CENJOWS

ISSUE BRIEF
IB/42/26

ALGORITHMIC WARFARE: A NEW PARAGIGM IN THE AGE OF ARTIFICIAL INTELLIGENCE

GP CAPT ASHISH KUMAR GUPTA (RETD)

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

CENJOWS

Algorithmic Warfare: A New Paradigm in the Age of Artificial Intelligence

Gp Capt Ashish Kumar Gupta (Retd) is a Senior Fellow at CENJOWS, New Delhi.

The development of warfare is closely connected to the development of humanity. War didn't just happen out of the blue; it was a natural result of plans to stay alive. In antiquity, war did not emerge out of nowhere but was a logical extension of the strategies to survive. As humanity evolved from primitive hunter-gatherer societies to advanced and complex civilisations, the trajectory of warfare also changed.[1] Sometimes, this trajectory followed a linear path with only a minor increase in severity and impact, while other times it leapt exponentially in the wake of new technologies, strategies, or both.[2] Modern warfare, shaped by artificial intelligence and quantum computing, is both a continuum of the past and an inflexion in its trajectory. In prehistoric times, the violent interactions between Neanderthals and early Homo sapiens were infrequent, geographically confined, and had not yet developed into a formalised institution. Even in these early times, some rules of war were clear: using simple weapons, working together, making plans, and hurting people. As human societies became more equal, people stopped living in nomadic groups and started living in permanent places. As a result, war changed too, becoming more organised.[3] The early civilisations in Mesopotamia, Egypt, and the Indus Valley transitioned to more structured forms of warfare, with organised armies and specialised weapons.

Warfare became a preferred tool for asserting/preserving political authority and expanding territories.[4]

The war is no longer an armed conflict between two standing armies trying to subdue each other. It became a canvas of strategic art made vivid by the evolution of military doctrines and strategic thought.[5] Today, warfare has entered the era of artificial intelligence and quantum computing, a transitional journey that could be termed a move toward algorithmic warfare. The transformation of warfare, from its primitive form in the hunter-gatherer age to the industrial age and now in the algorithmic warfare era, is not merely a transition in the use of weapons or platforms.[6].

Industrial warfare emphasised mass, mechanisation, and national resource mobilisation. Decision-making was hierarchical and suffered from individual biases. The philosophical aspect of this era was eloquently articulated by Carl von Clausewitz, whose 'theory of war' underpinned its political framework and unpredictability. Clausewitz defined war as "the continuation of politics by other means," amalgamating warfare and statecraft into one unified concept[7]. He propagated well-known ideas such as the fog of war, friction, and the centre of gravity to highlight military complexity and unpredictability; however, during the industrial era, battles mainly focused on attrition. The victory or defeat depended on the quality of intelligence, logistical constraints, and the limitations of communication technology. The sluggishness of information gathering, the cumbersome analysis process, post-analysis decision-making, dissemination of orders, and rigid chain of command structures inhibit commanders' ability to shorten the OODA loop (Observe, Orient, Decide, Act) beyond limits.

Clausewitzian Perspective on War

Clausewitz's theory has stood the test of time. It is largely independent of technological advancements and focuses more on human and psychological dimensions. In a war, the long and short-term outcomes remain largely unpredictable. Even the most sophisticated systems can commit errors, leading to unimaginable consequences. Uncertainty and unforeseeable outcomes stemming from technical breakdowns, miscommunication, human limitations, and human errors impact military operations. Identifying the centre of gravity provides an opportunity to mitigate an adversary's strength. However, as warfare evolved from the 20th century to the digital era, it

became evident that a strictly Clausewitzian perspective had its constraints. The rapid tempo of contemporary operations, the plethora of information, and the growing complexity of military systems created demands that exceeded the limitations of traditional decision-making methods. Clausewitz provided profound insights into the nature of war; nonetheless, his paradigm lacks a definitive approach to address the rapidity and volatility of contemporary battlefields.

John Boyd's OODA Loop

In this context, John Boyd developed the OODA loop, a framework that altered how the military decision-making process was understood. Boyd's Observe, Orient, Decide, Act model treated conflict less as a sequence of fixed moves and more as a continuous interaction between adversaries attempting to anticipate, disrupt, and outpace one another. What mattered was not simply firepower or numerical strength, but the ability to process unfolding events faster and more coherently than the opponent.

The model gained influence partly because it reflected the uncertainty of real combat situations. Decisions in war are rarely made with complete information. Commanders observe fragments, interpret them through prior experience and training, and then act under pressure. During the Gulf War, for example, coalition forces benefited from faster information flow and more flexible command structures, while Iraqi responses often lagged behind the changing battlefield conditions. Boyd's framework captured that imbalance fairly well. It suggested that confusion and delay could weaken an adversary even before physical destruction became decisive.[8] The OODA loop offered something slightly different from the more philosophical treatment of war associated with Carl von Clausewitz. Clausewitz was concerned with the nature of war, uncertainty, political intent, and friction. John Boyd, however, seemed more interested in how decisions are actually made under pressure and how one side can disrupt the opponent's ability to respond coherently. His framework feels more operational, perhaps because it emerged from practical military experience rather than abstract theory alone. Boyd argued that success in conflict depends less on making perfect decisions and more on making workable decisions faster than the adversary can process events. That distinction matters. In combat, waiting for complete clarity often

means reacting too late. A force that adapts quickly, even if imperfectly, may unsettle an opponent still trying to interpret the situation. One can see traces of this thinking in modern manoeuvre warfare, where tempo and initiative frequently outweigh rigid control.

The idea also fits naturally with decentralised command structures. Lower-level commanders are expected to respond to changing conditions without constantly waiting for higher approval. During the Gulf War, for instance, coalition forces benefited from faster information flow and more flexible command arrangements than Iraqi forces, whose responses were often slower and tightly centralised. Still, Boyd's model is not without limits. Faster decisions do not automatically produce better outcomes, especially when information itself is manipulated or incomplete. Yet the enduring appeal of the OODA loop probably lies in its realism. War rarely allows enough time for certainty, and militaries that recognise this tend to organise themselves differently. The OODA loop is frequently credited with accelerating decision-making, and that reputation is justified to a considerable extent. Yet the framework depends heavily on human cognition, which introduces complications that are harder to standardise than military doctrine sometimes assumes. The limitation becomes especially visible during the orientation phase. This is the stage where raw information is interpreted, filtered, and given meaning, and that process is far from neutral.

John Boyd understood that people do not process information in identical ways. Experience, training, institutional culture, personal assumptions, and even stress levels shape how a situation is interpreted. Two officers may receive the same intelligence feed and still arrive at different conclusions about what is unfolding. One may see a tactical opportunity, while another sees escalation risk. The variation is not necessarily irrational. It reflects the subjective nature of perception itself. This becomes more pronounced under operational conditions. Human attention is limited, especially in environments saturated with information. Fatigue, cognitive bias, and emotional strain can narrow judgment at precisely the moment clarity is most needed. Recent conflicts have shown instances in which commanders acted on incomplete drone feeds or misread electronic interference. The problem was not a lack of data but difficulty in interpreting it accurately in real time.

Therefore, the effectiveness of the OODA loop seems tied to more than speed alone. Fast decisions made through distorted perception may create confusion rather than advantage. What matters, perhaps, is the quality of cognition under pressure, the ability to adapt, filter noise, and revise assumptions before the situation changes again.[9]

The entry of artificial intelligence and large-scale data analytics into warfare has started to alter how military decisions are made, and perhaps more significantly, who or what is making them. Decision-making was once assumed to be an essentially human function shaped by judgement, intuition, training, and experience under pressure. That assumption now appears less stable. In many operational settings, machines are no longer limited to supporting commanders with background calculations. They increasingly assist in identifying targets, filtering intelligence feeds, prioritising threats, and recommending responses at speeds that human staff struggle to match.

This shift has contributed to what is often described as algorithmic warfare. The phrase can sound slightly exaggerated at times, yet the underlying change is real enough. Modern military systems generate enormous volumes of data through satellites, drones, sensors, radar networks, and communications intercepts. Human operators cannot process all of it in real time. AI-enabled systems, however, can scan patterns across vast datasets within seconds, flag anomalies, and produce assessments while events are still unfolding. Recent conflicts have offered partial demonstrations of this trend. In the Russia-Ukraine conflict, for example, automated data fusion and drone-supported targeting shortened the time between detection and strike. Similar developments are visible in maritime surveillance, where AI tools track vessel movement patterns that would overwhelm human analysts if done manually.

Still, the idea of removing humans entirely from the decision loop remains contentious. Machines may process faster, but speed alone does not guarantee sound judgement. Algorithms operate within the quality of the data and assumptions used to train them. Misidentification, biased datasets, or manipulated inputs can quickly distort outcomes. Even so, AI systems increasingly compress every phase of the OODA loop, often

forcing human decision-makers to react at a pace shaped by machines rather than by deliberate reflection.[10]

In the observation phase of the OODA loop, military systems now pull in enormous amounts of data from satellites, drones, radar stations, communication intercepts, and ground sensors spread across different operational domains. The volume alone makes purely human interpretation difficult. During orientation, algorithmic systems begin filtering this information, searching for patterns, flagging anomalies, and attempting to produce a coherent operational picture from what is often fragmented or contradictory input. The process appears efficient, although the clarity generated by algorithms can sometimes create a misleading sense of certainty.

The decision phase increasingly relies on predictive analytics that propose workable courses of action along with estimated probabilities and projected outcomes. Commanders may still retain formal authority, yet their choices are often shaped by machine-generated recommendations delivered at speeds that are difficult to challenge in real time. In some settings, especially missile defence or autonomous drone operations, delays of even a few seconds can alter outcomes. Action introduces another shift. Once authority is delegated to autonomous or semi-autonomous systems, execution may occur with minimal human intervention. Air defence systems already operate in this manner under certain conditions, reacting faster than human operators could reasonably manage. However, reducing human involvement also narrows opportunities for hesitation, reinterpretation, or restraint. The OODA loop, therefore, becomes compressed by automation, with machines accelerating each phase while humans increasingly supervise processes they may no longer fully control in practice.

From Human-Centric to AI-Mediated Decision Cycle

AI-enabled decision systems have begun to compress time in warfare in ways that would have seemed unrealistic only a few decades ago. Decisions that once moved through layers of analysis, discussion, and authorisation over several hours, sometimes longer, can now unfold within seconds or even milliseconds. Missile defence systems already operate at such speeds because human reaction alone is

often too slow to intercept incoming threats. The broader consequence, however, is more unsettling than simply “faster warfare.”

This acceleration has increasingly been described as “Hyperwar,” a term introduced in 2019 by John R. Allen and AI researcher Amir Husain[11]. The phrase refers to the sharp compression of the OODA loop, where observation, orientation, decision, and action occur at machine speed rather than at a pace shaped by human deliberation. In practical terms, AI systems can analyse sensor feeds, identify patterns, prioritise threats, and trigger responses before human operators fully interpret the situation.

Yet the issue is not merely speed. Human cognition struggles when events unfold faster than meaningful reflection becomes possible. Under such conditions, commanders may gradually shift from active decision-makers to supervisors monitoring automated processes they cannot realistically evaluate in real time. Supporters of AI-driven warfare argue that this reduces hesitation and improves responsiveness. Critics, however, worry that compressed timelines leave little room for judgement, restraint, or reconsideration once systems begin to interact autonomously. The concern, therefore, is less about machines becoming intelligent in an abstract sense and more about warfare increasingly unfolding at a tempo where human intervention starts to feel structurally delayed.

In the decision-making process, the human-in-the-loop dependence evolves into human-out-of-the-loop. In the ‘algorithmic warfare’ realm, the pace of war accelerates in proportion to machine processing speed. In Hyperwar, the decision-maker's role, traditionally assigned to humans, is increasingly being entrusted to machines. As AI systems become more intelligent and powerful, humans’ cognitive limitations will impede the decision loop. Consequently, human decision-makers will be under pressure to delegate greater authority to machines.

The Algorithmic War Paradigm

In algorithmic warfare, the components that traditionally add up to define the extent of military power have somewhat regressed from their preeminent positions. These have been replaced by data, communication, and computational prowess. The ability to amass troops, spur industrial production, and boost firepower, though a determinant

in war, is under pressure to maintain its exalted position as AI and machine learning capabilities are increasingly relied upon to achieve a favourable outcome in a conflict. The centre of gravity shifts from physical assets to information dominance and decision superiority[12]. Information superiority is not a completely new paradigm but rather an evolutionary one, which, according to some experts, is more of a revolutionary phenomenon. This paradigm has prompted a relook at many foundational concepts and discourses. The command-and-control structures need to be reconfigured to integrate AI systems into decision-making processes under watchful human oversight. The decisions, emanating from command-and-control structures, need to be executed by actors, either human or machine or both, to achieve objectives in the shortest possible time.

The doctrinal, strategic, and tactical progression from Clausewitz's insights to Boyd's OODA loop to AI-enabled decision-making does not represent discrete breaks in the evolution of warfare. In warfare, each progression is an appendage that enhances the capability of existing and enduring principles.

Carl von Clausewitz remains difficult to dismiss even in an era shaped by artificial intelligence, precision weapons, and real-time surveillance networks. His argument that war is ultimately tied to political purpose still explains more than many technologically focused theories sometimes admit. Advanced military capability may alter the speed and scale of conflict, yet it does not remove uncertainty or guarantee political success. The ongoing tensions and conflict involving Iran, the United States, and Israel illustrate this rather sharply[13]. Military operations, economic pressure, covert activity, and diplomatic coercion are all tied to larger political objectives. For the United States and Israel, these objectives have included constraining Iran's regional influence, weakening its nuclear infrastructure, and, in some circles at least, encouraging internal political change. Iran's priorities appear narrower but no less political: regime survival, strategic deterrence, and maintaining relevance within regional power dynamics. Yet battlefield or technological superiority has not translated neatly into political resolution. Airstrikes may damage infrastructure and degrade military capability, but they do not automatically produce stable outcomes or compel political surrender. The persistence of ceasefire negotiations, indirect bargaining,

sanctions, and international pressure suggests that the conflict remains shaped by calculations extending far beyond military exchanges alone.

Clausewitz anticipated something close to this problem. Tactical or operational success can coexist with political ambiguity. A state may dominate militarily and still struggle to secure the conditions it originally sought. The present conflict reflects that tension. None of the principal actors appears to have fully achieved the political objectives that justified escalation in the first place, which perhaps explains why the conflict continues to shift between confrontation, restraint, and uneasy negotiation rather than reaching any decisive endpoint.

In the ongoing confrontation involving Iran, the United States, and Israel, John Boyd's OODA loop framework appears visible in fairly practical ways. Each side is constantly observing battlefield developments, collecting intelligence, interpreting signals, and adjusting responses as conditions change. Surveillance systems, intercepted communications, satellite imagery, drone feeds, and cyber intelligence all feed into this cycle. Information is gathered quickly, filtered, assessed, and then pushed toward decision-makers who must act before the situation shifts again.[14] However, the conflict also exposes the fragility of the process. The OODA loop assumes a certain level of clarity between observation and action, yet modern conflict rarely offers that stability. Intelligence can be incomplete, manipulated, delayed, or politically filtered before it reaches commanders. Electronic interference, disinformation, and asymmetric tactics complicate interpretation at every stage.

Iran's approach has been particularly disruptive in this respect. Rather than relying purely on conventional military confrontation, it has often used proxy networks, dispersed operations, calibrated missile attacks, cyber activity, and strategic ambiguity. Such tactics slow the opponent's orientation phase by making intentions harder to interpret. A drone strike, for example, may simultaneously convey military signalling, political messaging, or deterrent intent. That ambiguity forces adversaries to spend more time assessing risk before responding. As a result, even technologically superior actors can find their decision cycles strained. The issue is not necessarily a lack of capability. It is the difficulty of maintaining coherent judgement when the

operational environment is deliberately designed to generate uncertainty faster than clear conclusions can be reached.

In many cases, their orientation and response cycles have been derailed. The tactical advantages accrued from air superiority fail to translate into long-term strategic gains owing to Iran's ability, despite being under intense air strikes, to adapt militarily and reorient politically. Boyd's OODA loop relevance has been reaffirmed in the Iran conflict, showing that cognition and adaptability, rather than just destruction, lead to a position of relative strategic advantage.

Algorithmic warfare, despite having a nice ring to it, sounds like a term yet to be copiously used in military parlance. Yet it has already made inroads into the military lexicon, shaping how modern wars are fought. In algorithmic warfare, algorithms are central: they process vast amounts of fragmented and unstructured data, turn them into actionable insights, and assist in decision-making. Algorithms can even be tailored to automate decisions to make autonomous choices. Think of a drone identifying a target not through a pilot's intuition but through pattern recognition trained on thousands of images. Or surveillance systems that flag "suspicious behaviour" long before any human analyst has time to look. It is efficient, undeniably so. Still, for some of us, empowering lines of code to undertake parts of warfare autonomously is unsettling.

Algorithmic warfare ramps up the tempo of task execution. High-stakes decisions requiring a significant amount of time running into hours, even days, for background research, analysis, and deliberation can be compressed into seconds. In the Iranian conflict, the U.S and Israel reportedly used AI-assisted systems to identify a list of targets, which even the best human brains could never match within a given time frame.

Palantir Technologies and the US Military.

The relationship between the U.S. military and Palantir Technologies has grown far more extensive than the company's early image as a niche analytics firm might suggest. Over the past decade, Palantir has become increasingly embedded within the American defence ecosystem, particularly in areas involving intelligence

integration and operational decision support. Its platforms, especially Gotham and the newer Artificial Intelligence Platform (AIP), are designed to pull together information from very different sources: satellite imagery, drone feeds, signals intelligence, logistics data, and human reporting[15].

For military commanders, the appeal seems fairly practical. Modern battlefields generate fragmented and often contradictory information at overwhelming speed. One surveillance feed may indicate troop movement, while intercepted communications suggest something different. Systems like Palantir attempt to organise these inputs into a continuously updated operational picture that commanders can interact with in real time. During high-pressure situations, including tensions involving Iran, such consolidation can shorten the gap between observation and decision.[16]

However, this also shifts the role of software within military structures. Palantir no longer functions merely as a background support tool handling isolated data analysis. Its platforms increasingly shape how information is prioritised, interpreted, and presented to decision-makers[17]. That distinction matters because the structure of information often influences the decisions themselves. Supporters argue that integrated systems reduce confusion and improve operational responsiveness. Critics, however, worry about growing dependence on algorithmic filtering that commanders may not fully understand or challenge under time pressure. The concern is less about a single company gaining influence and more about how military judgement gradually adapts to software-generated realities that appear coherent, even when the underlying data may still contain uncertainty.

In recent years, the relationship between the U.S. military and Palantir Technologies has expanded well beyond conventional intelligence support. Its software platforms, including Gotham, Foundry, and the Artificial Intelligence Platform (AIP), increasingly operate closer to the centre of operational planning and battlefield management. They assist with mission planning, sensor fusion, logistics coordination, and the construction of a live operational picture drawn from multiple streams of information. The demand for such systems reflects the pace and complexity of contemporary warfare. Modern battlefields produce far more data than human staffs can comfortably process in real time. Supersonic aircraft, long-range precision missiles, drone swarms, loitering

munitions, satellite feeds, and signals intelligence systems all generate continuous inputs that change by the minute. Under combat conditions, expecting a commander to absorb fragmented information from several disconnected systems and still make coherent decisions quickly seems increasingly unrealistic.

This is where Palantir's role becomes significant. Its platforms attempt to fuse scattered inputs into a single operational interface, reducing the delay between observation and response. A commander no longer needs to move manually between separate intelligence feeds, communication systems, and targeting displays. The software organises and prioritises information before it reaches the decision-maker. However, the deeper implication may lie elsewhere. As military organisations rely more heavily on integrated AI-driven systems, software begins shaping how battlefield reality itself is perceived. Decisions may appear faster and more coherent, yet they are also increasingly filtered through algorithmic structures that commanders do not always fully interrogate under pressure. The issue, therefore, is not merely efficiency. It is how military judgement gradually adapts to machine-curated understanding of war.

Palantir Technologies appears to have moved beyond supporting the traditional "kill chain" model toward something closer to a distributed kill web architecture. The older kill chain framework followed a relatively linear sequence: detect, identify, target, engage. Contemporary battlefields, however, rarely function in such an orderly manner. Information now flows simultaneously across satellites, drones, ground sensors, cyber networks, naval platforms, and airborne systems, often with multiple actors interacting simultaneously. Palantir's platforms seem designed for this more networked environment. Instead of treating military operations as isolated chains of action, they integrate multiple sensors, intelligence streams, and decision nodes into a continuously connected operational structure. A drone detecting movement, a satellite capturing imagery, and a signals intelligence platform intercepting communications can all feed into the same system, almost in real time.

The shift matters because modern warfare increasingly rewards adaptability over rigid sequencing. If one sensor or platform fails, another can potentially fill the gap. That flexibility resembles a web more than a chain. At the same time, such

interconnectedness creates dependence on software integration and uninterrupted data flow. The architecture becomes more resilient in some respects, yet perhaps more vulnerable to disruption, overload, or manipulation in others. The classic kill chain follows a linear trajectory, with transitions occurring in sequence, i.e., one step followed by another. The traditional model is usually described as: finding the threat, fixing its position, tracking its movement, targeting it, engaging it, and assessing the result. Each phase can commence only after the preceding phase is successfully completed. The kill chain model loses its viability and effectiveness in contested environments where multiple domains operate simultaneously. A disruption in any link can interrupt the chain. Palantir's systems help in moving beyond that linear structure into a networked kill web.[18]

From Kill Chain to Kill Web

Algorithmic warfare is accelerating the transition from the traditional kill chain to the modern kill web. In an age of multiple-domain systems operating simultaneously, a linear kill chain becomes highly susceptible to disruptions at any step[19]. A single broken link could bring the whole process to a grinding halt. This is where the accruable advantages of algorithmic warfare come to the fore. AI systems can ingest unprecedented amounts of data simultaneously from various sources, identify patterns, quantify threats, and recommend commensurate responses. Instead of a sequential flow of information, one step at a time, multiple nodes in the network can be primed to act on information derived from the same shared picture. The process becomes distributed rather than sequential. In effect, algorithms act like spiders, weaving the threads of information received from separate sensors and shooters into a web of options.

Still, there is no panacea for addressing war-associated uncertainties[20]. Conceptually, a kill web appears to be the perfect solution, yet wars are inherently ambiguous. Algorithms, no matter how well trained, could misread patterns and offer options that, when evaluated with cognitive oversights, will be costly and impractical. Though the transition from kill chain to kill web, using algorithms, is strategically significant, it does not eliminate fog and friction or rid commanders of moral responsibility.

Some may argue that entrusting machines, especially in war, with decision-making capabilities seems dehumanising, as it empowers them to make decisions against humans (enemy soldiers) based on calculation rather than moral understanding. Decisions that carry the weight of life and death need to be conscience-driven, empathetic, and contextual. A machine can identify patterns and, sometimes, recommend actions based on probabilistic inferences. When the anthropocentric qualities are removed from the decision-making process, war becomes a dehumanised endeavour without any emotional mooring and risks becoming more mechanical and emotionally distant. Killing may begin to look like a technical task rather than a grave human act.

However, it would also be inaccurate to brand algorithmic warfare as purely dehumanising. The targeting decisions made by algorithms enable precision targeting, reducing collateral damage compared to older, less discriminating methods. Early warning systems might help in climbing down the escalation ladder before a hostile threat materialises. Across the globe, powerful militaries have embraced technologies that promise greater control. Algorithmic systems are another addition to this upward trajectory, though the impact and autonomy they offer do feel different.
Warfare today can be characterised by a hybrid model that combines elements of all three paradigms: Clausewitzian theory, Boyd's OODA loop, and algorithmic decision-making.

None of these paradigms is capable of addressing present-day strategic challenges on its own. Carl von Clausewitz argued that war remains an extension of politics pursued through violent means, and despite dramatic technological change, that observation still feels difficult to escape. States do not go to war simply because they possess advanced weapons or autonomous systems. They fight to secure political objectives, alter strategic conditions, compel behaviour, or preserve regime survival. Recent conflicts, including the Nagorno-Karabakh conflict, the Russia-Ukraine conflict, and ongoing confrontations in the Red Sea and wider Middle East, reflect this fairly clearly. Military operations may appear technologically sophisticated, yet they remain tied to political intent underneath the machinery.

At the operational level, John Boyd's OODA loop introduces another layer to the discussion. Modern battlefields move quickly and often unevenly. Drone strikes, missile defence systems, cyber operations, and electronic warfare compress the time available for interpretation and response. Commanders are expected to observe changing conditions, interpret fragmented information, make decisions, and act before the adversary adapts. In practice, the side that cycles through this process more coherently tends to gain a temporary advantage, even without overwhelming force.

Artificial intelligence complicates the picture further. AI systems can process vast streams of sensor data, identify patterns, and generate recommendations at speeds beyond human cognition. This considerably accelerates the OODA loop, especially in information-saturated environments. Yet the deeper shift may not simply be faster warfare. Human judgement increasingly operates inside machine-shaped timelines. Political objectives still guide war in the Clausewitzian sense, but algorithmic systems now influence how quickly military organisations move toward those objectives, sometimes before deliberation fully catches up.

A more workable approach may lie in a hybrid model that draws selectively from each paradigm rather than treating any single one as sufficient on its own. Political judgement in the Clausewitzian sense still matters because wars continue to revolve around strategic objectives and human consequences. Boyd's emphasis on tempo, adaptability, and decision advantage remains relevant in fast-moving operational environments. At the same time, AI-driven systems offer clear advantages in processing data, identifying patterns, and reducing delays in complex battlespaces.

Relying entirely on one framework appears increasingly limiting. Human judgement alone struggles under the volume and speed of modern warfare, yet fully automated decision-making introduces risks of miscalculation and overdependence on algorithmic interpretation. A blended model, therefore, seems more practical, where machines assist with speed and data integration while humans retain responsibility for interpretation, restraint, and political intent. The balance may never remain stable for long, though that instability itself probably reflects the nature of contemporary conflict. Clausewitzian theory will shape both the political purpose and the strategic extent of war[21]. The adaptability and pace of strategic and tactical plans will align with Boyd's

theory. Algorithm-driven systems will drive sensing, analysis, and coordination efforts across domains. The coming together of these three paradigms defines war as political, cognitive, and computational simultaneously.[22]

Strategic decision-making will continue to be predominantly anthropocentric, rooted in individual conditionings, judgment, training, and contextual understanding. On the other hand, an AI system will be entrusted with operational and tactical decisions, as well as execution, to elicit fast, proportional responses. The challenge is to effectively enmesh these three paradigms, leading to the realisation of strategic objectives driven by technological advantages, tactical efficiency, and operational competence. However, there are doctrinal and ethical challenges that need fresh perspectives and strategic insights. The technology is evolving at an unprecedented pace, untethered from ethical frameworks meant to guide it - the formulation and implementation of international law struggle to remain relevant and face challenges to universal acceptance.

The deeper challenge may not be machine autonomy itself, but how human cognition gradually adjusts to living and operating alongside it. That adjustment is unlikely to happen smoothly. Military organisations can introduce advanced autonomous systems relatively quickly; changing human judgement and behavioural habits takes far longer. People are conditioned to question, interpret, and intervene. Fully trusting automated systems, especially in high-stakes environments, does not come naturally, even when those systems consistently outperform humans in speed and data processing.

At the same time, overreliance creates a different problem. Psychologists often describe this tendency as “automation complacency,” where operators become excessively confident in automated outputs simply because the system has worked reliably in the past[23]. Commercial aviation has already demonstrated aspects of this issue. Pilots managing highly automated aircraft sometimes lose situational awareness precisely because routine tasks are handled so effectively by software until an abnormal event suddenly demands rapid human intervention.[24]

A similar risk exists in military systems driven by AI-supported targeting, missile defence, or battlefield management software. When machine-generated assessments

align with expectations, operators may stop questioning them closely. Ambiguous data can be overlooked, contradictory signals ignored, or flawed outputs accepted without sufficient scrutiny. The difficulty emerges when the system encounters conditions outside its training assumptions. Human intervention is then expected to recover control quickly, although by that stage the operator may already be cognitively detached from the decision process.

Highly automated systems, therefore, do not necessarily reduce the need for human cognition. They alter its character. Instead of continuously controlling operations, humans increasingly supervise, interpret exceptions, and intervene during failure conditions. That sounds manageable in theory. In practice, regaining control over a fast-moving automated process under pressure may require a different kind of judgement than military institutions have traditionally trained for.

Conclusion

The character of contemporary warfare seems increasingly shaped by an uneasy interaction between older strategic thought and rapidly evolving technology. Carl von Clausewitz still feels relevant because, despite drones, AI systems, and autonomous weapons, wars continue to revolve around political objectives. States use force to secure deterrence, preserve influence, maintain regime survival, or alter strategic balances. The tools have changed dramatically. The underlying motivations are perhaps less than expected. At the operational level, John Boyd’s OODA loop has gained renewed importance precisely because modern conflict moves at such uneven speed. Military organisations now compete to observe, interpret, and respond faster than their adversaries can adapt. Artificial intelligence intensifies this process by analysing data at scales that exceed human cognition. Satellite feeds, drone imagery, signals intelligence, cyber inputs, and battlefield communications can now be processed almost continuously, compressing the time between detection and action. In that sense, technology has not displaced classical strategic ideas. It has altered the tempo at which those ideas operate.

Yet the rise of algorithmic warfare introduces tensions that military institutions do not seem to have fully resolved. As operational systems shift away from relatively linear kill chains toward networked kill webs, software increasingly shapes how threats are

identified, prioritised, and engaged. Human operators remain present, though their role is gradually shifting from direct control to supervision and intervention in exceptional circumstances. Systems associated with Palantir Technologies illustrate this transition fairly clearly. Integrated AI platforms can improve coordination, reduce informational overload, and accelerate battlefield decisions. However, dependence on algorithmic systems also creates opacity. Commanders may trust outputs they cannot meaningfully interrogate in real time, especially under operational pressure. Overconfidence in automation, combined with compressed decision cycles, risks narrowing opportunities for reflection and restraint.

The deeper issue, then, may not be whether militaries can build more advanced machines. They almost certainly can. The harder question concerns whether political judgement, ethical responsibility, and human accountability can remain intact when warfare increasingly unfolds at machine speed. Future military effectiveness will probably depend less on technological possession alone and more on how carefully states balance automation with disciplined human control.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces, or the Government of India. 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.

ENDNOTES

[1] Lawrence H. Keeley, *War Before Civilization: The Myth of the Peaceful Savage* (New York: Oxford University Press, 1996); Azar Gat, *War in Human Civilization* (Oxford: Oxford University Press, 2006); Jeremy Black, *War and Technology* (Bloomington: Indiana University Press, 2013).
[2] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976); Martin van Creveld, *The Transformation of War* (New York: Free Press, 1991); Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007).
[3] Brian Fagan, *Cro-Magnon: How the Ice Age Gave Birth to the First Modern Humans* (New York: Bloomsbury Press, 2010); Chris Stringer, *The Origin of Our Species* (London: Allen Lane, 2011); Rebecca Wragg Sykes, *Kindred: Neanderthal Life, Love, Death and Art* (New York: Bloomsbury Sigma, 2020).
[4] Azar Gat, *War in Human Civilization* (Oxford: Oxford University Press, 2006); Trevor N. Dupuy, *The Evolution of Weapons and Warfare* (Indianapolis: Bobbs-Merrill, 1980); John Keegan, *A History of Warfare* (New York: Alfred A. Knopf, 1993).
[5] Lawrence Freedman, *Strategy: A History* (Oxford: Oxford University Press, 2013); Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999).
[6] Martin van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York: Free Press, 1989); Lawrence Freedman, *The Future of War: A History* (New York: PublicAffairs, 2017).
[7] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 87.
[8] Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (London: Routledge, 2007).
[9] Ibid.
[10] Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (London: Routledge, 2007); Mick Ryan, *War Transformed* (Annapolis, MD: Naval Institute Press, 2022).
[11] John R. Allen and Amir Husain, *Hyperwar: Conflict and Competition in the AI Century* (New York: Diversion Books, 2021).
[12] Mick Ryan, *War Transformed: The Future of Twenty-First-Century Great Power Competition and Conflict* (Annapolis, MD: Naval Institute Press, 2022).
[13] Reuters, “U.S. Positive on Iran Deal Talks but Still Uncertain as Ceasefire End Nears,” April 21, 2026

[14] Reuters, “Iran Tightens Control of Hormuz After U.S. Calls Off Renewed Attacks,” April 23, 2026.
[15] Palantir Technologies, “About Palantir,” corporate history materials; Christopher O’Donnell, “Palantir and the Military’s Data Problem,” *Defense One*, various reports on Afghanistan and Iraq-era adoption.
[16] Palantir Technologies, “About Palantir,” corporate history materials; Christopher O’Donnell, “Palantir and the Military’s Data Problem,” *Defense One*, various reports on Afghanistan and Iraq-era adoption.
[17] Reuters, “Pentagon to Adopt Palantir AI as Core U.S. Military System, Memo Says,” March 20, 2026.
[18] John R. Allen and Amir Husain, *Hyperwar: Conflict and Competition in the AI Century* (New York: Diversion Books, 2021); Mick Ryan, *War Transformed* (Annapolis, MD: Naval Institute Press, 2022).

[19] John R. Allen and Amir Husain, *Hyperwar: Conflict and Competition in the AI Century* (New York: Diversion Books, 2021).
[20] Hew Strachan, *The Direction of War* (Cambridge: Cambridge University Press, 2013).
[21] Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976); Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Little, Brown and Company, 2002).
[22] Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007).
[23] Raja Parasuraman and Victor Riley, "Humans and Automation: Use, Misuse, Disuse, Abuse," *Human Factors* 39, no. 2 (1997): 230-253.
[24] Herbert Lin and Amy Zegart, eds., *Bytes, Bombs, and Spies* (Washington, DC: Brookings Institution Press, 2018).