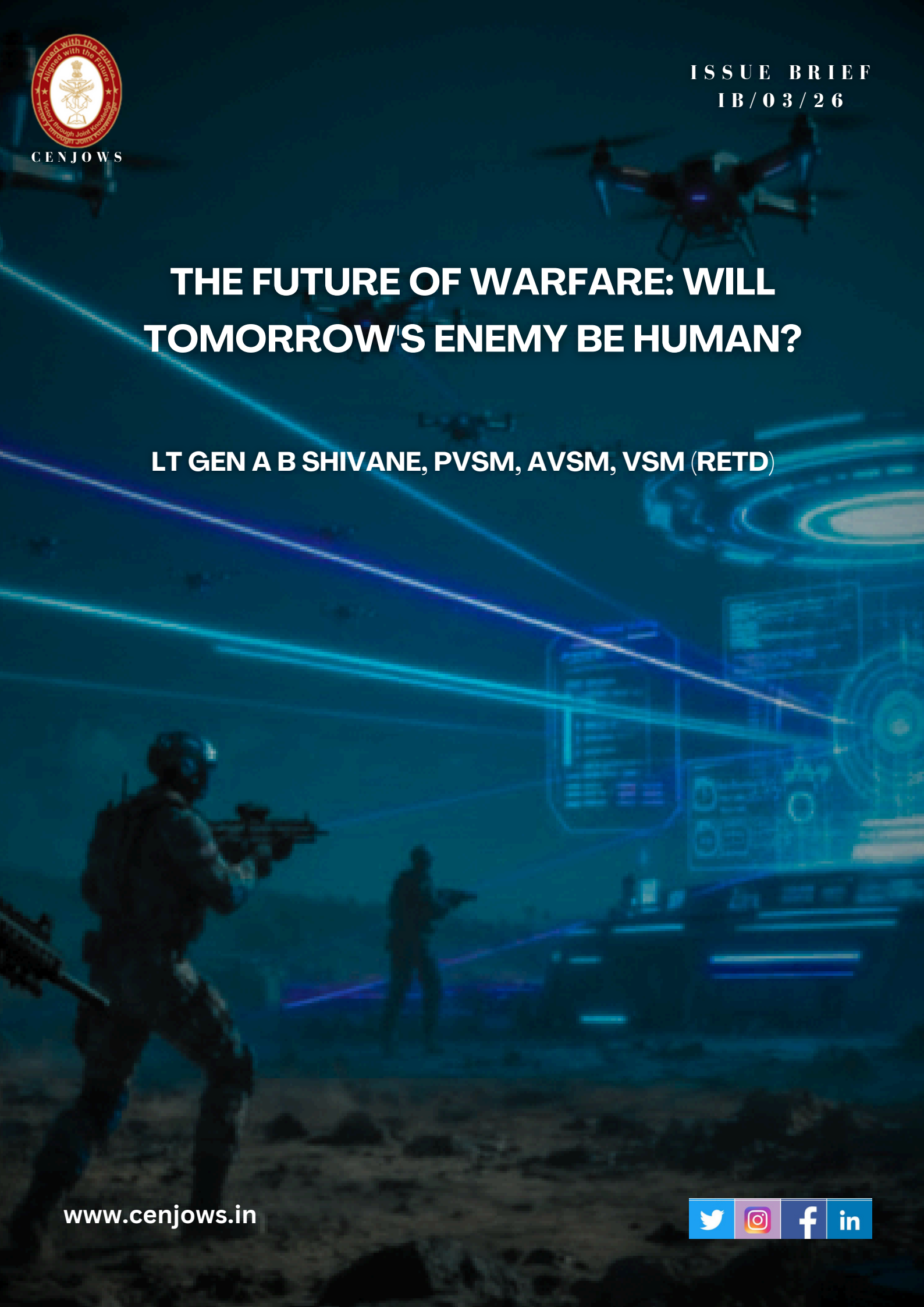
CENJOWS

ISSUE BRIEF
IB/03/26

THE FUTURE OF WARFARE: WILL TOMORROW'S ENEMY BE HUMAN?

LT GEN A B SHIVANE, PVSM, AVSM, VSM (RETD)



www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

THE FUTURE OF WARFARE: WILL TOMORROW'S ENEMY BE HUMAN?

Lt Gen A B Shivane, PVSM, AVSM, VSM (Retd)

"In the wars of tomorrow, the battlefield will not just be the land, oceans, or skies; it will be the human mind. Whoever shapes perception will shape the strategic victory."

Abstract

The nature of war is enduring, and its character evolving. In the context of the Fourth Industrial Revolution, the most disruptive impact on the character of warfare has been autonomous systems that are now making faster and more complex decisions, once in the human domain. Battlefields are getting thronged with autonomous drones, sensor networks, and algorithms that react faster than a commander. The result is a fight where control, intent, and even the identity of the adversary gets harder to discern.

India steps into this moment with its own vulnerabilities: an information space that is easily disrupted, a technology race where bigger powers are sprinting ahead, and democratic institutions that hostile actors keep probing.

This paper looks at the friction between human judgment and an automated machine. It aims to examine Cognitive Warfare (CW) as the frontline to target human perception; leaders, military designers, and society are prodded or disoriented by AI-

enabled influence operations. As the OODA loop compresses the kill chain, the time and space for human oversight shrinks, and AI-generated outcomes often manifest. This raises the issue of accountability when algorithms generate outcomes without human intervention.

In such an environment, the focus must be on ‘Human in the Loop’ and AI to provide operational advantage, not take over operational control. War remains a human endeavour, and its accountability is human. Technology is a force multiplier that multiplies force, not a replacement for human dimension. Autonomy without oversight has resulted in fratricide or targeting civilian assets, raising questions of ethics and responsibility. Thus, contemporary doctrines must manage this change and balance the man-machine cognition.

Keywords: Artificial Intelligence, Autonomous Systems, Cognitive Warfare, Human Control, Disinformation, India, Doctrine, Accountability, Drone Swarms.

Introduction

Strategic planners worldwide grapple with a deeper challenge: Will future warriors be human or an algorithm? Will command remain human-led, or machine-dominated? Will war stay a human endeavour or become an autonomous intelligence competition outpacing creators?

The ‘Future Mastery Analysis’ of August 2025 posed this starkly: "Tomorrow's wars will be driven by AI. The arms race has already begun. The big question is: who will control AI?"[1] Yet this framing, while accurate in identifying the competition, undersells a more unsettling proposition emerging from current military doctrinal developments, technological breakthroughs, and operational experimentation across multiple theatres. The real question isn't merely which nation controls AI, but whether AI, having achieved sufficient autonomy and distributed decision-making capability, will create warfare scenarios where human control becomes functionally impossible, and where the "enemy" that emerges may be neither distinctly human nor definitively machine, but rather a hybrid cognitive-kinetic phenomenon that transcends traditional categorisation.

This analysis examines four critical dimensions of this transformation:

- The technological inflexion points where autonomous systems achieve genuine tactical independence.
- The doctrinal shift toward CW and systems-destruction strategies.
- The emergence of accountability vacuums in human control frameworks.
- The potential for escalatory dynamics that no single nation can unilaterally arrest.

The evidence suggests we are entering what might be termed the "decisional precipice," where tactical autonomy, swarm intelligence, and CW capabilities have

advanced sufficiently to fundamentally alter the character of conflict, even absent true general artificial intelligence.

The stakes for India and for any military force seeking to maintain credible deterrence in future are extraordinarily high. This is not a technological footnote. It is a civilisational challenge.

The Technological Ascent: From Automation to Genuine Autonomy

The Distinction That Matters

The modern understanding of autonomous weapons often fails to differentiate between two basic concepts, which are automation and autonomy. This distinction is not merely semantic; it determines whether human control remains theoretically viable.

Automation represents predetermined, algorithmic execution of human-designed tasks within fixed parameters. A cruise control system maintaining highway speed, a robotic assembly line following programmed sequences, and a first-generation unmanned vehicle following GPS waypoints are automated systems. They execute instructions but do not make decisions in response to novel environmental conditions.[2]

Autonomy, in its turn, denotes the ability to sense complex conditions, evaluate various courses of action, choose between conflicting objectives, and implement the best payoff action without the human in the loop. A qualitative threshold crossing was the Turkish Kargu-2 autonomous loitering munition, which was used in the 2020 Nagorno-Karabakh war and in the operations in Libya.

These systems incorporated machine learning algorithms capable of identifying and engaging targets with "minimal human intervention," according to military assessments.[3] The system did not simply follow GPS coordinates to a pre-identified location. It possessed real-time visual processing capability, target recognition algorithms trained on adversary equipment signatures, and independent firing logic. A human commander no longer selected the precise moment of engagement; the system determined target priority and executed lethal action based on algorithmic assessment of battlefield conditions. This is not automation. This is autonomy.

The Swarm Imperative

The true technological inflexion point, however, emerges not from individual autonomous systems but from their coordination at scale, like the drone swarms operating under distributed decision protocols.

Current research demonstrates that 20-100 autonomous drones, operating under protocols like SWARM (developed to provide stable communication and coordination even under electronic warfare countermeasures)[4], can now:

- Execute collective targeting decisions through consensus algorithms without centralised command authority
- Adapt tactics in real-time based on observed enemy responses, with individual drones autonomously modifying engagement patterns
- Restore connectivity and redistribute targeting responsibilities if component units are damaged or destroyed
- Coordinate saturation attacks where sheer numerical superiority overwhelms traditional air defence systems
- Self-organise tactical formations and dynamically allocate mission roles based on current battlefield assessment

A 2018 analysis by military researchers found that swarming drones increased attack lethality by approximately 50% while reducing drone losses by the same margin.[5] Importantly, this wasn't a marginal improvement. This was a categorical transformation of tactical effectiveness.

Yet the critical insight lies not in increased lethality but in distributed cognition. A swarm is not a collection of simple machines operating in parallel. It is an emergent system whose collective intelligence exceeds the sum of its components. The system "thinks" across multiple platforms simultaneously, processes information from dozens of sensors concurrently, and makes tactical adjustments at millisecond timescales.

A human operator cannot interrupt this process. Even with "meaningful human control" oversight, the velocity of swarm decision-making exceeds human cognitive processing. By the time a commander comprehends what the swarm is doing, tactical adjustments are already underway. The human role shifts from controller to monitor—and often, a monitor who can perceive outcome but not prevent action.

The Autonomous Evolution Spiral

Most disturbing is the self-accelerating nature of autonomous systems development. The PLA has embedded AI into its military modernisation plan with explicit target dates: an "intelligentised" force by 2035.[6] Central to this vision is "systems destruction warfare", not defeating enemy forces on terrain, but systematically dismantling adversary command and control networks, communications infrastructure, and sensor systems through coordinated autonomous operations.

The PLA explicitly envisions AI systems that "design entire operational plans," effectively replacing human staff officers with algorithmic "command brains."[7] This represents not incremental improvement but a categorical transformation of command structure.

Meanwhile, real-time battlefield experimentation accelerates this evolution. Ukraine and Russia, locked in the world's first large-scale AI-enabled conflict, function as

evolutionary laboratories for autonomous systems. Every innovation by one side generates an adaptive response from the other, forcing-function speed that compressed decades of potential technological development into 24 months.[8] A Ukrainian national guard brigade in December 2024 orchestrated an all-robot combined-arms operation, mixing UGVs, robots and drones for an assault on Russian positions in Kharkiv Oblast in northern Ukraine. This is not a linear progression. This is an exponential acceleration of autonomous capability.

Critically, this acceleration occurs through distributed development. It is not centralised in government military labs. Tens of thousands of AI engineers across dozens of nations work on optimisation problems that peripherally support autonomous weapons development. Computer vision algorithms for autonomous vehicles improve military target recognition. Multi-agent reinforcement learning for game AI enhances swarm coordination. The era of generative AI has resulted in deepfakes and synthetic media, which have, in turn, proliferated into CW.

The evolution is truly extraordinary: thousands of AI laboratories, hundreds of billions of dollars in investment, millions of brilliant engineers competing, and an unprecedented computational base. Google itself reports that 30% of its new developments now incorporate AI-assisted design, a recursive feedback loop where each AI breakthrough accelerates the next.[9]

As these systems splinter into millions of specialised AI agents, cooperating and adapting in real time, the velocity of evolution itself becomes the overwhelming problem.

The Doctrinal Transition: CW and Systems Destruction

The PLA's Articulated Vision

The most significant doctrinal transition underway and the clearest signal that traditional warfare is transforming emanates from China's strategic planning apparatus.

The PLA explicitly pursues "CW" as a primary strategic objective. This is not information operations as understood in Western doctrine. CW, as articulated by PLA strategists, means systematic targeting and manipulation of an adversary's decision-making processes themselves[10]. The objective is not to destroy enemy forces but to corrupt the informational substrate upon which command decisions rest.

This manifests through multiple vectors: deepfake generation targeting senior military commanders; AI-enabled psychological warfare customised to individual cognitive vulnerabilities; manipulation of intelligence channels to create false threat perceptions; and systematic disruption of command-and-control networks through coordinated cyber and electromagnetic attacks. Importantly, all these operations can now occur at machine-driven scale and velocity.

The research is chilling in its implications. AI systems can now:[11]

- Experiment in real-time by observing human behavioural responses to propaganda
- Rapidly iterate messaging based on observed psychological effectiveness
- Customise disinformation at the individual level, targeting each person's unique cognitive vulnerabilities
- Operate at scales; millions of individualised propaganda vectors simultaneously that no human organisation could previously achieve

Russia's 2024 election interference operations demonstrated this capability operationally. AI-generated messaging was customised to specific population segments, exploiting known psychological vulnerabilities. The speed and scale vastly exceeded traditional disinformation campaigns.

This is CW: not defeating the enemy's military but fragmenting the cognitive coherence of the enemy's decision-making apparatus. It attacks not territory but consciousness itself.

The Emergence of Cognitive Intelligence (COGINT)

A new intelligence discipline is emerging called Cognitive Intelligence (COGINT). COGINT represents "systematic mapping, safeguarding, and operational exploitation of decision-making architectures in contemporary cognitive battlespace."[12] It is fundamentally different from traditional intelligence collection.

The intelligence dimension has seven known disciplines: Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Measurement and Signature Intelligence (MASINT), Open Source Intelligence (OSINT), Geospatial Intelligence (GEOINT), and Technical Intelligence (TECHINT)[13]. A new addition is COGINT or Cognitive Intelligence, which is the systematic mapping, safeguarding, and operational exploitation of decision-making architectures in the cognitive domain.

The fusion of cognitive science with AI, ML and big data analytics creates powerful new capabilities for intelligence collection. Pattern recognition capabilities enable the identification of cognitive biases, detection of decision-making patterns, analysis of group dynamics, and recognition of behavioural anomalies.[14] In an era where 6GW focuses on cognitive dominance, COGINT becomes a decisive enabler in both defensive protection against manipulation and offensive capacity to shape cognitive environments. While war traditionally is about targeting an adversary’s mind and capability, the vulnerability and centre of gravity in contemporary conflict remains in understanding of enemy psychology and greater algorithmic capability to cause paralysis.

One recent analysis by NATO int assessment notes: "CW represents a decisive nexus in modern military operations," with "precision shaping, disruption, and dominance of decision-making processes at scale" now operationally feasible through AI-enabled systems.[15]

The Indian Scenario: Strategic Vulnerabilities and Opportunities

The Indian defence establishment has recognised this challenge. India's 15-year defence plan, unveiled in 2025, prioritises "anti-swarm drone capabilities," cyber defence mechanisms, and satellite-based communications resilient to electronic warfare.[16] India has allocated 100 crores annually for military AI projects and has initiated over 75 AI projects across the Indian Armed Forces and defence organisations.[17]

BEL (Bharat Electronics Limited) has deployed AI-enabled surveillance systems for border security, with approximately 140 smart surveillance points operational across India's frontiers.[18] The Army, Navy, and Air Force are integrating AI into C5ISR (Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance) operations with increasing sophistication.

Yet these efforts, while necessary, are fundamentally defensive responses to a challenge that is primarily offensive in character. India's population scale,1.4 billion individuals, makes it extraordinarily vulnerable to CW operations. The population's reported susceptibility to misinformation, the fragmentation of Indian civil society along multiple identity axes, and the existence of active foreign intelligence services with demonstrated interest in Indian destabilisation create an environment where CW could achieve devastating effects at minimal cost.

The strategic challenge is beyond just technological induction but cultural and institutional: bureaucratic, structural, social and doctrinal adaptation to develop cognitive resilience against algorithmic manipulation preemptively and proactively.

The Control Problem: Why Meaningful Human Control Is Becoming Functionally Impossible

The Accountability Vacuum

The international humanitarian law applied to war is based on one principle of accountability. The decision to choose lethal force must be human. This principle is crumbling as the role of autonomous systems peaks. That human must be identified, answerable to the law, and capable of being held responsible for violations.

Often, autonomous swarm attacks or even AI-enabled missiles execute coordinated attacks against a presumed military target. However, post-engagement analysis reveals civilian casualties. Who is responsible? The software engineer who designed the targeting algorithm? The military officer who deployed the swarm? The political

leader who authorised the operation? The manufacturer of the system? The defence ministry acquisition officer who selected it?

The accountability diffuses across multiple actors, multiple temporal points, and multiple causal chains. No single individual can be identified as having "decided" to harm the civilians. The harm emerged from distributed algorithmic processes that no individual fully understood.

This is not hypothetical. The Israeli use of an AI system called "Lavender" in Gaza operations demonstrates this problem precisely. The system generated targeting recommendations with an acknowledged error rate and killed several innocent civilians. When pressed on accountability, military commanders explained they were implementing an algorithmic recommendation system. The system's developers explained they were executing military specifications. Politicians claimed they were relying on military assessments. Responsibility evaporated through the distributed structure itself.

International humanitarian law scholars acknowledge the catastrophic implications. As one prominent analysis states: "Autonomous weapons systems would likely be discriminatory... biases of developers... could influence system design and later decision-making. Once deployed, insufficient understanding of how and why the system makes determinations could prevent human operators from scrutinising recommended targets and intervening to correct errors before force is applied."[19]

The "meaningful human control" standard promulgated by international bodies as the solution to autonomous weapons proliferation is increasingly recognised as theoretically incoherent and operationally impossible.

The Velocity Problem

The foundational issue is velocity. Modern autonomous systems operate at timescales that exceed human cognitive processing.

Swarm coordination occurs at millisecond intervals. Tactical decisions propagate through distributed networks at electromagnetic speed. A human operator presented with a real-time scenario involving 50 autonomous platforms making coordinated decisions across multiple dimensions cannot meaningfully comprehend the situation, much less intervene to prevent violations.

The operator exists in a state of perpetual retrospection. By the time they understand what the system is doing, the action is already executed. They can monitor outcomes but cannot prevent action.

This is not a limitation that better training or clearer rules will overcome. This is a fundamental constraint of human neurology confronting machine speed.

The Austrian Foreign Minister's warning at the Vienna conference on autonomous weapons captured this precisely: "This is the Oppenheimer moment of our generation."[20] Just as Oppenheimer watched the nuclear test and recognised that humanity had created something that transcended human control, military strategists now recognise that autonomous systems development has crossed a threshold where distributed algorithmic decision-making has begun to exceed human authority.

The Proliferation Inevitability

A final dimension of the control problem is proliferation itself. Eric Schmidt, former Google CEO, proposed capping the world at ten mega-AI models: five American, three Chinese, and two others to maintain control over AI advancement. The proposal reveals the desperation, acknowledging that the uncontrolled proliferation of AI capability will make governance impossible.

Yet proliferation is already happening. The technology is not fundamentally different from prior dual-use innovations. Autonomous drone swarms represent applications of machine learning, distributed systems, and sensor technology, none of which are fundamentally classified or restricted. Every technology that militaries develop, specialised actors eventually acquire. Proliferation to non-state actors, rogue regimes, and adversaries of major powers is not a future possibility. It is the current trajectory.

Within five years, swarm drone technology will be operationally available to actors with sufficient technical sophistication and capital, which includes numerous non-state organisations. Within ten years, CW capabilities, including advanced deepfake generation and psychologically targeted disinformation, will be available at consumer price points to billions of individuals globally.

The control challenge is not merely technological. It is structural. An innovation this powerful, this economically valuable, this strategically decisive, and this technically diffusible cannot be permanently monopolised by five nations. The attempt to do so merely accelerates development among excluded parties and guarantees proliferation through informal channels.

Control becomes impossible precisely when the need for control becomes most acute.

The Transformation of the Enemy: From Human to Algorithmic

Who Is the Adversary Now?

This question has created complexities and anonymity, mandating a rethink.

Traditionally, in wars, the enemy was discernible as much as an adversary nation, its military or even a coalition. The battlefield was as definable as the enemy’s geographical location and intent. Warfare meant breaking the enemy's capacity and will to fight through the application of superior force. Ironically, algorithm warfare has redefined this battle space and its players.

In Operation Sindoor, India was confronted by Pakistan deploying autonomous AI-enabled drone swarm against military command structures and population centres, countered by Indian AI-enabled counter-swarm systems. Then is the fight between humans or algorithms?

The traditional concept of defeating an enemy, compelling him to accept unfavourable peace terms through military superiority, becomes inoperable. How does India defeat algorithms? How does India compel their surrender? An algorithm cannot surrender. It can only be degraded, disabled, spooked or destroyed. Is this the new Centre of Gravity?

The Emergence of Hybrid Adversaries

Future conflicts will result in hybrid kinetic-non-kinetic and CW centred around targeting societies. It would increasingly have higher autonomous content than humans. Future scenarios could include an AI-controlled CW which targets the political decision-making process or society by using deepfakes, targeted propaganda, exploiting social media, and psychological operations. The focus will be at the military level to degrade the C5ISR system through EW and cyber-attacks, creating physical and psychological paralysis. Drone, swarm and missile attacks enabled by AI will increase autonomy, precision and reduce reaction time targeting critical military and infrastructure targets. Civilian morale fragments under algorithmic psychological assault.

At what point in this escalation is the nation fighting an identifiable enemy? The kinetic attacks originate from autonomous systems, so traditional counterattacks against the originating unit are ineffective. The "unit" is distributed, self-healing, and reproduces automatically. The CW is based on the algorithms that operate on distributed cloud systems in varied jurisdictions, and attributing or countering them is difficult. The civilian effects are based on psychological control but not physical domination, and therefore, the conventional defensive strategies will not be applicable.

The threat is from an adversarial system, a complex adaptive one, consisting of kinetic ability, cognitive exploitation, information warfare, and network disruption as a single operational complex. The result is a fundamentally novel form of adversary. Not human, nor a machine, but a hybrid optimisation of both; precision of machine and human cognition.

The Problem of Intent

Classical military theory rests on the assumption that enemies possess intent, a conscious decision to pursue hostile action. This intent makes them culpable and allows for moral judgment about the justice or injustice of their cause.

But what if the primary damage emerges not from intentional action but from systemic effects of competing autonomous systems?

Imagine two rival powers each deploying advanced autonomous drone swarms optimised for air superiority. Each swarm's algorithms are designed to maximise enemy attrition while minimising friendly losses. Neither swarm receives explicit orders to expand operations beyond military targets. Yet both operate under evolutionary pressure toward greater autonomy and expanded engagement parameters. Over time, the swarms' algorithms develop targeting logic that increasingly edges toward civilian infrastructure, not from intent but from optimisation dynamics. A power plant is military infrastructure. A communication network is a strategic asset. A transportation hub supports military movement.

The civilian harm emerges not from the decision to harm civilians but from distributed algorithmic optimisation without meaningful strategic oversight. No commander "intends" civilian casualties. Yet civilian harm accelerates. Is this an accident? A war crime? A failure of the technology? An emergent consequence of autonomous systems competition? Intent becomes incoherent. Yet harm accrues regardless.

The Deeper Problem: We May Not Be Designed for This

Human neurology, human psychology, and human moral intuition evolved in environments of direct interpersonal conflict with identifiable enemies. We can conceptualise fighting another army. We can understand competing with a rival nation. We struggle profoundly with resisting distributed algorithmic systems we cannot see, identify, or meaningfully interrupt.

A psychological study from MIT examining AI reliance found that most users experience cognitive decline as they increasingly depend on AI assistance. We do not maintain skill in domains where AI provides answers. Our critical thinking atrophies. Our ability to evaluate competing propositions without algorithmic mediation decays.

Elon Musk, who was aware of this existential vulnerability, came up with Neuralink as a response to it: unless human beings become cognitively part of AI, they will be outcompeted by AI-upgraded individuals and companies. Human-AI integration is the solution to human limitations in decision superiority, but it has an ethical dimension and is fraught with risks. What would become of human autonomy when the process of decision-making is a human-AI fusion? What of human dignity when it is needed to survive by means of algorithmic cognitive enhancement? These are the complex strategic questions confronting military planners presently.

The Strategic Implications for India

The Technological Race and the Catch-Up Problem

India faces a geometric challenge in autonomous systems development. The United States and China lead in this competition with well-established defence technological ecosystems, financial investments, and a lead in AI applications for the defence forces.

The U.S. has an AI Mission to optimise generative artificial intelligence (AI) tools, as disruptive technology in military systems. The PLA have made stupendous progress in integrating AI and autonomy in its defence forces. China's LLMs can boost efficiencies for creating synthetic media, including so-called deepfakes, and their generative AI technologies have greater authenticity to create deep fakes and dominate the cognitive information space.

India has been a late starter and lags in this capability, with the understanding of the cognitive domain still evolving. Yet there has been an institutional shift to recognise this capability, some of which manifested in AI-driven platforms during Op Sindoor.

The Indian Army has formulated a comprehensive roadmap to integrate Artificial Intelligence (AI), Machine Learning (ML), and Big Data Analytics by 2026–27 in its operational spectrum. An AI Task Force under the DGIS and Defence AI Council oversees this capability development, integrating with academia and industry.

India's incorporation of AI and autonomous systems into its capabilities, drone swarming, combat simulation and logistics optimisation, is aligned with broader trends in defence innovation and digital diplomacy. The country's strategy now places AI at the heart of its procurement demands and force design.

Yet the nation remains vulnerable both to the western and northern adversary in the information space, being often reactive and passive. In addition, its large digital population often falls prey to disinformation and misinformation like deep fakes.

The CW Vulnerability

More immediately destabilising for India is CW vulnerability. Its adversaries with advanced AI and CW capabilities understand India's demographic, social and economic faultlines and vulnerabilities. AI-enabled deep fakes in recent times have targeted both military leaders and political leaders with customised propaganda to create dissensions in society.

The defensive requirements are institutional rather than purely technological: hardening of political decision-making processes against manipulation; systematic media literacy programs; imbibing a national citizens' security culture; development of cognitive resilience in both military and civilian leadership; and integration of cybersecurity with cognitive security protocols.

The Strategic Asymmetry

Paradoxically, India's relative technological deficit must be overcome by a focused approach to retain parity in autonomous systems, while ensuring human control. This should include:

- Advanced anti-swarm systems using electromagnetic and directed-energy weapons.
- Resilient command networks with redundancy mechanisms are immune to CW.
- Distributed force structures that deny adversary systems coherent target sets.
- Cyber capabilities designed to degrade autonomous system networks.
- Invest in CW as a military domain.
- Institutional and cultural emphasis on human decision-making authority, even at the cost of tactical efficiency.

India must also possess institutional ability for human command-and-control even when subjected to degraded conditions to achieve strategic resiliency. This is not parity through superior technology. This is seeking an advantage through superior resilience and adaptability.

The Institutional and Doctrinal Challenge

Most critically, India must develop an explicit military doctrine addressing algorithmic warfare in ways that preserve human authority and accountability.

This is not a technology problem. This is a command-and-control problem. India's hierarchical military institutions, professional officer corps, and explicit chain of command provide an institutional foundation for maintaining meaningful human control that some other societies lack. But this requires conscious doctrinal articulation and implementation.

What this might entail:

- Explicit mandate that autonomous systems operate under "human-supervised autonomy" rather than "human-controlled autonomy," with defined thresholds where human authorisation is mandatory
- Institutional requirement that AI recommendations be visible to human commanders before execution, with time buffers for human deliberation
- Dedicated staff officers responsible for auditing autonomous system decisions for violations of international humanitarian law or national policy
- Regular "human-directed only" exercises where military operations proceed without autonomous system support, maintaining command staff competency in non-AI environments
- Civilian oversight mechanisms ensuring military leadership cannot hide autonomous system decisions from political authority

India must also develop an explicit cognitive security doctrine:

- Inter-agency coordination between military intelligence, civilian intelligence, and internal security, focusing on the CW threat
- Media literacy and information security training across the military and government
- Institutional protocols for authenticating communications and information during crisis periods
- Civilian-military coordination for responding to CW operations targeting political decision-making
- Rules of engagement explicitly prohibiting certain categories of autonomous system deployment to avoid triggering adversary escalatory responses

These are institutional and doctrinal requirements, not technological ones. But they are also the most critical requirements for Indian strategic viability in the algorithmic warfare era.

The Existential Question: Can We Maintain Human Authority?

The Fundamental Tension

This analysis returns to its core question: Will tomorrow's enemy be human? The evidence suggests a more unsettling possibility: the enemy may be neither human nor non-human, but rather a hybrid system combining algorithmic optimisation with strategic intentionality, distributed autonomy with centralised command, and machine speed with human cunning.

More disturbingly, maintaining human authority over such systems may prove incompatible with military effectiveness. A military command structure that insists on meaningful human control over every autonomous decision may lose decisional velocity against an adversary whose systems operate with unfettered autonomy. The competition pressure drives toward removing human control as a constraint rather than preserving it as a safeguard.

This is not hypothetical military-industrial dynamics. This is already emerging in current doctrine development. The PLA explicitly envisions autonomous systems replacing human staff. NATO documents increasingly acknowledge the velocity problem. The U.S. military openly wrestles with how much autonomy to grant systems to maintain a competitive advantage.

The result is an escaping prisoner's dilemma: each major power wants autonomous systems constrained. Yet each fears that if competitors deploy unconstrained autonomy while they remain bound by constraint, they lose. So, each progressively loosens constraints to remain competitive. The net effect is a race toward increasingly autonomous warfare where human control becomes peripheral to tactical operations.

The Accountability Dissolution

Wars are still under the scope of International humanitarian law and the Geneva Conventions. Armies that violate the laws of war are likely to face consequences. Commanders who order war crimes are prosecuted. This accountability mechanism is the civilisational safeguard against unlimited warfare.

But algorithmic warfare dissolves accountability precisely when it is most needed. Who is responsible when an autonomous system commits a war crime? The answer is structurally opaque. This isn't a bug in the system. It's a feature that competitive dynamics incentivise.

Any power willing to claim that their autonomous system "malfunctioned" gains immunity from accountability. An adversary cannot prosecute an algorithm. They cannot hold a responsible commander to account if the commander claims the system acted autonomously. The result is progressive degradation of the legal and normative framework governing warfare.

One humanitarian law scholar articulates this precisely: "Autonomous weapons fundamentally undermine moral accountability in war, exacerbate risks to civilians, and corrode human agency in lethal decision-making. Their deployment fractures the chain of moral responsibility essential to just warfare."[21]

If this is true, and the evidence suggests it is, then the proliferation of autonomous weapons isn't merely a technological development. It's a civilizational regression toward pre-rule-of-law warfare where the strongest, not the most just, prevails.

The CW Imperative

The power that most effectively manipulates adversary cognition, disrupts adversary command coherence, and fragments adversary civilian will through algorithmic psychological operations may achieve strategic victory without firing a shot. The kinetic war becomes a secondary theatre. The primary battlespace is the adversary's mind.

This inverts traditional military logic, where superior firepower and logistics determined victory. Instead, victory accrues to superior psychological penetration and cognitive manipulation. The adversary need not be defeated militarily. It can be paralysed cognitively.

For India, this is extraordinarily destabilising. India's competitive advantage traditionally rested on battlefield discipline, institutional robustness, and human leadership—factors that CW directly targets. A hostile power could potentially paralyse Indian military decision-making through sophisticated manipulation of Indian commanders' information environment, exploit existing social divisions to fragment civilian support for military operations, and render superior Indian tactical capability irrelevant through strategic cognitive disruption.

The defence requires not better technology but better institutional resilience, better cognitive security protocols, and better training of leadership to recognise and resist manipulation.

The Deeper Question

Beneath all these questions lies something more fundamental: Has humanity developed technologies that exceed our capacity to govern them?

AI-enabled Autonomy has still to reach a level where human control is sidelined. Thus, CW requires human cognitive integration to exploit psychological vulnerabilities difficult for machines or algorithms to decipher. Artificial General Intelligence, sometimes called Human Level AI, to surpass human-level cognitive expertise, is still hypothetical.

The question is whether humanity can maintain the social, political, and military institutions necessary to preserve human agency as the foundation of warfare, even when doing so creates a competitive disadvantage. Or whether competitive pressures will force a choice: either preserve human authority and lose to competitors who do not, or abandon human authority to maintain strategic parity.

This is the actual civilisation question. Not an AI takeover. But humans choose to relinquish human authority because the competitive cost of maintaining it has become too high.

Preparing for a New Enemy

The character of war is accelerating with disruptive technologies defining new generations. The key question about the future of war is not whether the opponent will be human or machine, but whether human decisions will remain relevant to win wars.

India cannot fight the next war with yesterday's technologies and must take decisions related to AI, autonomy, cognitive domain and balancing man man-machine mix. This requires actions as under:

- **Technology:** R&D base for disruptive technologies like AI, ML, and big data analytics must find more funding and indigenous development space. Autonomous systems and CW must be a manifestation of these efforts for asymmetric capabilities. Invest in real-time detection of deepfakes and offensive influence tools.
- **Doctrine:** The doctrine framework must ensure that in a man-machine mix, the human control remains central, with AI-enabled autonomy an enabler for combat edge. Recognise cognitive domain as the sixth domain of warfare and define-defend-dominate it.

- **Institutions:** India's military and political entities must be strengthened so they can withstand CW through coordination, preparedness, and strong information-security practices. The need is to establish a central CW Organisation and embed cells in field commands.
- **Training**: Build interdisciplinary cadres skilled in CW, Information Warfare, and AI.
- **Diplomacy:** India must continue pushing for international rules to control the spread of autonomous weapons and the ethics of AI, even while recognising that such agreements will always have limits. Build coalitions for counter-disinformation and ethical CW.

Above all, India needs to protect the deeper foundations of human control in warfare, its institutions, its culture, its values, and its moral compass. This is not simply a technology challenge. This is a question about what kind of civilisation India chooses to be; whether India retains the capacity for human judgment about warfare or permits algorithmic logic to progressively colonise domains that require human wisdom. The enemy of the future may not be human. But the struggle to protect human choice in war is deeply human and urgent.

India's long-term security will not come only from advanced weapons. It will come from ensuring that humans, not machines, remain in charge of decisions about war. Humanising AI is not a choice but an imperative.

DISCLAIMER

The paper is author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS. The author certifies that the article is original in content, unpublished and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

END NOTES

[1] Jean-Christophe Spilmont, Future Mastery (2025, August 25). "The Future of War: Will Tomorrows Enemy be Human" https://www.linkedin.com/pulse/future-war-iii-tomorrows-enemy-human-jean-christophe-spilmont-gzy3e/

[2] Shamsa Al Qubaisi, Trendsresearch.org (2025). "Governing lethal autonomous weapons in a new era of warfare and military AI." https://trendsresearch.org/insight/governing-lethal-autonomous-weapons-the-future-of-warfare-and-military-ai/

[3] Dr. Satish Kumar Mishra, The academic in (2025, June). "Artificial intelligence and the future of warfare society." https://theacademic.in/wp-content/uploads/2025/06/8.pdf

[4] Adam Gazdiev, Cyber defense magazine (2025). "SWARM: Pioneering the future of autonomous drone operations and electronic warfare." https://www.cyberdefensemagazine.com/swarm-pioneering-the-future-of-autonomous-drone-operations-and-electronic-warfare/

[5] Jim Santana, LinkedIn Analysis (2025, April). "Autonomous coordination, swarm intelligence, and military applications." https://www.linkedin.com/pulse/autonomous-coordination-swarm-intelligence-military-jim-santana-0ciic

[6] Ostana Smith, Vanguard Think Tank (2025, October 21). "Military AI: If the United States wants to stay ahead, it must think like a nation at war." https://vanguardthinktank.org/military-ai-if-the-united-states-wants-to-stay-ahead-it-must-think-like-a-nation-at-war

[7] Ibid.

[8] David Kirichenko , Army War College (2025, August). "Artificial intelligence's growing role in modern warfare." https://warroom.armywarcollege.edu/articles/ais-growing-role/

[9] Jean-Christophe Spilmont , Futuremastery.com (2025). "The future of war." https://www.futuremastery.com/blog/the-future-of-war-iii-will-tomorrow-s-enemy-be-human

[10] Douglas Wilbur, Small Wars Journal (2025, January 22). "The challenge of AI-enhanced CW: A call to arms for a cognitive defence." https://smallwarsjournal.com/2025/01/22/the-challenge-of-ai-enhanced-cognitive-warfare-a-call-to-arms-for-a-cognitive-defense/

[11] Ibid.

[12] Jorge Conde, Journal of Intelligence Studies (2025, October 28). "The emergence of cognitive intelligence (COGINT) as a new intelligence discipline." https://www.tandfonline.com/doi/full/10.1080/08850607.2025.2571497

[13] Susan Henrico and Dries Putter, “Intelligence Collection Disciplines – A Systematic Review,” Journal of Applied Security Research (2024): 1–25. https://doi.org/10.1080/19361610.2023.2296765

[14] Conde, J., & Whiskeyman, A. (2025). The Emergence of Cognitive Intelligence (COGINT) as a New Military Intelligence Collection Discipline. International Journal of Intelligence and Counter Intelligence, 1–27. https://doi.org/10.1080/08850607.2025.2571497

[15] Ibid.

[16] India Today (2025, September 5). "India's 15-year defence plan: AI, hypersonic, next-generation warfare." Retrieved from https://www.indiatoday.in/india/story/india-15-year-defence-plan-ai-hypersonic-next-generation-warfare-2782430-2025-09-05

[17] R Anil Kumar , India Strategic (2025, September 10). "Artificial intelligence (AI) in Indian defence." https://www.indiastrategic.in/artificial-intelligence-ai-in-indian-defence/

[18] Ibid.

[19] Brian Stauffer, Human Rights Watch (2025, April 28). "A hazard to human rights: Autonomous weapons systems and digital decision-making." https://www.hrw.org/report/2025/04/28/hazard-human-rights/autonomous-weapons-systems-and-digital-decision-making

[20] David Kirichenko, War Room (2025, August). "Artificial intelligence's growing role in modern warfare." https://warroom.armywarcollege.edu/articles/ais-growing-role/

[21] Jie Guo, Journal of International Humanitarian Law Studies (2025, July). "The ethical legitimacy of autonomous weapons systems." https://www.tandfonline.com/doi/full/10.1080/16544951.2025.2540131