactical attacks with a short-term goal of destruction.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

The case of Myanmar offers a different scenario, with a focus on the integration of cyber attacks within a tolerant or unregulated environment. The development of large-scale cyber scam networks originating from Myanmar illustrates this point. These networks, often involving trafficked individuals, suggest a hybrid scenario of cybercrime, organized crime, and a tolerant state.

VII. RESULT & ANALYTICAL FINDINGS

Deconstructing the selected infrastructural breaches exposes a stark operational reality: cyber offensives directed at the Indian subcontinent have wholly abandoned opportunistic disruption in favor of sustained, architecturally complex siege strategies. Forensic cross-examination of these incidents reveals a high degree of sectoral hyper-specialization among state-aligned threat actors. Proxy groups infiltrating energy networks such as the entities suspected in the Mumbai grid anomaly[5] prioritize dormant persistence and geopolitical leverage. Conversely, actors breaching financial architectures, evidenced by the Cosmos Bank heist[7], engineer their intrusions strictly for scalable economic extraction to bypass international sanctions. Intrusions into defense perimeters remain hyper-focused on silent, long-haul intelligence vacuums.

Applying the Cyber Kill Chain overlay to these seemingly disparate attacks unravels an unsettling operational symmetry. Regardless of the infrastructural target or the suspected state sponsor, these campaigns share a rigid, industrialized anatomical structure. Adversaries consistently weaponize extended reconnaissance phases and exploit human-layer vulnerabilities to establish deep-rooted network persistence, often dwelling undetected for months before initiating any disruptive payload execution.

Perhaps the most critical divergence from traditional threat modeling is the empirical validation of hybrid cybercrime convergence. The Myanmar-based syndicates[8] represent a fundamental mutation in the regional threat landscape. The forensic footprint points away from isolated hacking cells and directly toward state-tolerated, industrialized fraud factories. The logistical reality of these operations relying heavily on the physical trafficking of forced operators through convoluted international transit corridors spanning Nepal, Dubai, and China—demonstrates a terrifying fusion of digital exploitation and transnational human trafficking. On the domestic front, this analysis repeatedly indicts a trifecta of systemic defensive failures across Indian critical infrastructure: fractured IT/OT network segregation, a chronic absence of real-time behavioral anomaly detection, and an unyielding susceptibility to sophisticated social engineering.

VIII. DISCUSSION

The empirical footprint detailed in our analysis directly corroborates broader international scholarship regarding the strategic patience of state-sponsored actors. Where previous geopolitical literature such as the macro-level incident analyses published by NATO CCDCOE[3] has theorized a global pivot toward stealth and persistent access over immediate kinetic disruption, this study firmly anchors that theoretical shift within the harsh reality of Indian infrastructure. The adversaries probing India's energy grids and financial switches are not acting in a vacuum; they are executing the exact long-haul intelligence and strategic pre-positioning doctrines warned about in contemporary cyber-conflict studies.

Crucially, the granular data reinforces the systemic legal inadequacies fiercely debated in modern cyber-law circles. The attribution paralysis heavily scrutinized within the *Tallinn Manual 2.0* [3] is not merely a theoretical friction point; it is a tactical mechanism actively weaponized against the Indian state. By deliberately laundering their intrusions through convoluted proxy networks and compromised third-party infrastructure, these state actors maintain plausible deniability. They maneuver comfortably within the gray zone, operating well below the strict thresholds of armed conflict that traditional international law demands for a definitive response.

The defining academic contribution of this research, however, lies in its exposure of the hybrid threat mutation. Traditional cybersecurity paradigms stubbornly treat state-level cyber warfare and transnational organized crime as parallel, non-intersecting tracks. By forensically mapping the Myanmar syndicates[8] where digital exploitation is

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

inextricably fused with the physical trafficking of human operators across international borders this paper violently disrupts that siloed thinking. The significance of this finding is absolute: the Indian national security apparatus is no longer combating isolated hackers or traditional state proxies. It is confronting industrialized, state-tolerated digital fraud factories operating at an unprecedented scale.

Consequently, the defensive posture prescribed by current siloed policies is fundamentally misaligned. Treating these multi-front intrusions as isolated technical anomalies or localized criminal acts represents a catastrophic strategic failure. Confronting this evolving, multi-dimensional threat architecture requires abandoning fragmented defenses in favor of an aggressive, unified synthesis of hardened network resilience, modernized domestic legislation, and proactive international diplomacy

IX. MODUS OPERANDI: PATTERNS IN STATE-SPONSORED CYBER OPERATIONS

State-sponsored cyber attacks, though varied in their target, have been found to follow a predictable and replicable attack lifecycle. The attack lifecycle refers to a series of activities that begin from intelligence gathering to the final execution. The attack lifecycle is generally divided into several stages, such as reconnaissance, initial access, persistence, lateral movement, and execution. Instead of referring to specific attacks, these stages refer to a well-planned process that has been developed to ensure maximum efficiency while maintaining a low profile.

The process begins with a stage called reconnaissance, in which adversaries aim to gather detailed information about their target. In the Indian context, this is clearly observed in attacks against defense personnel, in which adversaries are found to be gathering intelligence through open-source intelligence gathering and social engineering. This stage is critical because it is said to determine the precision of all future activities.

Following this stage, adversaries aim to gain initial access to their target. In several cases, such as the AIIMS Delhi cyber attack, adversaries are found to gain initial access through compromised credentials or vulnerable systems. This stage is still found to be one of the most exploited vulnerabilities, owing to a mix of both technical and psychological factors.

Following initial access, adversaries aim to ensure persistence, which helps them maintain their position for a longer period. In cases of attacks against critical infrastructure, such as power grid attacks, adversaries are found to have developed malware that remains undetected within their systems.

The next phase is the lateral movement phase, where the attackers increase their position in the network to reach the critical systems. This is well demonstrated in the financial sector attacks, such as the one on Cosmos Bank, where the attackers moved from the initial entry point to the critical transaction system. The lack of proper network segmentation is the biggest contributor to this phase.

Finally, the whole operation is completed with the execution phase, where the attackers achieve the objective of the operation. This could include the disruption of the system, the exfiltration of data, or financial fraud. The AIIMS ransomware attack is a classic case of the execution phase through system disruption, financial sector attacks through fraud, and infrastructure through possible sabotage or control.

From the above phases, it is evident that the common thread is that the attackers' success is not based on the technology used but rather on the ability to maintain access without being detected. This clearly indicates that the attackers are not engaging in a random activity but a well-planned operation. This is a clear indication that security is paramount in all sectors.

INDIA'S CYBER THREAT LANDSCAPE

India's cyber threat environment is characterized by a complex array of risks from state-sponsored actors and transnational cyber networks. In this context, India's rapidly growing digital economy with increasing critical infrastructure is faced with a multi-front cyber threat environment in which various sectors are concurrently targeted for strategic, economic, and intelligence-driven purposes.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

A key dimension of this threat environment is the sustained threat to critical infrastructure sectors like energy, banking, and defence. In this context, the threat to the energy sector is sustained by the growing digitization of the sector's infrastructure and operational systems, which increases susceptibility to external intrusion and potential disruption. Similarly, in the financial sector, sustained cyber operations target sophisticated cyber operations to exploit banking systems, financial transactions, and digital payment systems. In the defence sector, cyber operations focus more on intelligence gathering through repeated attempts to compromise personnel, communication systems, and sensitive information.

These sector-specific cyber operations are not in isolation from one another but are connected in a larger context of sustained cyber operations against India. In this context, India is faced with a sustained cyber threat environment in which adversaries attempt to conduct cyber surveillance for long-term strategic advantages.

In this context, India has put in place various institutional mechanisms to address this threat environment, including the Indian Computer Emergency Response Team (CERT-In) and the National Critical Information Infrastructure Protection Centre (NCIIPC). The former is tasked with serving as a national nodal agency for coordinating incident response and dissemination of various advisories to stakeholders, whereas the latter is tasked with protecting critical information infrastructure sectors like power, banking, telecommunications, and government systems.

Despite all these institutional structures in place, challenges still remain. The level of sophistication of cyber threats often outstrips the capabilities of existing response measures. The level of coordination between agencies in real-time, as well as a lack of shared proactive intelligence on threats, still creates vulnerabilities. In addition, the growing involvement of private organizations in critical infrastructure creates a further layer of complexity in terms of overall security.

Within this context, India's position in terms of cybersecurity will need to move from a purely reactive response to a proactive approach in terms of anticipating threats and building resiliency. This will involve coordination between agencies, as well as real-time monitoring and response capabilities.

LEGAL FRAMEWORK AND LIMITATIONS

India's defensive posture is critically undermined by an anachronistic statutory architecture. The primary legal scaffolding governing digital conflict the Information Technology (IT) Act of 2000[1], loosely augmented by the Unlawful Activities (Prevention) Act (UAPA)[2] was drafted for an era of localized, opportunistic cybercrime. When deployed against the industrialized, state-sponsored warfare detailed in the preceding case studies, this framework immediately fractures.

Interrogating the IT Act reveals severe operational blind spots. Section 66F[1] attempts to codify "cyber terrorism" to penalize the unauthorized penetration of national infrastructure. Yet, its definitional scope remains dangerously ambiguous, lacking the granular legal triggers necessary to classify let alone prosecute complex state-proxy engagements. Section 69 might grant sweeping domestic surveillance and interception powers, but it remains a bluntly reactive tool, functionally impotent as a deterrent against offshore Advanced Persistent Threats (APTs). Similarly, Section 70 attempts to legally ring-fence "protected systems" such as power grids and financial nodes. However, as the forensic realities of the Mumbai grid anomaly and the Cosmos Bank heist explicitly demonstrate, simply designating an asset as "protected" on paper does absolutely nothing to bridge the enforcement vacuum when the aggressor operates from across a heavily militarized border.

Attempts to shoehorn these modern digital offensives into the Unlawful Activities (Prevention) Act have proven equally disastrous. The UAPA was forged to dismantle physical terrorist syndicates; applying its statutes to decentralized, transnational cyber operations relies on strained interpretive leaps rather than solid jurisprudence. The most glaring casualty of this legislative stagnation is the absolute absence of "cyber warfare" as a recognized legal classification within Indian law. By failing to legally distinguish between a localized financial hack and a coordinated, state-funded economic assault on the banking sector, the current statutes inadvertently provide diplomatic cover for foreign adversaries

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

The Unlawful Activities (Prevention) Act (UAPA) provides a broader legal framework intended to address threats to national security, which could include cyber terrorism. Yet again, such a connection to cyber incidents remains indirect and often relies on interpretive mechanisms.

Despite all these provisions, legal gaps remain. Notably, there remains a lack of formal definition or inclusion of cyber warfare as a legal entity in India. This creates confusion in the categorization of large-scale cyber warfare activities perpetrated by states, particularly in those situations where activities overlap between cybercrime and acts of war. Additionally, the issue of jurisdiction remains a major challenge in dealing with cyberattacks, which often come from outside national borders. The legal instruments in place demonstrate a low level of effectiveness in dealing with external state actors.

These gaps highlight the need for legal reform in light of the changing nature of cyber threats, particularly in distinguishing between criminal, terrorist, and state-sponsored activities.

Ultimately, this definitional void creates a state of perpetual jurisdictional paralysis. The legal instruments currently available to Indian authorities demand clear, localized attribution to function effectively. Against state-tolerated hybrid syndicates operating out of Myanmar, or hostile state proxies laundering their routing through international servers, India's domestic laws are effectively disarmed. The current statutory environment does not deter state-sponsored cyber operations; its profound ambiguity actively invites them.

ATTRIBUTION CHALLENGES IN CYBER OPERATIONS

Attribution is one of the most complex and unsolved puzzles in the study of state-sponsored cyber operations. The process of establishing the real origin of an attack is inherently complex because of the prevalence of obfuscation techniques and the international nature of cyberspace. In the context of cyber warfare operations, attribution is often the weakest link in the cyber domain.

From a technical point of view, attackers often use proxy servers, virtual private networks, or compromised computers located across multiple countries to hide their tracks. As a result, tracing the real origin of an attack is often not possible, with the attackers often leaving false clues about their origins.

The problem is further complicated by false flag operations wherein attackers often attempt to masquerade as other groups or nations. As a result, attribution is often false, which further increases tensions between nations.

From a legal point of view, the Tallinn manual 2.0 provides guidelines for establishing state responsibility only if there is evidence of control or direction. However, in practice, establishing such evidence is extremely difficult, particularly if the attack is conducted via proxies or loosely affiliated groups.

The above factors have a significant effect on attribution since the lack of reliable attribution undermines deterrence and allows both state and non-state actors to act with impunity in cyberspace.

POLICY RECOMMENDATIONS

India's cybersecurity strategy must evolve from a fragmented and reactive posture to a cohesive and intelligence-driven strategy that is capable of effectively countering state-sponsored cyber warfare and cyber terrorism. The increased focus on critical infrastructure attacks underscores the importance of considering cybersecurity an integral part of the country's security strategy rather than a mere technological issue.

The development of a National Cyber Warfare Doctrine is a critical requirement that must clearly define the thresholds of a cyber attack and distinguish between cybercrime, cyber terrorism, and state-sponsored cyber warfare. The absence of such a classification creates ambiguity in the response strategy, especially when the target is critical infrastructure such as the power grid or the country's nuclear facilities.

The security of critical infrastructure sectors such as the energy sector, financial sector, healthcare sector, and the country's nuclear facilities must also be enhanced. This includes the segregation of information technology and operational technology networks, constant monitoring, and security audits to ensure the early identification of

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 13, April 2026 Impact Factor: 8.2

vulnerabilities. This is particularly important so that the critical infrastructure is not compromised by advanced threat actors over a prolonged period of time.

India must also look to enhance the coordination of real-time threat intelligence through the integration of various agencies such as CERT-In, NCIIPC, and the defence cyber agencies. A unified framework for the sharing of threat indicators between the private and public sectors must also be developed.

In the financial sector, cyber attacks have to be viewed as a potential threat of economic aggression, for which transaction monitoring has to be improved. In the defense and government sectors, addressing the threat of phishing and social engineering attacks involves addressing the human factor through strict cyber discipline, training, and communication.

In a legal context, there is a need for reform to address jurisdictional issues and a general lack of a framework for cyber warfare. Strengthening international cooperation could be useful.

In light of the difficulty of attribution, a structured approach to addressing cyber attacks, which combines technical forensics with intelligence, is recommended for India. At the same time, the rise of hybrid threats such as cyber crime syndicates in Myanmar underlines the need for a coordinated response to such threats.

In conclusion, a comprehensive approach is required to strengthen India's response to cyber threats.

X. CONCLUSION

This analysis has empirically demonstrated that the cyber threat matrix confronting India has permanently shifted from decentralized, opportunistic criminality to industrialized, state-sponsored sectoral warfare. By cross-examining systemic breaches across the energy, financial, and defense vectors, this study established a distinct operational symmetry among adversaries specifically, a weaponization of the Cyber Kill Chain that prioritizes dormant network persistence and strategic pre-positioning over immediate kinetic impact. Furthermore, the forensic mapping of the Myanmar-based syndicates validated a critical mutation in the regional threat landscape: the absolute convergence of state-tolerated digital exploitation and physical, transnational human trafficking.

Consequently, this research confirmed the profound operational inadequacy of India's current statutory scaffolding. The Information Technology Act and the UAPA are structurally incapable of navigating the attribution complexities and state-proxy engagements inherent in these modern offensives. Relying on these anachronistic legal definitions to combat multi-dimensional, hybrid cyber warfare guarantees continued jurisdictional paralysis. Ultimately, the data dictates that to secure its critical infrastructure, India cannot rely on fragmented, reactive responses; it must forge a unified, proactive defense doctrine that legally, technically, and diplomatically addresses the harsh realities of modern proxy conflict.

REFERENCES

[1]. Government of India, "The Information Technology Act, 2000," Ministry of Electronics and Information Technology, New Delhi, India, 2000.
[2]. Government of India, "The Unlawful Activities (Prevention) Act, 1967," Ministry of Home Affairs, New Delhi, India, 1967.
[3]. M. N. Schmitt, Ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. Cambridge, U.K.: Cambridge University Press, 2017.
[4]. United Nations Office on Drugs and Crime (UNODC), "Comprehensive Study on Cybercrime," United Nations, Vienna, Austria, Feb. 2013.
[5]. Insikt Group, "China-Linked Group RedEcho Targets the Indian Power Sector Amid Heightened Border Tensions," Recorded Future, Somerville, MA, USA, Threat Analysis Report, Feb. 2021.
[6]. Kaspersky Global Research and Analysis Team (GReAT), "DTrack and the Lazarus Group: Targeted Attacks on Critical Infrastructure," Kaspersky Lab, Moscow, Russia, Sep. 2019.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 13, April 2026
Impact Factor: 8.2

[7]. Reserve Bank of India (RBI), "Cyber Security Incident – Cosmos Co-operative Bank Ltd.," RBI Financial Stability Reports, Mumbai, India, Aug. 2018.
[8]. Office of the United Nations High Commissioner for Human Rights (OHCHR), "Online Scam Operations and Human Trafficking into Southeast Asia," United Nations, Geneva, Switzerland, Aug. 2023.
[9]. Indian Computer Emergency Response Team (CERT-In), "National Cyber Security Threat Report 2022," Ministry of Electronics and Information Technology, New Delhi, India, 2023.
[10]. European Union Agency for Law Enforcement Cooperation (Europol), "Internet Organised Crime Threat Assessment (IOCTA) 2023," The Hague, Netherlands, 2023.
[11]. National Critical Information Infrastructure Protection Centre (NCIIPC), "Guidelines for the Protection of Critical Information Infrastructure," Government of India, New Delhi, India, V 2.0, 2019.
[12]. Mandiant Threat Intelligence, "Advanced Persistent Threat (APT) Groups: Operational Tactics and Strategic Targeting in the Indo-Pacific," Mandiant, Reston, VA, USA, 2023.