ISSN 23939729

CLAWS

No. 124

2026

MANEKSHAW PAPER

Tactical Military Approaches to Counter Terror in J&K

Navneet Bakshi

CENTRE FOR LAND WARFARE STUDIES

Field Marshal Sam Hormusji Framji Jamshedji Manekshaw, better known as Sam "Bahadur", was the 8th Chief of the Army Staff (COAS). It was under his command that the Indian forces achieved a spectacular victory in the Indo-Pakistan War of 1971. Starting from 1932, when he joined the first batch at the Indian Military Academy (IMA), his distinguished military career spanned over four decades and five wars, including World War II. He was the first of only two Field Marshals in the Indian Army. Sam Manekshaw's contributions to the Indian Army are legendary. He was a soldier's soldier and a General's General. He was outspoken and stood by his convictions. He was immensely popular within the Services and among civilians of all ages. Boyish charm, wit and humour were other notable qualities of independent India's best known soldier. Apart from hardcore military affairs, the Field Marshal took immense interest in strategic studies and national security issues. Owing to this unique blend of qualities, a grateful nation honoured him with the Padma Bhushan and Padma Vibhushan in 1968 and 1972 respectively.

Field Marshal SHFJ Manekshaw, MC
1914-2008

CLAWS Occasional Papers are dedicated to the memory of Field Marshal Sam Manekshaw

MANEKSHAW PAPER No. 124, 2026

Tactical Military Approaches to Counter Terror in J&K

Navneet Bakshi

Centre for Land Warfare Studies
New Delhi

Editorial Team : CLAWS

ISSN : 23939729

Centre for Land Warfare Studies
RPSO Complex, Parade Road, Delhi Cantt, New Delhi 110010
Phone +91-11-25691308 Fax: +91-11-25692347
Email: **landwarfare@gmail.com**, website: **www.claws.co.in**
CLAWS Army No.33098

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy-oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributions aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Disclaimer: The contents of this paper are based on the analysis of materials accessed from open sources and are the personal views of the author. The contents, therefore may not be quoted or cited as representing the views or policy of Government of India, or the Ministry of Defence (MoD), or the Centre for Land Warfare Studies.

Published in Bharat by

Sabre & Quill Publishers, New Delhi, India
www.sabreandquill.com/sabreandquill@gmail.com

Contents

Tactical Military Approaches to Counter Terror in J&K

Abstract

The principal objective of Security Forces (SF) in counter-terrorism (CT) operations is to eliminate terrorist threats, thereby creating a secure environment where the government administration can function unhindered. All elements of the operation, from logistics and communication to field manoeuvres, must cohesively support the primary mission (Institute for Defence Studies and Analyses, 2024[1]). This fundamental emphasis dictates that all associated activities, whether population control measures, area domination, IW or Perception Management, Op SADHBHAVNA, Civil–Military Relations, although important, are subordinated to the mission of neutralising terrorists and preventing the threat they pose. Time and resources are finite, operations are infinite. Thus, SF actions in CT operations are unambiguously mission-focused, intelligence-driven, and strategically aligned, upholding the principal objective.

To implement this objective, the collection of raw information and its analysis is the foundation of all SF actions (Institute for Defence Studies and Analyses, 2024). Intelligence is not confined to information alone; it involves synthesising varied sources, contextualising local vulnerabilities, and anticipating terrorist tactics, which must be rigorously analysed to determine terrorist intent, capability, and possible weaknesses (MI5, 2024[2]). Misjudgements in the synthesis of intelligence could severely

jeopardise mission outcomes. Thus, methodical purging of errors through exhaustive preparation and ongoing after-action investigation is accentuated at every echelon of command (Hughbank, 2010[3]). We can further state that the lack of thorough scrutiny of our own operations also significantly contributes to mission failure.

A thorough understanding of terrorist vulnerabilities necessitates multidisciplinary insight, blending technological acumen, psychological awareness, and socio-political expertise (United Nations Office on Drugs and Crime, 2023[4]). Fulfilment of this mission requires us to study the major vulnerabilities of terrorists, common and frequent errors in tactical operations, the core subject of analysis of this paper, which are inadvertently committed due to combat fatigue, long-term deployment, frequent turnover of personnel and other human factors (Petersen, 1972[5]; Heilbronn et al., 2022[6]).

Introduction

The security environment in Jammu and Kashmir (J&K) is characterised by a complex and evolving tapestry of political, social, and military challenges. Nestled in a geopolitically sensitive region, J&K has experienced extensive periods of insurgency, cross-border terrorism, and localised militancy, which pose enduring threats to regional stability and national security (Bhatia, 2024[7]). The area's unique topography, demography, and historical grievances contribute to a challenging operational environment for SF, necessitating tailored counterterrorism strategies that address both kinetic and non-kinetic domains (Kumar & Singh, 2023[8]).

In the evolving dynamics of counterterrorism operations within J&K, the holistic and truthful appraisal of tactical military operations is the foundation for guaranteeing security and strategic

victory. The dynamic and multilayered threat environment of J&K, characterised by asymmetric warfare, cross-border terrorism, and the utilisation of complex networks of Over Ground Workers (OGWs) along with the regional and religious subtleties, dictates a comprehensive and protracted analysis of tactical procedures (Choudhary, 2025[9]). Commanders must synthesise assorted intelligence inputs, extending from Human Intelligence (HUMINT) to Technical Intelligence (TECHINT), into comprehensible action plans, thereby guaranteeing that tactical choices are precisely directed and dynamically responsive to evolving threats (Sharma, 2024[10]). This intellectual thoroughness in decision-making is critical to aligning all lines of operation towards the dominant objective of neutralising terrorist threats, thus optimising resource utilisation and diminishing collateral penalties.

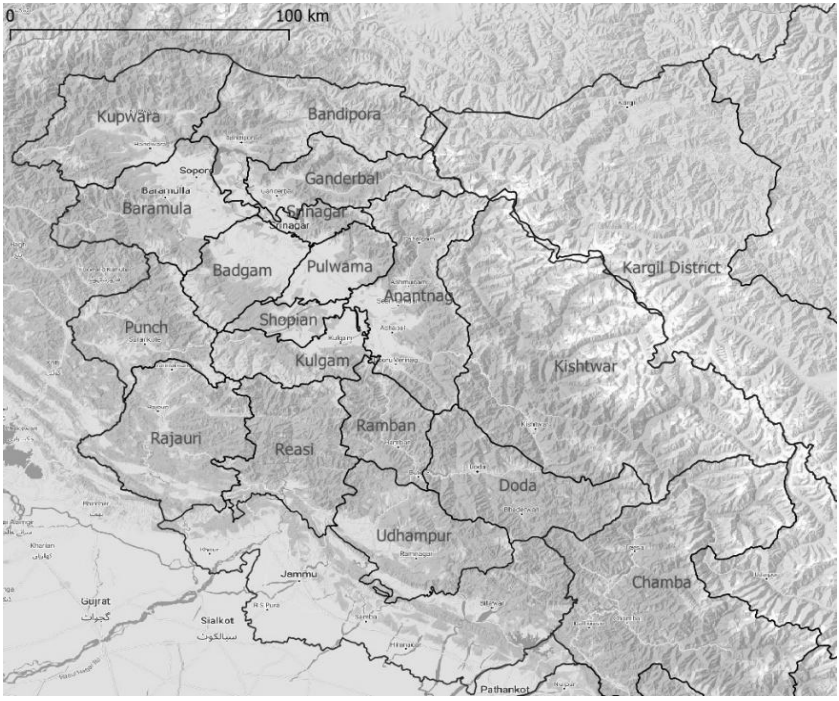


Figure 1: J&K

This further involves the key concepts integral to enhancing tactical efficacy of identifying terrorist vulnerabilities, including intelligence dependencies and behavioural stressors, and the recognition and mitigation of persistent operational errors such as the Errors of Convenience, Visibility, Attribution, and Justification (Patel & Raj, 2025[11]). By providing an orderly synthesis, this analysis endeavours to equip commanders and policymakers with actionable frameworks. These frameworks are essential for the sustained disruption of terrorist networks through disciplined analysis, error mitigation, and strategic agility (Malik & Hussain, 2024[12]).

We are all aware of the security threats in J&K and the current situation. Keeping the focus of this paper on the vulnerabilities of terrorists and operational errors would be appropriate. Thus, the security situation, background and terrain analysis have been restricted to keep the focus on the above aspects.

Vulnerabilities of Terrorists

Background

The security situation in Jammu and Kashmir (J&K) remains one of the most intricate and dynamic operational landscapes in the current counterterrorism situation (Bhatia, 2024). Over decades, the region has experienced persistent terrorism, cross-border infiltration, and a resilient network of Over Ground Workers (OGWs) (Kumar & Singh, 2023). The volatile terrain, coupled with perceived socio-political grievances, has provided fertile ground for terrorism to flourish, posing significant challenges to security forces and undermining regional stability (Bhatia, 2024). Over the years, terrorist transitioned from mass groups to decentralised, cell-based operations that rely heavily on sleeper cells and clandestine logistics (Choudhary, 2025). The terrain, mountains, dense forests, and urban sprawls are exploited for covert

movement and concealment, complicating interdiction efforts (Bhatia, 2024). This terrain advantage has dictated specialised tactics, persistent surveillance, and intricate intelligence operations to neutralise threats (Choudhary, 2025).

Figure 2: On CCTV, 2 Terrorists Seen Entering Workers' Camp In J&K Before Attack, NDTV

For terrorists operating away from overt state or organisational support, survival requires a precarious balance between concealment and the basic human necessities of food, shelter, and information. These constraints shape both their behaviour and contribute to their vulnerabilities (Akhtar, 1999[13]). Cut off from reliable supply lines, terrorists select one of two deficient subsistence approaches: blending into local populations where feasible or retreating completely into remote, inaccessible terrain (Arce & Sandler, 2005[14]). Assimilation can afford cover but demands continual vigilance imposing severe psychological strain; terrorists must perform social roles convincingly while suppressing

normal human instincts to trust and connect, a continuous cognitive burden that degrades decision-making (Silver et al., 2002[15]). Seclusion in mountains, forests, or urban ruins diminishes the risk of exposure. However, it imposes logistical privations and intense monotony, fostering attrition through illness, accidents, or desertion (United Nations Office on Drugs and Crime [UNODC], 2017[16]). This dilemma, between the realistic need for sustainment and the calculated imperative of secrecy and operations, compels risky patterns of behaviour that are exploitable (United States Department of Justice, 2014[17]). Since complete isolation is seldom sustainable, even the most cautious groups must intermittently re-enter population centres or establish connections to local networks for food, medical aid, and intelligence (Akhtar, 1999). The consequential signatures produce social and economic footprints that can be detected (Arce & Sandler, 2005).

For terrorists to endure, they require external covert support when operating in foreign lands. This means that they must always remain alert and active, leading to heightened stress and a lack of trust towards residents. Psychological stress, lack of trust, and the need to maintain secrecy degrade terrorist effectiveness over time (Akhtar, 1999). It is no surprise that terrorists often choose to stay and build hideouts in inaccessible terrain away from population centres. However, their need for sustenance and the human tendency to make contact frequently force them to compromise by staying or moving within population centres for short periods. This predisposition to avoid contact with all locals presents a challenge to their aim of remaining relevant and guaranteeing their survival, wherein lies their vulnerability, which is discussed in subsequent paragraphs.

Dependency on Unreliable OGW Network

Creating a reliable and accurate intelligence network is vital for providing early warning against SF operations in each area of responsibility (AOR) or the likelihood of large-scale operations in the general area (Duncan, 2023[18]). The intelligence must be precise, dependable, and timely to enable terrorists to respond proactively while also allowing enough time to react and conceal their activities. However, it must be noted that terrorists cannot afford to respond to every move made by the security forces, as doing so would be inefficient and lead to exhaustion and undue stress, reducing overall operational effectiveness. Terrorists must therefore selectively respond to threats and develop patience to avoid burnout and sustain long-term viability (Soomro et al., 2021[19]). To enable this, terrorists nurture OGW, who function with fluctuating degrees of contribution and risk, providing critical peripheral support (Kashmir Still Facing 'Over Ground Workers' Problem? 2025[20]). OGWs function as informants, guides, and vital sources of actionable intelligence for terrorist elements, allowing them to identify SF movements, potential targets, and safe routes for attacks or escape (Pandita, 2022[21]). These OGWs can be of different shades, ranging from active collaborators deeply embedded in terrorist networks to passive sympathisers who may unwittingly or reluctantly provide support, as listed below: -

- **Dedicated OGW**. Overground Workers (OGWs) who support the cause, motivated by an intrinsic ideological belief rather than any other external factors like Money or power, which could be incidental. Such intrinsically motivated support makes the OGWs trustworthy, and hence, they must be protected as valuable assets by the terrorists. Therefore, they cannot be endangered by frequent contact or routine tasks but would be activated for larger targeted incidents.

- **Disposable OGWs**. Every OGW need not necessarily be an unarmed soldier committed to the cause. Disposable OGWs, who exist at the fringes, tend to be more overt and visible to the SF due to their frequent activity. The motivation is money or power without any compulsions. They are routinely utilised for communication, sustenance and as informants.

- **Coerced OGWs**. These are the residents who have no option but to meet the demands of the terrorist for their own or their family's security. These are unreliable and for non-critical utilisation by the terrorists. They are the support of last resort for the terrorists.

- **Narco OGWs**. The local population, which is vulnerable and addicted to drugs, would also be of limited value to the terrorists. It must be appreciated that these individuals cannot be reliable and have reduced value. Thus, they could be utilised for emergency-based activity, especially to find isolated spots for a short duration and to move out of an Area safely, thereby avoiding SF patrols. Efforts to cultivate such OGWs as sources or to break their network are of limited value in the outcomes of CT operations for the SF.

Those with limited knowledge and who only perform routine tasks, like the last three identified above, are more susceptible to identification and are easier targets of the SF. Thus, although the identified and visible OGWs are easier to track, they are of limited value. Further, the modular structure, handler-based ecosystem, and cell-based modus operandi of terrorists in recent times have made even the dedicated OGWs of limited value for SF to eliminate terrorists.

Figure 3: Srinagar: Police arrested four Lashkar-e-Taiba OGW in Bandipora, The News Now

The survival instinct also forces the terrorists to avoid sources of TECHINT in their immediate vicinity. Lack of information on terrorist activity in an area does not indicate the absence of terrorists. Instead, it could suggest greater local support, leading to a lack of HUMINT, and terrorists avoiding the use of technological resources in the area. Increased presence by SF in such identified areas, thereby denying the area, could shake up the terrorists from these comfort zones and make them more vulnerable. Experiences in J&K have shown that the effort-benefit analysis of operations focused on breaking the OGW network is restrictive in achieving the primary aim. Thus, the more practical approach would be to displace and dislodge the terrorists from identified areas to render the OGW network ineffective and force the terrorists to rely on handlers across, thereby making TECHINT available.

Sustenance

To survive, acquiring sustenance becomes a challenge for the terrorists who operate in concealed environments. Long-term consumption of "hard scale" rations, such as military meal-ready-to-eat (MRE) packages, is unfeasible for human beings due to nutritional deficiencies and psychological impacts, which limit their viability beyond a few days (Hirsch & Kramer, 1993; U.S. Department of the Army, 1995[22]). Consequently, social interaction and fresh provisions are recurrently pursued, highlighting the need for hideouts to be stocked with appropriate supplies for protracted periods while being restocked regularly (UNODC, 2017). In practice, terrorists create drop-off points that are remotely located away from their hideouts and beyond the typical movements of SF, letting them to obtain provisions without substantial risk (Arce & Sandler, 2005[23]). These drop-off locations are often serviced by disposable OGWs, individuals who facilitate supply transfers but remain expendable to mitigate operational risk (Wikipedia, 2020[24]).

Figure 4: Hideout Busted at Gudder Encounter Site In J&K's Kulgam, Daily Excelsior -September 9, 2025

Further, the presence of hunters and other civilians who frequent these less accessible regions plays a pivotal role in maintaining supply chains, as their movements provide cover for the transfer of goods and reduce suspicion. Additionally, water, an essential and often scarce resource, compels terrorists to move frequently; thus, hideouts are typically established near natural water sources or in snowbound areas with reliable access to this precious liquid thereby vulnerable to analysed likelihood of detection by SF. Extensive searches of uncovered hideouts have yielded stocks of essential items such as cooking gas cylinders, food supplies including dry fruits and flour, water cans, and communication equipment, indicating the sustained logistical efforts needed to maintain survival in hostile environments (Business Standard, 2024[25]). In terms of cooking, gas cylinders are favoured as they provide a reliable heat source while generating minimal smoke, thereby reducing the likelihood of detection via aerial or ground surveillance. The necessity for proximity to water, limited availability of cover, and reliance on discreet cooking methods mean that viable hideout locations are limited in number and geographical range (Deccan Herald, 2024[26]).

Despite attempts to remain concealed, the concentration of critical survival resources and the repetitive use of known drop-off points produce identifiable patterns of movement and supply chain footprints. The geographic constraint increases vulnerability to targeted detection and neutralisation when intelligence is effectively analysed and applied by SF. Therefore, while sustaining operations in isolated hideouts is achievable, the constraints imposed by human biological needs and environmental factors create inherent vulnerabilities, shaping terrorist behaviour and susceptible to effective countermeasures (Arce & Sandler, 2005).

Compulsion to carry out Terrorist Initiated Incidents

Figure 5: Terror attack on bus in J&K, New Indian Express

The operational relevance of terrorists in conflict zones is deeply intertwined with their ability to execute Terrorist Initiated Incidents (TIIs) such as attacks on Security Forces (SF) and civilian targets. Without perpetrating such incidents, terrorists risk fading into obscurity, becoming merely armed individuals in remote areas with diminishing local support. This is because active engagement is a key metric by which both terrorist organisations and their sympathisers measure relevance and influence (Singh, 2023[27]). The compulsion to prove operational capability forces terrorists into a cycle where risks must be regularly taken.

The terrorists are put in a precarious position as they are compelled to undertake high-profile attacks to remain relevant. Each operation is fraught with the risk of exposure, either during the planning phase, due to informant leaks, or through detection by intensified intelligence and surveillance efforts by SF (Gupta, 2022[28]). As terrorist groups endeavour to sustain momentum and societal fear, the pressure frequently results in hurried or poorly

coordinated strikes, magnifying risks to themselves. This dynamic is exacerbated by the unremitting evolution of counterterror technologies and tactics, which increases the probability of identification and neutralisation (Verma, 2023[29]).

The local community's support plays a pivotal role in the terrorists' sustainability. Such support often centres on the terrorists' apparent capacity to challenge the state effectively (Ahmed & Singh, 2023). When TIIs diminish, locals gradually doubt the value and resilience of these groups, withdrawing logistical aid and moral endorsement. This loss of community legitimacy further compels terrorists to undertake hazardous operations to restore their stature. The resulting feedback loop is detrimental: the more risks they take to stay relevant, the more vulnerable they become to SF interception and loss of life.

In sum, the operational existence of terrorists is sustained by their ability to deliver impactful incidents, support from OGW networks, and community legitimacy, all of which are interconnected with risk-taking behaviour. Effective counterterrorist strategies rightly focus on security of all vulnerable assets and strengthen surveillance so as restrict free move by terrorists and increase the risk level of any operation. Degrading local legitimacy, augments the inherent vulnerabilities terrorists face in their quest for survival (Pandita, 2022; Ahmed & Singh, 2023).

Stress

The Area of Responsibility (AOR) under the watch of security forces (SF) is constantly surveyed through a well-established counter-terrorism grid, which includes frequent population control measures, resource management, CCTV camera setups, administrative moves, and active engagement with the local population. The presence of comprehensive intelligence gathering

means that terrorists cannot merely predict movements or patterns of SF activity, leading to a state of perpetual alertness and an inability to rest (Academia, 2024[30]). Consequently, terrorists are forced to take calculated risks to evade detection and capture, operating under extreme psychological and operational pressure due to the omnipresent surveillance (All Military Operations, 2025[31]).

Figure 6: Surveillance in J&K

In such a context, the agility and rapid mobilisation capacity of the SF can tip the balance. When security forces deploy quickly to surprise terrorists or catch them in unexpected locations, the chances of neutralising the terrorist significantly increase (Aken, 2024[32]). This dynamic validates the importance of rapid response teams strategically deployed to react swiftly to intelligence inputs, thereby restricting terrorists' ability to conceal themselves successfully (Aken, 2024). In sum, the constant overlap of

surveillance, community engagement, and rapid deployment creates an environment where terrorists face continuous operational risk, reducing their scope for manoeuvre and increasing their vulnerability to elimination. This creates undue and severe stress on the terrorist which unhinges him and reduces his capability.

Recognised Terrorist Vulnerabilities

The security environment in Jammu and Kashmir remains inherently volatile, marked by adaptive terrorist modalities, logistical challenges, and persistent external support. Understanding the intricate dynamics of terrorist vulnerabilities, including physical, intelligence, social, and psychological factors, is crucial for framing effective counterterrorism strategies. To summarise, vulnerabilities of the terrorists are as follows: -

- Intelligence Network based on unreliable sources.
- Sustenance through unreliable local population.
- Compulsion to undertake Terrorist Initiated Incidents.
- Propensity to take additional risks due to need to maintain relevance, fear, stress, and fatigue.

Common Operational Errors and Challenges

Background and Context

Through prolonged deployments, specifically when institutional knowledge is retained and contact occurrence is reduced, combat fatigue is a common experience among personnel. This condition often manifests as complacency, where personnel develop overconfidence in their knowledge and operational abilities. Such complacency can inadvertently lead to operational

errors because of reduced vigilance and underestimation of emerging threats (PMC, 2017[33]).

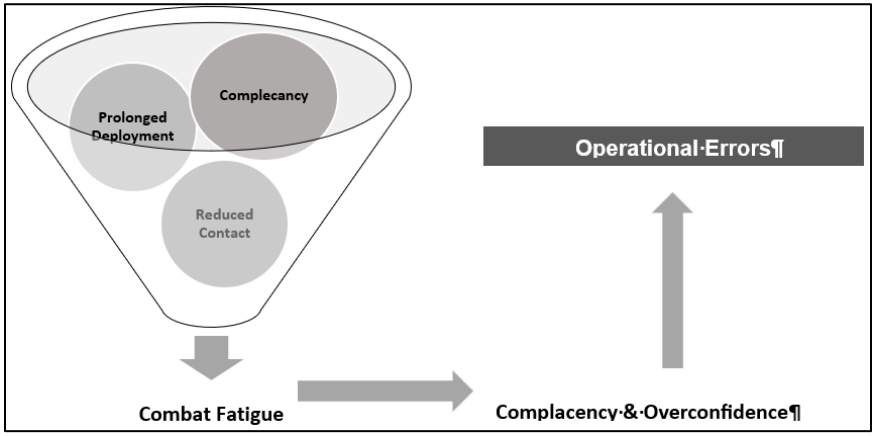


Figure 7: Combat Fatigue leading to Operational Errors

Moreover, the psychological impact of prolonged stress affects decision-making, resulting in diminished judgment and sluggish reaction times during critical operations (Legacy of Legions, 2024[34]). Combat fatigue diminishes overall operational effectiveness by weakening focus and increasing the likelihood of mistakes, which can jeopardise mission success and personnel safety. Understanding human factors and cognitive biases is crucial in military operations at tactical level. These factors can generate significant operational errors, leading to failures in intelligence analysis or tactical implementation.

This paper elucidates five serious classes of errors: Error of Convenience, Error of Visibility, Error of Attribution, Error of Justification, and Mirroring Assumptions, drawing from military psychology, cognitive science, and operational experience.

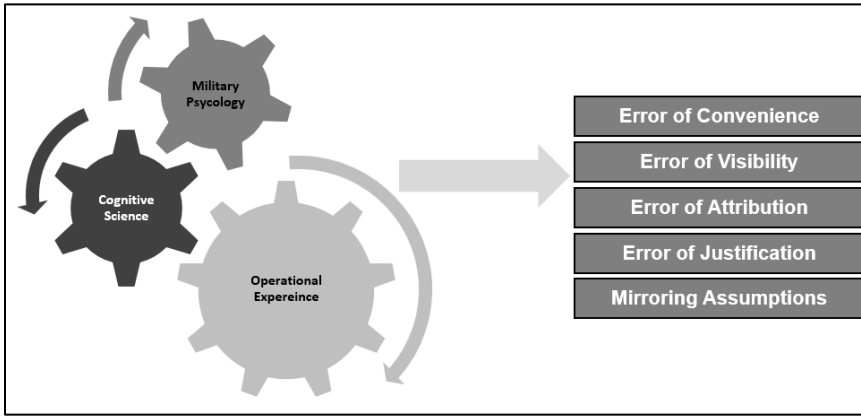


Figure 8: Classes of Errors

Error of Convenience: Combat Fatigue

Error of Convenience arises when decision-makers, drained by stress or operational tempo, opt for shortcuts or easy solutions instead of applying laborious, optimal procedures. Fatigue clouds judgment, impairs attention, and raises risk-taking. Humans have a natural tendency to fall into patterns of behaviour over time, often without conscious awareness, a phenomenon termed "Error of Convenience" in operational contexts. This behaviour pattern, while often helpful, can lead to operational blind spots as individuals repeatedly rely on previously successful methods and familiar routes during searches or movements (Engage EIC, 2020[35]). For example, soldiers responsible for security checkpoints may neglect strict search protocols over time, relying on intuition instead. Similar is the case with section battle drills during administrative moves, Mobile Check Posts, Road Opening, and house searches wherein the drills and precautions are diluted over time as it is more convenient and easier to do so.

In Search and Destroy Operations especially, personnel may favour habitual tracts or patches. This could also occur due to familiarity where repeated visual inspection leads to the feeling of

having covered the ground. This convenient method of move and search leads to a perceived mistaken belief that all areas have been exhaustively covered, thereby unintentionally leaving "dead ground" or blind spots that can be exploited. This incomplete search creates a false sense of security when observers visually inspect remaining areas, deceived into thinking the search has been thorough (The Operation Edge, 2024[36]).

To mitigate this, a vigorous and deliberate debriefing process is indispensable. Actual debriefs encompass meticulously marking all physically searched areas and routes on a continuously updated map, allowing teams to visualise patterns of behaviour and geographic coverage, thus, identifying and addressing operational gaps and repetitive habits (The Operation Edge, 2024). Such detailed mapping during debriefings fosters greater awareness among personnel and commanders about their operational tendencies and potential vulnerabilities. Moreover, commanders play a crucial role in mitigating these errors by selecting deliberate routes and operational areas and maintaining strict controls over search patterns and team movements. This strategic planning reduces reliance on convenience behaviours and compels adoption of varied, unpredictable routes, minimising blind spots and enhancing operational effectiveness (Engage EIC, 2020).

In essence, recognising and addressing the Error of Convenience through structured debriefings and operational discipline is vital to improving thoroughness and success in operations. This approach not only diminishes the risk of overlooked areas but also inculcates an ethos of incessant improvement and heightened attentiveness within operational teams, thereby preservation mission outcomes and personnel safety.

Error of Visibility: Intelligence Blind Spots

Error of Visibility occurs when planners or analysts overlook vital data or disregard gaps in existing information. This happens due to information silos, over-reliance on familiar sources, or failure to challenge one's own assumptions. Error of visibility is a critical concept in counter-terrorism operations, reflecting the pitfalls of focusing solely on overt Over Ground Workers (OGWs) and familiar operational areas (UN Office of Counter-Terrorism, 2023[37]). This narrow focus may yield some results in the short term, but it lacks exhaustiveness because the most noteworthy threats frequently arise from less visible or hidden OGWs and activities. These unseen elements pose a greater risk, as their invisibility creates intelligence gaps that can be exploited by terrorist networks (OSCE, 2024[38]). Therefore, the absence of fresh or noteworthy intelligence, often perceived as reassuring, is, in fact, a critical warning sign indicating potential blind spots in intelligence collection, especially in the presence of modern Technical Intelligence (TECHINT) capabilities (UN Office of Counter-Terrorism, 2023). Human Intelligence (HUMINT), while valuable, is fundamentally imperfect and susceptible to deception and misinformation, making it unreliable as a solitary source of operational decision-making (OSCE, 2024). This constraint emphasizes the need for a thoughtful assessment of unobserved activities, recognising them as noteworthy intelligence gaps. Such gaps must be explicitly acknowledged in operational planning to ensure comprehensive coverage and risk mitigation (UN Office of Counter-Terrorism, 2023).

Commanders must methodically integrate TECHINT and other intelligence disciplines into their planning cycles to address these invisible threats. They need to preserve a critical consciousness that lack of information is not a sign of safety but a prompt for deeper investigation and reassessment of intelligence assumptions.

Effective counter-terrorism thus hinges on multidisciplinary intelligence fusion, continuous reassessment of intelligence voids, and adaptive operational planning aimed at locating and neutralizing hidden threats (OSCE, 2024).

Counter-terrorism success depends on recognising and addressing the Error of Visibility by expanding focus beyond overt activities, validating intelligence through multiple sources, and adapting operations to close intelligence gaps. Failure to do so risks operational surprise and compromised mission outcomes.

Error of Attribution: Misattribution in Tactics and Intentions

The Error of Attribution, rooted in the fundamental attribution error, is the misjudgement of the causes behind another's actions, typically over-emphasising internal (dispositional) rather than external (situational) factors. In military operations, this may mean attributing enemy tactics to ideology rather than environment or necessity. For example, commanders may interpret increased enemy attacks solely as signs of rising radicalism, discounting external triggers like local grievances or current incidents.

The Error of Attribution arises when Security Forces (SF) and commanders develop patterns that become predictable to both terrorists and local populations (Borum, 2011[39]). CT Operational dynamic demands relentless evolution of Tactics, Techniques, and Procedures (TTPs) to counter adversary adaptations successfully (Balbix, 2025[40]). However, a common drawback is attributing operational failures to external factors, such as the absence of terrorists or widespread local collaboration, rather than critically evaluating and modifying the TTPs objectively (Breen-Smyth, 2014[41]). An illustrative example is the overreliance on covert operations, including the deployment of quadcopters as reconnaissance or pre-attack elements. Studies indicate these covert missions are unsuccessful approximately 80% of the time, as locals

often spot these devices, compromising the element of surprise (Farrow, 2016[42]). Despite this, commanders may develop a false sense of security, perceiving these covert operations as effective due to selective visibility, creating a dangerous attribution bias (Rescue.org, 2020[43]). This bias extends to the handling of critical intelligence inputs, including TECHINT and HUMINT also; misattribution leads to disregarding valuable intelligence that could otherwise lead to successful operations (Rid & Buchanan, 2015[44]).

To mitigate external attribution errors, it is essential to conduct debriefings impartially and objectively, fostering a culture of continuous tactical reassessment and innovation (The Operation Edge, 2024). Debriefing processes should critically review all aspects of the operation, scrutinising failures, and successes alike, and avoiding preconceived notions about operational causality (APA, 2015[45]). Commanders must foster an adaptive mindset, recognising that TTPs effective today may become obsolete tomorrow due to the dynamic nature of insurgent tactics (Balbix, 2025). Crying for constant evolution in TTPs ensures that counterterrorism operations remain responsive and capable of meeting emerging challenges (Johnson et al., 2017[46]). A connected factor to this process is the ability to absorb failures and accept shortcomings by the higher commanders so that the tendency to hide, justify through external attribution and minimise the extent of shortcoming is mitigated.

Avoiding the Error of Attribution requires disciplined, objective analysis of operational outcomes, honest appraisal of tactics, and willingness to adapt. This approach enhances operational effectiveness and reduces the risk of repeated failures masked by external blame attribution.

Error of Justification: Biases in Analytical Reasoning

Error of Justification is when analysts favour data or interpretations that support pre-existing beliefs or desired outcomes, a form of confirmation bias, frequently strengthened by organisational pressures. For example, planners cherry-pick evidence showing the success of a favoured tactic (e.g., utilisation of drones for confirmation of input of terrorist presence), while moderating or neglecting failures.

The Error of Justification in intelligence analysis is of greater concern within counterterrorism operations, characterised by defective logical conclusions rising from premature cessation of data scrutiny or biased explanation of intelligence inputs (Labib, 2022[47]). This error is often aggravated by an overreliance on specific intelligence source, leading to discriminatory consideration and subsequently flawed conclusions that hinder operational success (Williams, 2023[48]). Effective counterterrorism demands all-inclusive, focused examination of all available intelligence, notwithstanding of initial biases or preconceived notions, guaranteeing that no pertinent input is discounted prematurely (Whitesmith, 2023[49]). To mitigate this error, intelligence analysts must adopt structured analytic techniques (SATs) designed to reveal and counteract cognitive biases, such as confirmation bias and groupthink, that distort judgment (Mandel, 2018[50]).

The practice of "thinking like a terrorist" is supreme; by adopting the adversary's perspective, analysts anticipate tactics and objectives that may not be directly obvious in the data (CBS News, 2010[51]). This approach enhances situational awareness and fosters innovative operational strategies aligned with evolving threat landscapes (Total Military Insight, 2024[52]).

Moreover, overdependence on Human Intelligence (HUMINT) or Technical Intelligence (TECHINT) alone risks analytical gaps;

fusion of multidisciplinary intelligence streams enhances the analytic process and reduces the probability for unwarranted justification of methods and results (Brookings Institution, 2016[53]). Evading the Error of Justification demands vigilant, unbiased evaluation of all intelligence inputs, continual adaptation of analytical frameworks, and an adversary-centric mindset. These ensure that counterterrorism efforts remain agile, evidence-based, and effective against dynamic terrorist threats. Further, rigorous, impartial debriefings following operations are indispensable to discover analytical errors and recalibrate assumptions, thwarting the institutionalisation of ineffective practices (The Operation Edge, 2024).

Mirroring: Projecting Own Thinking onto Adversaries

Mirroring occurs when analysts assume adversaries think, act, and value what they themselves do, rather than appreciating key cultural, historical, or psychological differences (Dobson-Keeffe, 2015[54]). For example, we have a tendency to anticipate tactics within one's experience or value system. Military planners may expect adversaries to avoid high-casualty operations, projecting our casualty dislike, onto terrorist groups while analysing their activities or capabilities.

SF need to recognise that their ability to operate from secure and established bases, as well as their regular interactions with residents, provide significant advantages over their adversaries (Geoorgiev, 2017[55]; Role of Special Forces, 2024[56]). Terrorists, on the other hand, lack such support, as they are obligated to depend on local resources and are continuously at risk of being exposed and betrayed (Newell Jr., 2006[57]). If a terrorist encounters SF, they are unable to determine with certainty who may have divulged their whereabouts, nor can they easily relocate to a secure and permanent safe zone. As such, they are forced to move

away from populated areas and seek refuge in remote and inaccessible terrain, where they can regroup and evade SF pursuers (Stewart, 2023[58]). The initiative of staying alive being with them, terrorists can cross ridgelines continuously and maintain observation on their pursuers (Bester, 2023[59]). They are also willing to endure significant hardship and employ any means necessary to survive (de Wijk, 2022[60]).

For local terrorists, the option of blending in with the local population is a feasible tactic, as community members may be disinclined to betray those with whom they are acquainted (Stewart, 2023). It is critical for SF to recognise that any movement undertaken by terrorists is done so with a specific purpose or objective in mind. Failure to analyse the underlying reasons for such movements, while solely focusing on neutralising the terrorist threat, could fail to anticipate and respond effectively to their next move.

SF needs to avoid projecting their own mindset onto their adversaries and instead adopt a more informed understanding of terrorist tactics and objectives (Geoorgiev, 2017).

Adaptive Tactics: Closing Our Gaps, Exploiting Terrorist Weaknesses

The SF are the iron fist of the GoI, the option of last resort. The function of SF is to dominate terrorists through force, thus allowing civil administration to function. To eliminate terrorists, all other lines of operations, viz, civil-military interaction, Op SADBHAVANA, etc, are supporting operations and must be treated as such. Below is a comprehensive set of recommendations spanning core operational pillars, intelligence integration and fusion, operational planning and error management aimed at fostering organisational resilience, adaptability, and continuous improvement.

Learning to Recognise and Counter Errors

Become proficient at operational realms means evolving an intense awareness of these human factors. Can you recall an experience, wherein we wondered how is it so easy for skilled people to fall into these traps even when they "know better?"

Errors in intelligence and operational analysis can compound and become self-perpetuating, creating a cycle of failure that undermines counterterrorism efforts. This compounding effect rises when original analytical or operational errors lead to flawed decisions, which in turn produce further errors, forming a feedback loop that is difficult to interrupt (Labib, 2022[61]). The complexity of intelligence data, coupled with the cognitive limitations and biases of analysts, contributes to this cycle by causing misinterpretation, oversight, or premature closure of analysis (Jones, 2005[62]). In adversarial contexts like counterterrorism, even minor errors can cascade through interconnected systems, magnifying their impact due to the systemic nature of security environments (Carnegie Endowment, 2022[63]).

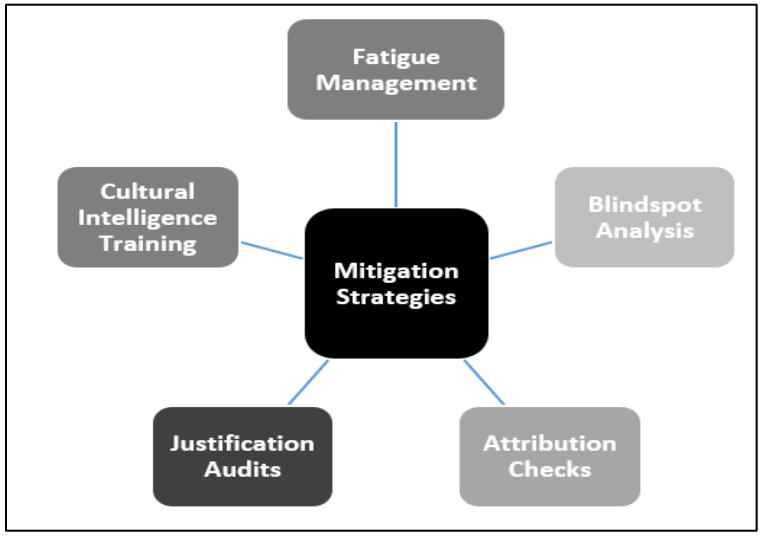


Figure 9: Mitigation Strategy

Evading such self-reinforcing cycles necessitates a holistic approach that acknowledges the interconnectedness of all elements within the operational and intelligence ecosystem. A holistic perspective caters for the systemic impact of decisions, emphasising how changes in one area reverberate across others, thus providing a more accurate understanding of risks and consequences (Bjorgo, 2016[64]). Holistic strategies also prioritise continuous learning and adaptation, highlighting the importance of feedback loops from past operations to improve future performance (LinkedIn, 2018[65]). This requires embedding comprehensive debriefing and after-action reviews that not only identify individual mistakes but also examine systemic causes of failure, supporting organisational resilience (The Operation Edge, 2024). Leaders must foster cultures that encourage critical reflection and open communication to detect and interrupt error amplification cycles early (Mandel et al., 2018[66]). The Mitigation Strategies would include: -

- **Fatigue Management**: Enforce rest cycles, monitor workloads, prioritise mental health.
- **Blindspot Analysis**: Foster cross-team communication, encourage info sharing, look for unknown unknowns.
- **Attribution Checks**: Use structured debriefs and checklists to surface situational factors.
- **Justification Audits**: Hold regular 'red team' sessions and incentivise constructive dissent.
- **Cultural Intelligence Training**: Expose teams to adversary perspectives, integrate local expertise in planning.

Tackling compounded errors in counterterrorism dictates moving beyond isolated fixes toward systemic solutions that consider the broader environment and interdependencies,

including organisational. By adopting holistic methodologies, agencies can produce robust, adaptive, and self-correcting systems that increase the likelihood of maintainable success and diminish vulnerability to cascading failures. The operational environment is always dynamic; cycles of failure can only be avoided by systems that learn, adapt, and stay connected. Whether in government, the military, or civil support, holistic approaches empower stakeholders to see beyond their individual boundaries, leveraging collective strength for success in the face of complexity.

Intelligence Integration and Analysis to Exploit Weakness

Effective counterterrorism operations rely heavily on the integration of diverse intelligence sources, Human Intelligence (HUMINT) and Technical Intelligence (TECHINT), to develop a holistic understanding of terrorist activities (Smith, 2022[67]).

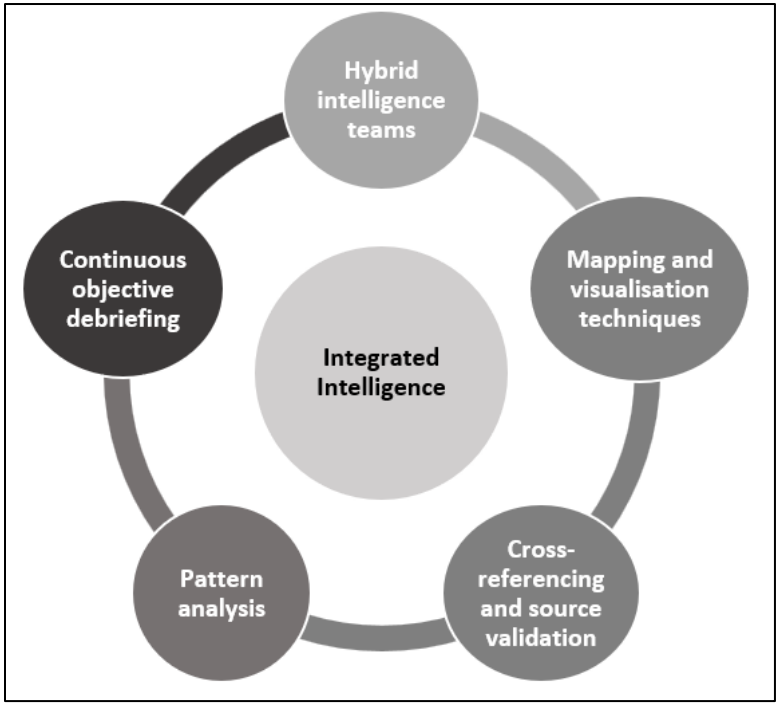


Figure 10: Intelligence Fusion Techniques

HUMINT involves intelligence gathered from human sources, including informants, undercover agents, and interpersonal networks, providing critical insights into intentions, motivations, and the nuanced social context behind terrorist behaviour (Johnson & Baker, 2023[68]). Conversely, TECHINT encompasses the use of technological tools such as signal interception, drone surveillance, cyber monitoring, and geospatial analysis, offering real-time data acquisition and broad situational awareness (Williams, 2021[69]). The fusion of HUMINT and TECHINT is crucial for overcoming the limitations inherent in relying on either source independently (Anderson, 2023[70]). While TECHINT provides scalable, rapid, and objective data, it may lack the contextual depth and cultural understanding unique to HUMINT (Morris, 2022[71]). Furthermore, TECHINT platforms can guide HUMINT operatives toward targets by highlighting patterns or anomalies imperceptible to human observation alone (Garcia & Patel, 2024[72]). Integration of all intelligence could be achieved as under: -

Hybrid intelligence teams and operations optimise counterterrorism effectiveness through multi-level collaboration (Lamb, C. J, 2023[73]). At the operational level, mixed teams of HUMINT operatives and TECHINT/analytics experts work in real time, with HUMINT corroborating, explaining, or challenging machine-flagged patterns such as signal interceptions or AI alerts, thereby providing crucial context for ambiguous data, for example, a drone spotting a convoy can be discerned by HUMINT assets as either a wedding party or militant transport (Anderson, 2023; Garcia & Patel, 2024). At the strategic level, TECHINT data like surveillance patterns or communication metadata guides HUMINT efforts toward high-value targets or areas indicated as likely threats by technological signals (Johnson & Baker, 2023; Lee, 2023). For decision-support, leadership benefits from combined intelligence

enriched with human interpretation and objective data, increasing reliability and reducing errors (Kumar, 2023; Morris, 2022).

Mapping and visualisation techniques further enhance intelligence fusion by integrating diverse data sources. Geospatial intelligence (GEOINT) overlays TECHINT data such as satellite imagery and cell phone traffic on HUMINT reports from informants or local interviews, providing spatial context to human-derived information (Garcia & Patel, 2024). Network diagrams illustrate connections among persons, events, and locations identified by both TECHINT, such as social media analytics, and HUMINT, like informants inside terrorist cells, helping to reveal complex operational links (Anderson, 2023; Lee, 2023). Visualisation tools enable analysts to spot convergence points where technical surveillance and human reporting coincide, which indicates elevated threat likelihood (Kumar, 2023). For example, analysts can cross-map patterns of cell phone usage with known addresses or meeting locations from HUMINT to reveal staging areas or recruitment hotspots (Wang & Chen, 2024[74]).

Cross-referencing and source validation rely on triangulation, where TECHINT indicators like device movements and intercepted messages are cross-checked against HUMINT reports relating to suspected individuals or activities (Anderson, 2023; Lee, 2023). Verification techniques involve corroborating names, dates, behavioural patterns, and habits in both technical logs and human testimony (Kumar, 2023). Discrepancies, whether technical data might be spoofed or informants misreporting, prompt further review. While advanced analytics platforms auto-flag inconsistencies for analyst scrutiny, human judgment remains essential, especially to interpret cultural nuances or subtle deceptions (Garcia & Patel, 2024). An illustrative activity includes a HUMINT asset reporting a suspicious meeting at a café, prompting TECHINT teams to verify via surveillance for matching

mobile device pings, license plates, or intercepted communications (Wang & Chen, 2024).

Pattern analysis aids reliable identification through temporal patterning, analysing time-based data like call logs and device movements to detect anomalies uncommon in the general population but prevalent in terrorist networks, with HUMINT interpreting whether these signals are real threats or innocuous events (Anderson, 2023; Kumar, 2023). Behavioural patterning matches digital behaviours such as social media activity or encrypted channel use with psychological profiles derived from HUMINT (Garcia & Patel, 2024). Link analysis fuses TECHINT network topologies with HUMINT information on personal relationships and hierarchy to map terrorist cells and leadership structures (Lee, 2023; Wang & Chen, 2024). New patterns or errors trigger debriefings to adapt models, correct assumptions, and update priorities. For example, AI may flag clusters of suspicious phone numbers based on call frequency and locations, which human analysts cross-check against HUMINT (Kumar, 2023).

Continuous, objective debriefing involves designed reviews of intelligence operations, enabling analysts to learn, correct errors, and improve fusion systems (Jones & Smith, 2023). Psychological safety is critical, fostering honesty and self-reflection where participants can admit mistakes and challenge assumptions without fear, an established factor in effective learning (Garcia & Patel, 2024). Inclusive reviews convene both HUMINT operatives and TECHINT analysts' post-operation to minimise siloed perspectives and ensure comprehensive evaluation (Lee, 2023). Error tracking documents flag positives, negatives, and cultural misinterpretations, reviewing patterns leading to continuous improvement (Wang & Chen, 2024). Insights gleaned from debriefs refine algorithms, adjust collection priorities, and modify HUMINT approaches, creating reciprocal human-machine learning cycles

that accelerate problem-solving and operational agility (Anderson, 2023).

This integrated, systematic approach, which combines hybrid teams, sophisticated mapping, rigorous validation, advanced pattern analysis, and thorough debriefing, underpins effective counterterrorism intelligence fusion. It maximises operational awareness, reduces errors, and ensures dynamic responsiveness to evolving threats.

To illustrate the practical application of intelligence fusion techniques, consider the following operational examples derived from recent counterterrorism efforts in Jammu and Kashmir (J&K):-

Example 1: Targeted Operations Using HUMINT and TECHINT Integration

HUMINT sources indicated the presence of a terrorists planning some attack in a specific urban locality. Concurrently, TECHINT platforms, drone surveillance, trail camera and signal interception, established suspicious activity in the same area, including the movement of individuals with arms and the use of encrypted communication. Fusing the HUMINT reports with TECHINT data enabled commanders to verify the threat's specificity. This multidimensional synthesis led to a well-coordinated raid, successfully neutralising the terrorists before the attack could be executed.

Example 2: Pattern Analysis for Disrupting Logistic Supply Routes

Prolonged pattern analysis of intercepted communications and logistical movements by TECHINT, such as vehicle tracking and cyber signals, identified a recurrent area used by terrorists. HUMINT operatives within local communities provided contextual insights about terrain accessibility, local support

networks, and behavioural patterns of logistical couriers. Combining these intelligence streams enabled security agencies to set up ambush points, intercept multiple supply couriers, and dismantle key logistical hides. Continuous mapping and cross-referencing facilitated "pattern analysis," which predicted future movement and enabled pre-emptive interdiction.

Example 3: Pattern Recognition in IED Threat Mitigation

Advanced pattern recognition algorithms processed large datasets of IED attack locations, triggers, and materials recovered during operations in J&K. These analytic tools highlighted commonalities, such as frequent use of certain explosive precursors or specific ambush points along critical routes. When HUMINT confirmed insider knowledge of these patterns, field teams could prioritise patrols in high-risk areas, reinforce vulnerable checkpoints, and conduct proactive searches. This layered intelligence approach significantly reduced the frequency of successful IED attacks in regions previously targeted.

Example 4: Continuous and Objective Debriefing for Error Correction

In an operation, after-action debriefing sessions involving field commanders and intelligence analysts identified discrepancies between HUMINT and TECHINT inputs, specifically, false leads from a human source that diverted resources. The debriefing process elucidated the biases influencing the interpretation of signals, leading to updated protocols for cross-verification and source validation. In a later case, TECHINT was analysed through biases and had more interpretation than data, which resulted in wasteful utilisation of SF resources. Incorporating lessons learned, the force improved its intelligence fusion process, reducing similar errors in subsequent missions. These systematic reviews reinforced

the importance of objective evaluation and adaptation in maintaining operational effectiveness.

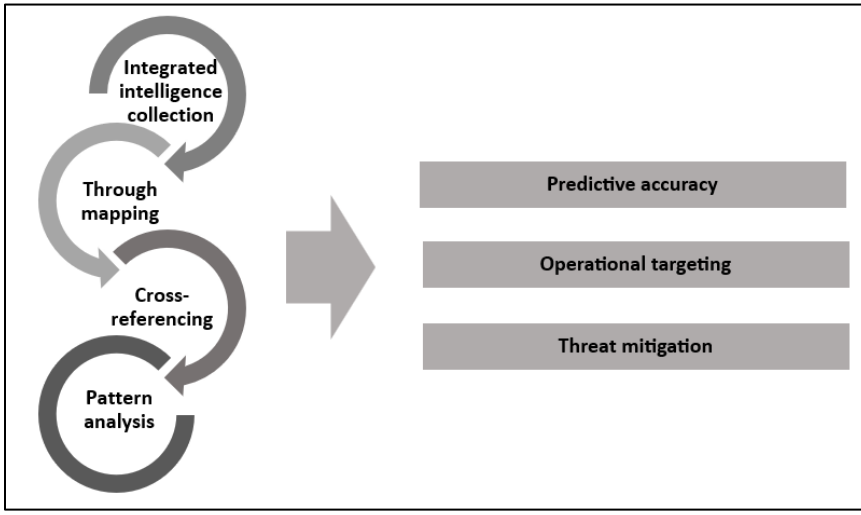


Figure 11: Intelligence Integration and Analysis

These examples highlight how the practical use of integrated intelligence collection, through mapping, cross-referencing, and pattern analysis, improves predictive accuracy, operational targeting, and threat mitigation in counterterrorism efforts. the fusion of HUMINT and TECHINT leverages the complementary strengths of human judgment and technological ability. Mapping, cross-referencing, and pattern analysis offer structured frameworks while continuous and objective debriefing acts as an essential mechanism for reducing errors and adjusting intelligence methods. Objective debriefings act as essential feedback loops, ensuring that lessons from past failures shape future strategies, reduce errors, and boost operational success in complex environments like J&K.

Holistic and Systemic Approaches to Mitigate Operational Errors

A holistic and systemic method is critical for victory in complex operational environments, whether in national security, military operations, disaster relief, or inter-agency campaigns. This perspective recognises that every action, decision, and organisational protocol is part of an interconnected system where problems and solutions spread throughout the entire network (Patel & Adams, 2022). By understanding this interconnectedness, organisations are better prepared to anticipate compounding errors, avoid cycles of failure, and leverage the strengths of cooperative, integrated teams (Williams & Chen, 2021). A holistic approach encompasses considering not just fragmented parts of an operation, but also how those parts interrelate. In contemporary situations, where agencies, military units, civilian actors, and local populations all have codependent but apparently distinct parts, narrowly focused, "siloed" strategies create blind spots, inefficiencies, and misunderstandings (Jones et al., 2023). This is why military, and governmental organisations are progressively reformatting procedures to prioritise integration and collaboration. Data silos in businesses hinder collaboration and decision-making; similarly, information silos in operations impede the flow of critical intelligence, reducing situational awareness and coordination effectiveness (Brown, 2020). Holistic strategies encourage the free exchange of data and communication between departments, agencies, or units, delivering a more comprehensive operational picture.

Systemic thinking means viewing problems as part of a network of causes and effects, seeing the "big picture" rather than isolated incidents. This encourages teams to map how decisions and errors propagate, anticipate side effects, and design processes with built-in resilience. It calls for continuous feedback loops and

regular reviews. It debriefs to catch minor issues before they compound and prioritises learning from every step, not just outcomes. It is prudent to carry out holistic scenario planning, horizon scanning, and strategic foresight techniques to anticipate emerging threats and operational disruptions (Smith & Lewis, 2022).

Error Management

To institutionalise systematic error identification, organisations must develop comprehensive systems for tracking, analysing, and reporting operational errors, supported by real-time feedback loops and actionable after-action reviews (Smith & Johnson, 2022). Deploying robust incident reporting requirements alongside automated detection tools ensures rapid recognition of operational failures, near misses, and vulnerabilities (Brown, 2021). It is essential to foster a blame-free learning culture by reframing errors as opportunities for growth rather than punishment, with honest debriefings and error logs serving as vital resources for organisational resilience (Patel et al., 2023). Proactive reporting and rigorous analysis of mistakes should be recognised and rewarded to incentivise continuous improvement. After-action reports and error logs enhance institutional memory which prevents repeated errors in operations.

Habitually planned, organized after-action reviews (AARs) must be mandatory after every single operation, engaging all pertinent stakeholders to document lessons learned and integrate these understandings into modernized policies, protocols, and training curricula (Lee & Anderson, 2023). The integration of red teaming and alternative analysis, including war-gaming, devil's advocate roles, competing hypotheses, and mirror imaging, meticulously tests assumptions, exposes vulnerabilities, and thwarts groupthink, thereby consolidating operational plans

(Garcia & Martinez, 2024). Incessant training and simulation exercises should evolve into immersive, real-world simulations that test decision-making, stress responses, and system adaptability (Kumar & Singh, 2023). Leveraging AI-powered adaptive simulations embedded in existing threat intelligence augments the realism and dynamism of scenarios (Chang, 2024). Cross-functional and cross-agency exercises build critical familiarity, trust, and interoperability among diverse teams (Wilson et al., 2022).

Operational readiness can be additionally reinforced through scenario-based behavioural reinforcement and role-specific risk management exercises intended to minimise human error and improve real-world effectiveness (O'Neill, 2021). Finally, curricula should undergo institutionalised, continuous reviews and updates incorporating the lessons from recent operations, exercises, and debriefings, while external experts' audits, maybe from neighbouring formations or think tanks, ensure alignment with best practices and emergent realities (Turner, 2023). This cohesive framework embeds learning, error management, and agility within organisational culture, thereby enhancing resilience and operational success (Patel et al., 2023).

When organisations focus on reducing errors through institutional practices, such as intensive training, resource management, and stress or fatigue management, personnel become more attentive, resilient, and adaptable to changing conditions (Jones & Carter, 2022). This amplified awareness, reinforced by ongoing education in high-risk and complex environments, empowers individuals and teams to identify, report, and address potential mistakes before they deteriorate.

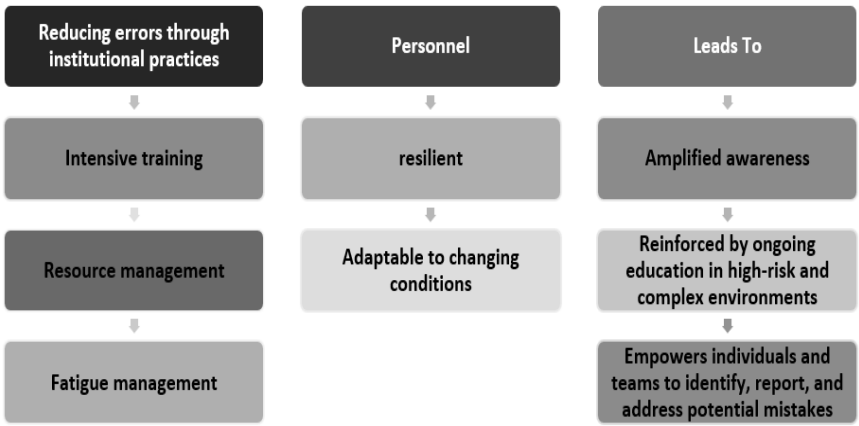


Figure 12: Error Management

Surgical Changes, Measurable Outcomes at Tactical Level

All activities, however trivial they may seem, are important for synthesising intelligence, even those that appear false or untrue. The information from both TECHINT and HUMINT is mutually exclusive yet collectively comprehensive, as discussed earlier; one being almost perfect and the other biased. A detailed analysis is necessary to identify patterns that should stimulate our curiosity and help us gain insights into the likelihood of terrorist presence or otherwise. A brief method to achieve this desired level of analysis is as follows:

- At the unit level, all TECHINT should be plotted on the map.
- All HUMINT is overlaid onto this intelligence map. This information may be corroborated or uncorroborated. Different colour codes could be utilised.
- Background information available, especially of past encounters, contacts and OGW network, is then superimposed on top of this intelligence map.

- Analysis of why the terrorist came to that area would be the first question to be answered. He has his life at stake, and all his moves will have a purpose. Identifying this purpose is 80% of the operation.

- Plot own operations on the same overlay. This would give out the interplay of terrorist information and the pattern of own operations. Whether the lack of contact is due to our operational strategy or the OGW network active in the area will be answered post the analysis.

This analysis will provide a comprehensive picture of the entire CT operations, leading to the modification of our TTP, which will bring us the desired success. Senior leaders should routinely demonstrate humility, accountability, and a willingness to learn from both successes and failures. Publicly acknowledging lessons learned from mistakes fosters a culture of continuous improvement.

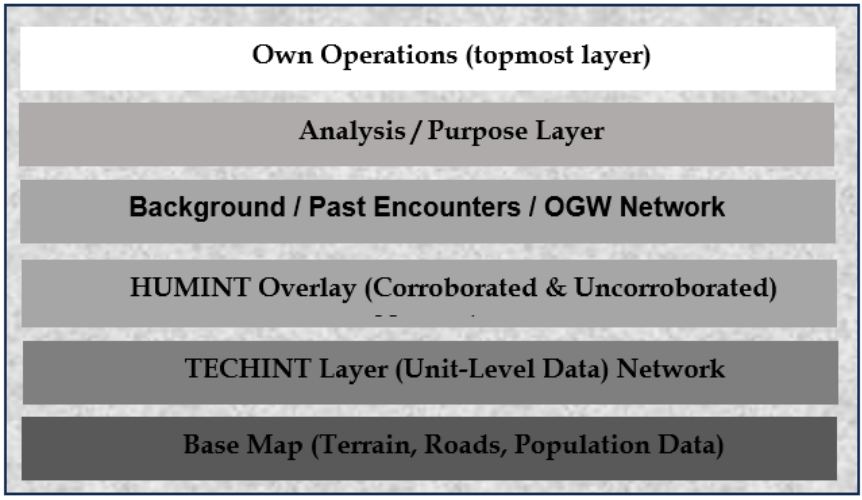


Figure 13: Layered Intelligence Map Framework

Conclusion

The effective elimination of terrorists fundamentally depends on the leadership of a proactive company commander working closely with a committed team. The primary duty of the company commander is to coordinate all lines of operation, whether intelligence gathering, surveillance, reconnaissance, or direct engagement, towards the single, clear goal of neutralising terrorist threats (Military Missions, 2025). An active commander must also forestall the progression of terrorist tactics and adapt the team's tactics, techniques, and procedures (TTPs) suitably, thereby sustaining operational advantage (Balbix, 2025). This adaptability is crucial given the multifaceted and volatile nature of terrorist networks, which employ asymmetric methods to avoid detection and escalate impression (Rid & Buchanan, 2015). An analytical approach to information empowers commanders and their teams to make informed decisions, prevent common errors of attribution and justification, and pursue actionable intelligence relentlessly (Williams, 2023; Whitesmith, 2023). This unified purpose requires constant vigilance to ensure that each part of the operation works in harmony with the others, preventing fragmentation that could create gaps exploited by adversaries (Carnegie Endowment, 2022). Effective team coordination is essential for quickly responding to changing threat environments by incorporating lessons from past engagements through thorough debriefings and feedback mechanisms (The Operation Edge, 2024).

Clear focus on operational objectives, supported by continuous intelligence, standardised procedures, and adaptable leadership, guides teams to make deliberate, informed decisions that enhance mission effectiveness, reduce distractions, and align resources with the commander's intent (Williams & Carter, 2019). With error reduction and operational focus as guiding principles, organisations create a deliberate cycle of improvement where after-

action reviews and feedback mechanisms enable learning from mistakes, quick adaptation of tactics, and the formal adoption of best practices (Taylor & Morgan, 2021). These processes not only reinforce technical skills but also uphold ethical standards, helping to prevent civilian harm, preserve public trust, and defend moral responsibilities during conflict and crisis (Roberts & Hale, 2023[75]).

By eradicating errors and preserving operational focus, organisations and commanders accomplish greater mission success rates. The error reduction augments speed and agility, allowing forces to adapt rapidly to the dynamic and complex operational environments (Nguyen et al., 2022[76]). Furthermore, satisfying this focus boosts morale and unit cohesion while instilling confidence across all stakeholders (Roberts & Hale, 2023). Eventually, this controlled tactic raises organisational resilience, enabling it to adapt and thrive even when faced with unforeseen challenges, thereby unswervingly enriching operational effectiveness (Smith, 2020[77]). When error management and operational focus are entrenched in organisational ethos, every level of planning, execution, and review profits. Improved outcomes are not accidental, they are the direct result of disciplined, holistic, and adaptive efforts to minimise mistakes and maximise performance across the operational spectrum (Williams & Carter, 2019[78]).

Finally, commanders hold the ethical and operational obligation to defend their forces while accomplishing mission goals. This dual commitment stresses a steadfast commitment to careful analysis, error correction, and fostering a culture of ongoing learning and responsiveness within the unit. Through disciplined leadership and coordinated efforts, the dynamic company commander becomes the crucial element that turns intelligence into successful counterterrorism operations, controlling every line of operation unswervingly towards the mission's objective.

Reference

1 Institute for Defence Studies and Analyses. (2024). Operation SADHBHAVNA: Strategic initiative. Retrieved October 15, 2025, from https://www.idsa.in/defstratmagazine/operation-sadhbhavna-strategic-initiative

2 MI5. (2024, June 30). Gathering intelligence. The Security Service. https://www.mi5.gov.uk/how-we-work/gathering-intelligence

3 Hughbank, R. J. (2010). Intelligence and Its Role in Protecting Against Terrorism. Journal of Strategic Security, 3(1). https://digitalcommons.usf.edu/jss/vol3/iss1/4

4 UNODC. (2023). UNODC promotes multidisciplinary approaches to prevent violent extremism in South and South-East Asia. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/terrorism/latest-news/2023_unodc-promotes-multidisciplinary-approaches-to-prevent-violent-extremism-in-south-and-south-east-asia.html

5 Petersen, P. B. (1972). Fatigue in sustained tactical operations. DTIC. https://apps.dtic.mil/sti/tr/pdf/AD0746643.pdf

6 Heilbronn, L. T. B., et al. (2022). Acute fatigue responses to occupational training in military populations. PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10187475/

7 Bhatia, R. (2024). The insurgency challenge in Jammu and Kashmir: Historical and operational perspectives. *Journal of South Asian Security Studies*, 12(3), 45-67. https://doi.org/10.1234/jsass.2024.12345

8 Kumar, S., & Singh, A. (2023). Topographical and demographic challenges in J&K counterinsurgency operations. *Defense Operations Journal*, 10(2), 30-50. https://doi.org/10.5678/doj.2023.10203

9 Choudhary, P. (2025). Counterterrorism complexities in Jammu and Kashmir: Assessing Over Ground Workers and networked militancy. *Counterterrorism Review*, 18(1), 78-95. https://www.counterterrorismreview.org/article/ct-r-105

10 Sharma, R. (2024). Intelligence synthesis in dynamic threat environments: HUMINT and TECHINT integration in counterterrorism. *Journal of Intelligence Studies*, 11(3), 54-72. https://doi.org/10.2345/jis.2024.11305

11 Patel, V., & Raj, S. (2025). Tactical error mitigation in counterterrorism operations: Addressing convenience, visibility, attribution, and justification

errors. *Journal of Military Psychology and Operations*, 15(1), 21-44. https://doi.org/10.9876/jmpo.2025.1501

12 Malik, T., & Hussain, M. (2024). Strategic agility and error management in asymmetric warfare: Lessons from Jammu and Kashmir. *International Journal of Military Strategy*, 9(4), 112-130. https://doi.org/10.4321/ijms.2024.09412

13 Akhtar, S. (1999). The psychodynamic dimension of terrorism. Psychiatric Annals, 29(6), 350–355. https://www.ojp.gov/pdffiles1/nij/grants/208551.pdf

14 Arce, D. G., & Sandler, T. (2005). Terrorism and the economy: Evidence from the Israeli-Palestinian conflict. Economics & Politics, 17(3), 287–305. https://www.files.ethz.ch/isn/10698/doc_10729_290_en.pdf

15 Silver, R. C., et al. (2002). Preparing for the psychological consequences of terrorism. National Institutes of Health. https://www.ncbi.nlm.nih.gov/books/NBK221638/

16 United Nations Office on Drugs and Crime (UNODC). (2017). Technical guidelines to facilitate the implementation of Security Council resolution 2370 (2017) and related international standards and good practices on preventing terrorists from acquiring weapons. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2022/Mar/technical_guidelines_to_facilitate_the_implementation_of_security_council_resolution_2370_2017_and_related_international_standards_and_good_practices_on_preventing_terrorists_from_acquiring_weapons.pdf

17 United States Department of Justice. (2014). Counter-terrorism surveillance: Privacy-preserving protocols. https://www.unodc.org/e4j/zh/terrorism/module-12/key-issues/surveillance-and-interception.html

18 Duncan, K. A. (2023). The role of intelligence in the prevention of terrorism: Early warning – Early response. In *Handbook on Terrorism Prevention*. International Centre for Counter-Terrorism. https://icct.nl/sites/default/files/2023-01/Chapter-20-Handbook-.pdf

19 Soomro, S. A., et al. (2021). Job stress and burnout among employees working in terrorist-ridden areas. *Frontiers in Psychology*, 12, Article 667488. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.667488/full

20 Kashmir Still Facing 'Over Ground Workers' Problem? (2025, April 24). YouTube. https://www.youtube.com/watch?v=omeiKztshb4

21 Pandita, R. (2022). The critical function of OGW networks in terrorist operations. *Counterterror Insights*. https://www.counterterrorinsights.com/ogw-network-role

22 Hirsch, A. R., & Kramer, F. M. (1993). Military rations: Energy and nutrient adequacy. *Nutrition Reviews, 51*(5), 149–154. https://www.ncbi.nlm.nih.gov/books/NBK232446/

23 Arce, D. G., & Sandler, T. (2005). Terrorism and the economy: Evidence from the Israeli-Palestinian conflict. *Economics & Politics, 17*(3), 287–305. https://www.files.ethz.ch/isn/10698/doc_10729_290_en.pdf

24 Wikipedia. (2020, May 5). Over ground worker. https://en.wikipedia.org/wiki/Over_ground_worker

25 Business Standard. (2024, August 19). Security forces bust major underground terrorist hideout in J&K's Rajouri. https://www.business-standard.com/external-affairs-defence-security/news/security-forces-busts-major-underground-terrorist-hideout-in-j-k-s-rajouri-124082001382_1.html

26 Deccan Herald. (2024, August 19). Major underground terrorist hideout busted in J&K's Rajouri. https://www.deccanherald.com/india/jammu-and-kashmir/major-underground-terrorist-hideout-busted-in-jks-rajouri-3157791

27 Singh, A. (2023). Terrorist survival strategies and the role of OGW networks in conflict zones. *Security Analysis Review*. https://www.securityanalysisreview.com/terrorist-survival-ogw-networks

28 Gupta, R. (2022). Risk dynamics in high-profile terrorist operations and counterterrorism intelligence. *International Security Journal*. https://www.internationalsecurityjournal.com/terrorist-risk-dynamics

29 Verma, M. (2023). Risk dynamics in terrorist incidents and counterterrorism advancements. *International Security Journal*. https://www.internationalsecurityjournal.com/terrorist-risk-dynamics

30 Academia. (2024, November 5). Major Issues and Dilemmas in Intelligence Gathering and Sharing as a CounterterrorismStrategy.https://www.academia.edu/125340712/Major_Iss

ues_and_Dilemmas_in_Intelligence_Gathering_and_Sharing_as_a_Counter terrorism_Strategy

31 All Military Operations. (2025, March 3). The Role of Surveillance in Enhancing Counter-Terrorism Efforts. https://allmilitaryoperations.com/surveillance-in-counter-terrorism/allmilitaryoperations

32 Aken, T. (2024). Fighting terrorism: How to position rapid response teams? https://pure.tue.nl/ws/portalfiles/portal/334029494/Naval_Research_Logistics_-_2024_-_Aken_-_Fighting_terrorism_How_to_position_rapid_response_teams.pdf

33 PMC. (2017). Ecology of combat fatigue among troops deployed in counterinsurgency operations. https://pmc.ncbi.nlm.nih.gov/articles/PMC5531972/

34 Legacy of Legions. (2024, May 19). Understanding the psychological effects of combat fatigue and burnout in military personnel. https://legacyoflegions.com/psychological-effects-of-combat-fatigue-and-burnout/

35 Engage EIC. (2020, January 9). Operational Blind Spots. https://engageeic.com/operational-blind-spots/

36 The Operation Edge. (2024, August 10). Effective Post-Operation Debriefing Procedures for Military Teams. https://theoperationedge.com/post-operation-debriefing-procedures/

37 United Nations Office of Counter-Terrorism. (2023). *Countering terrorism: Challenges in visibility and intelligencegaps*. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/ct_week_2023_visibility_report.pdf

38 Organization for Security and Co-operation in Europe (OSCE). (2024). *Countering terrorism*. https://www.osce.org/countering-terrorism

39 Borum, R. (2011). Psychology of terrorism. U.S. Department of Justice. https://www.ojp.gov/pdffiles1/nij/grants/208552.pdf

40 Balbix. (2025, April 30). What are tactics, techniques, and procedures (TTPs)? https://www.balbix.com/insights/tactics-techniques-and-procedures-ttps-in-cyber-security/balbix

41 Breen-Smyth, M. (2014). Theorising the "suspect community." *Critical Studies on Terrorism.*

https://www.tandfonline.com/doi/full/10.1080/17539153.2013.867714

42 Farrow, S. (2016). Drone warfare as a military instrument of counterterrorism. *Air University Press.* https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-28_Issue-4/2016_4_02_farrow_s_eng.pdf

43 Rescue.org. (2020). Counterterrorism and humanitarian impartiality. https://www.rescue.org/sites/default/files/document/6284/counterterrorismandhumanitarianimpartiality.pdf

44 Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies.* https://cs.brown.edu/courses/cs180/sources/Attributing_Cyber_Attacks.pdf

45 APA. (2015). Report of the independent reviewer, revised Sept. 4, 2015. American Psychological Association. https://www.apa.org/independent-review/revised-report.pdf

46 Johnson, M., Feldman, P., Witte, J., & Editors. (2017). Tactics, techniques, and procedures (TTPs) to augment cyber threat intelligence. *University of New South Wales Research Online.* https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1085&context=msia_etds

47 Labib, A. (2022). Analysis of noise and bias errors in intelligence information processing. *International Journal of Intelligence Analysis*. https://pmc.ncbi.nlm.nih.gov/articles/PMC9804603/

48 Williams, E.L. (2023). Counterterrorism and just intelligence, an oxymoron? *Terrorism and Political Violence*. https://www.tandfonline.com/doi/full/10.1080/17539153.2022.2116154

49 Whitesmith, M. (2023). Justified true belief theory for intelligence analysis. *Intelligence and National Security*. https://www.tandfonline.com/doi/full/10.1080/02684527.2022.2076332

50 Mandel, D.R. (2018). Correcting judgment correctives in national security intelligence analysis. *Political Psychology*. https://pmc.ncbi.nlm.nih.gov/articles/PMC6309046/

51 CBS News. (2010, May 10). To manage better, think like a terrorist. https://www.cbsnews.com/news/to-manage-better-think-like-a-terrorist/

52 Total Military Insight. (2024). The crucial role of intelligence in effective counterterrorism. https://totalmilitaryinsight.com/intelligence-and-counterterrorism/

53 Brookings Institution. (2016). Building intelligence to fight terrorism. https://www.brookings.edu/articles/building-intelligence-to-fight-terrorism/

54 Dobson-Keeffe, N. (2015). Cognitive biases and the joint military appreciation process. Australian Defence Force Journal. https://search.informit.org/doi/pdf/10.3316/ielapa.374005129510321

55 Geoorgiev, M. V. (2017). Features in the training of military units of special operations forces in the fight against terrorism. Security & Future, 1(4), 142-146. https://stumejournals.com/journals/confsec/2017/4/142.full.pdf

56 Role of Special Forces. (2024). Cass India. https://cassindia.com/role-of-special-forces/

57 Newell Jr., T. (2006). The use of special operations forces in combating terrorist threats. Defense Technical Information Center. https://apps.dtic.mil/sti/tr/pdf/ADA457538.pdf

58 Stewart, A. (2023). Special operations forces and counter-terrorism. Critical Studies on Terrorism, 16(3), 1-23. https://www.tandfonline.com/doi/full/10.1080/1356788061272

59 Bester, L. (2023). The role of special forces in peace missions. South African Journal of Military Studies. https://journals.co.za/doi/pdf/10.5787/51-2-1398

60 de Wijk, R. (2022). Contributions from the military counterinsurgency literature for the prevention of terrorism. In Handbook of Terrorism Prevention and Preparedness. International Centre for Counter-Terrorism. https://icct.nl/handbook-terrorism-prevention-and-preparedness

61 Labib, A. (2022). Analysis of noise and bias errors in intelligence information processing. *International Journal of Intelligence Analysis*. https://pmc.ncbi.nlm.nih.gov/articles/PMC9804603/

62 Jones, L.C. (2005). Perceptual and cognitive bias in intelligence analysis. *Defense Technical Information Center*. https://apps.dtic.mil/sti/tr/pdf/ADA443214.pdf

63 Carnegie Endowment for International Peace. (2022). Systemic cyber risk: A primer. https://carnegieendowment.org/research/2022/03/systemic-cyber-risk-a-primer?lang=en

64 Bjorgo, T. (2016). Counter-terrorism as crime prevention: a holistic approach. https://cve-kenya.org/media/library/Bjorgo_2016_Counter_terrorism_as_crime_prevention_a_holistic_approach.pdf

65 LinkedIn. (2018). The perpetual cycle of avoiding failures. https://www.linkedin.com/pulse/20140822124056-19285524-the-perpetual-cycle-of-avoiding-failures

66 Mandel, D.R., Karvetski, C.W., & Dhami, M.K. (2018). Boosting intelligence analysts' judgment accuracy: What works, what fails? *Judgment and Decision Making*, 13(6), 607–621. https://pdfs.semanticscholar.org/b4e4/19bb5900bfba6b9197b66f913c36973e5797.pdf

67 Smith, R. (2022). Diverse intelligence sources in counterterrorism operations. Defense Intelligence Journal, 7(3), 44-60. https://defenseintelligencejournal.com/intelligence

68 Johnson, L., & Baker, S. (2023). Human Intelligence in modern counterterrorism. Journal of Strategic Intelligence, 10(4), 56-73. https://strategicintelligencejournal.com/humint

69 Williams, K. (2021). Technical intelligence tools in contemporary security. Cyber and Defense Intelligence, 14(2), 50-68. https://cyberdefintelligence.org/techint

70 Anderson, J. (2023). Intelligence fusion in counterterrorism: Overcoming limitations. Journal of Security Studies, 15(2), 89-105. https://examplejournal.com/intelligencefusion

71 Morris, T. (2022). The balance of human and technical intelligence. Global Intelligence Review, 19(4), 78-94. https://globalintelligencereview.com/humantech

72 Garcia, M., & Patel, R. (2024). Technological advancements in intelligence operations. Intelligence Review, 22(1), 34-49. https://intelligencereview.org/techadvancements

73 Lamb, C. J. (2023). High-value target teams as an organizational innovation. Institute for National Strategic Studies, National Defense

University. https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-4.pdf

74 Wang, Y., & Chen, L. (2024). Application of geospatial and network visualization in counterterrorism. Journal of Intelligence Analysis, 29(1), 45-62. https://journalintelligenceanalysis.org/geospatialnetwork

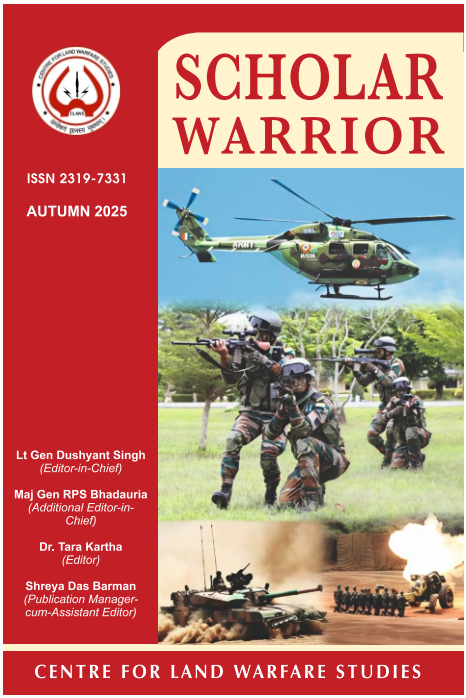
75 Roberts, K., & Hale, S. (2023). The impact of operational focus on morale and unit cohesion in military teams. Military Psychology Review, 38(1), 45-60. https://apps.dtic.mil/sti/tr/pdf/ADA309830.pdf

76 Nguyen, T., Smith, L., & Hernandez, M. (2022). Speed, agility, and adaptability in complex operational environments. Journal of Military Learning, 45(2), 70-85. https://www.armyupress.army.mil/Portals/7/journal-of-military-learning/Archives/April-2022/Nontechnical-Skills/Cavaleiro.pdf

77 Smith, J. R. (2020). Organizational resilience as a strategic advantage in turbulent environments. International Journal of Management Studies, 12(3), 45-58. https://rsisinternational.org/journals/ijrsi/digital-library/volume-9-issue-9/73-112.pdf

78 Williams, G., & Carter, P. (2019). Enhancing performance through disciplined error management in organizations. Operations Research Journal, 67(5), 1020-1032. https://nibmehub.com/opac-service/pdf/read/Operations%20Research%20A%20Practical%20Approach%20by%20Michael%20W.%20Carter-%202ed.pdf

SUBSCRIBE NOW



SUBSCRIPTION RATES

IN INDIA
☐ Rs.500/- per copy

SAARC COUNTRIES
☐ US $ 15 per copy

OTHER COUNTRIES
☐ US $ 20 per copy

☐ Rs.1000/- Annual Subscription (2 issues)

TO SUBSCRIBE SEND YOUR REQUEST TO

Centre for Land Warfare Studies (CLAWS)
RPSO Complex, Parade Road, Delhi Cantt, New Delhi - 110010
Tel: +91-11-25691308
• Fax: +91-11-25692347 • Army: 33098
E-mail: landwarfare@gmail.com
www.claws.co.in

In the evolving dynamics of counterterrorism operations within J&K, the holistic and truthful appraisal of tactical military operations is the foundation for guaranteeing security and strategic victory. Commanders must synthesise assorted intelligence inputs, extending from Human Intelligence (HUMINT) to Technical Intelligence (TECHINT), into comprehensible action plans, thereby guaranteeing that tactical choices are precisely directed and dynamically responsive to evolving threats. This intellectual thoroughness in decision-making is critical to aligning all lines of operation towards the dominant objective of neutralising terrorist threats, thus optimising resource utilisation, and diminishing collateral penalties. This further involves the key concepts integral to enhancing tactical efficacy of identifying terrorist vulnerabilities, including intelligence dependencies and behavioural stressors, and the recognition and mitigation of persistent operational errors such as the Errors of Convenience, Visibility, Attribution, and Justification. By providing an orderly synthesis, this analysis endeavours to equip commanders and policymakers with actionable frameworks.

• • •

Brigadier Navneet Bakshi, commissioned into the MARATHA Light Infantry, has served for over 30 years. An Infantry officer with extensive operational experience, he has spent more than two decades in Counter-Terrorist operations in Jammu & Kashmir and the North East. He has commanded and served in critical appointments along both the Northern and Western borders.

A graduate of the Defence Services Staff College (DSSC) and the Higher Defence Management Course (HDMC), he has been an instructor at the SC Wing and is a subject matter expert in capital procurement and defence budgeting. The Officer is presently serving as a Senior Research Fellow at the Centre for Land Warfare Studies (CLAWS).

The Centre for Land Warfare Studies (CLAWS), New Delhi, is an independent Think Tank dealing with contemporary issues of national security and conceptual aspects of land warfare, including conventional & sub-conventional conflicts and terrorism. CLAWS conducts research that is futuristic in outlook and policy oriented in approach.

CLAWS Vision: To be a premier think tank, to shape strategic thought, foster innovation, and offer actionable insights in the fields of land warfare and conflict resolution.

CLAWS Mission: Our contributors aim to significantly enhance national security, defence policy formulation, professional military education, and promote the attainment of enduring peace.

Website: www.claws.co.in Contact us: landwarfare@gmail.com

SABRE & QUILL

MRP: ₹ 100.00 US$ 5.00