Issue Brief #278

April 2026

The Convergence Age: Technology, Power, and the Fragility of Peace

S. Anirudha Rao and Aran Hooda

Contemporary warfare is being redefined by the convergence of AI, space systems, cyber capabilities, autonomous platforms, and emerging technologies into a unified operational continuum. Traditional frameworks centred on asymmetry, domain separation, and sequential escalation are therefore becoming insufficient to unpack the dynamics of modern conflict.

This IPCS Issue Brief examines the convergence across five interrelated domains: AI, space power, unmanned systems, cyber and cognitive warfare, and emerging technologies including quantum and hypersonic systems. Drawing on contemporary conflicts—from Ukraine and Gaza to the Red Sea and South Asia—it demonstrates how converged technologies compress decision cycles, expand the battlespace into civilian infrastructure and public perception, and blur the boundaries between competition and conflict.

Introduction: The Dissolution of Asymmetry

Modern conflict is undergoing a structural transformation driven by the collapse of boundaries between domains.[1] Artificial intelligence, space systems, cyber capabilities, autonomous platforms, and information operations no longer operate in isolation. They increasingly function as a single, interdependent system that reshapes how the battlefield is perceived and conceptualised. For decades, strategists interpreted conflict through the prism of asymmetry i.e. between the strong and the weak, conventional armies and irregular forces. That vocabulary is now insufficient. What defines contemporary warfare is convergence: the fusion of technologies, actors, domains, and decision cycles into one integrated battlespace where advantage flows from speed, integration, and adaptability.

[1] Lawrence Freedman, *The Future of War: A History* (New York: PublicAffairs, 2017)

In this environment, small, networked groups can generate disproportionate effects through drone swarms, narrative manipulation, or digital infrastructure disruption, while major militaries confront the fragility of their own interconnected systems. Power increasingly resides in the ability to integrate technologies, process information rapidly, and maintain resilience under sustained informational and cognitive pressure. As these systems converge, the traditional distinctions between state and non-state actors, front lines and rear areas, and military and civilian infrastructure steadily erode.

The Issue Brief proceeds in four substantive sections. It begins with artificial intelligence, identifying it as the principal accelerator of convergence and examining its impact on targeting, decision-making, and cognition. The second section analyses space as the connective infrastructure of modern conflict, highlighting orbital vulnerability and commercial dependence. The third section explores drones and unmanned systems as visible manifestations of cross-domain integration. The fourth examines cyber and cognitive operations, where infrastructure and perception converge into a continuous battlespace. The report concludes with a discussion on governance, escalation management, and deterrence in the convergence age.

Artificial Intelligence and the New Battlespace

AI as the engine of convergence

Artificial intelligence is no longer an adjunct to warfare but its organising logic. It binds sensors, shooters, decision-makers, and narratives into a single operational rhythm, enabling speed, scale, and integration across domains. Through data fusion, pattern recognition, and automated recommendation, AI compresses decision cycles and accelerates operational tempo, while magnifying error at machine speed when misapplied. In doing so, AI represents the strategic inflection point of the convergence age. It multiplies capability while embedding algorithmic mediation into sovereign decision-making and increasing reliance on private technological infrastructure. This section demonstrates that transformation across five interrelated developments: the shift from decision support to decision dominance; the automation of target selection at scale; divergence in governance frameworks among major powers; the operationalisation of AI-enabled swarming; and the expansion of generative systems into the cognitive domain. Together, these strands illustrate that strategic advantage will accrue not to those who automate fastest, but to those who combine technical integration with assurance mechanisms that preserve human judgment despite algorithmic speed.

Decision support to decision dominance

AI's military impact emerges not through a singular 'wonder weapon', but through a transformation in tempo. During the ongoing Russia–Ukraine war, platforms integrating satellite imagery, drone feeds, and human intelligence enable near–real-time targeting, compressing decision cycles from hours to minutes and allowing smaller forces to strike with disproportionate precision.[2][3] This marks a transition from decision support to decision dominance i.e. the ability to act faster than an adversary can respond. Yet acceleration also reveals a dependency: decisive operations increasingly hinge on proprietary algorithms, privately owned data pipelines and corporate discretion. Strategic leverage thus migrates beyond traditional military command structures. In a converged environment, AI multiplies effectiveness only when transparency, sovereignty, and accountability evolve alongside capability. Speed without assurance creates fragility; dominance without control invites escalation.[4]

Algorithmic targeting at scale

The next inflection point lies in the automation of selection itself. Investigations into Israel's AI-assisted targeting systems, notably Lavender and Gospel, reveal the capacity to process vast datasets and generate strike nominations at machine speed.[5] While the operational gain is tempo, the strategic cost is opacity. Automation bias risks displacing human judgment, while accountability diffuses across data, code, and command structures.[6] As decision chains become algorithmically mediated, traceability of intent erodes. The imperative therefore is to govern technology instead of slowing it. Audit trails, data provenance, and enforceable human oversight are stabilising mechanisms. In converged warfare, discrimination must keep pace with speed.

Ethics and governance of military AI

Recognising these risks, states adopt divergent approaches to responsible AI. The US emphasises human accountability through a human-in-the-loop model within its Department of Defense Responsible AI framework.[7] The EU prioritises traceability and auditability under the Artificial Intelligence Act.[8] These differences are strategic in addition to regulatory. In the absence of shared thresholds for acceptable AI use, escalation control becomes fragile: what one actor perceives as augmented decision-making

[2] Kofman, M., et al. *Military Lessons from the Ukraine War*. CNA, 2022

[3] Watling, J. and Reynolds, N. *Meatgrinder: Russian Tactics in the Second Year of the Ukraine War*. Royal United Services Institute, 2023

[4] Kofman, M., et al. *Military Lessons from the Ukraine War*. CNA, 2022

[5] +972 Magazine. "Lavender: The AI System Behind Israel's Targeting." April 2024.

[6] Chesney, R. and Citron, D. "Deepfakes and the New Disinformation War." *Foreign Affairs*, 2019.

[7] U.S. Department of Defense. *Responsible Artificial Intelligence Strategy and Implementation Pathway*. Washington, D.C., 2022

[8] European Union. *Artificial Intelligence Act*. Official Journal of the European Union, 2024

may be interpreted by another as automated aggression. In a converged environment, misperception travels as fast as data.

Swarming and the speed of war

AI-enabled swarming is the physical manifestation of decision dominance. Programmes such as the US Department of Defense Replicator initiative, alongside parallel efforts in China, Russia, and Iran, aim to deploy large numbers of attritable autonomous systems capable of coordinated action at machine speed.[9][10][11] These systems invert traditional cost equations, allowing low-cost autonomy to saturate high-value defences. In such engagements, outcomes may be determined before human commanders can intervene, compressing decision space and challenging inherited doctrines of command and escalation management.

AI, deepfakes, and cognitive warfare

AI's influence extends beyond kinetic operations. The circulation of a synthetic video in 2022 purporting to show Ukrainian President Volodymyr Zelenskyy urging surrender marks an early demonstration of deepfakes as instruments of psychological warfare.[12] Subsequent cases reveal how rapidly such fabrications can be generated, amplified, and exploited; often faster than they can be credibly debunked.[13] A similar pattern emerges during the 2025 post-Pahalgam India–Pakistan crisis, where manipulated visuals, recycled footage, and AI-assisted narrative amplification circulated widely across digital platforms in the immediate aftermath of the attack.[14][15] Competing interpretations of events gain traction before official clarifications stabilise the information space. In a nuclearised regional context, such velocity of perception risks narrowing diplomatic space and compressing decision-making timelines. These developments signal the convergence of military operations and social manipulation. Generative AI enables deception that can destabilise public trust, distort democratic processes, and complicate crisis response.[16] In this environment, domestic populations are no longer observers but active terrain. Authenticity defence, which includes content provenance, rapid attribution, and trusted public communication, has therefore become as vital to deterrence as air or missile defences.

[9] U.S. Department of Defense. *Replicator Initiative Fact Sheet*. 2023

[10] Congressional Research Service. *Autonomous Weapons Systems and Military Applications*. 2024

[11] Scharre, P. *Army of None: Autonomous Weapons and the Future of War*. W.W. Norton & Company, 2018

[12] BBC News. "Deepfake Video Purporting to Show Zelensky Calling for Surrender." March 2022

[13] Chesney, R. and Citron, D. "Deepfakes and the New Disinformation War." *Foreign Affairs*, 2019

[14] ABC News (Australia), "Misinformation War Rages Online amid India-Pakistan Crisis," May 23, 2025

[15] *Observer Research Foundation*, "Weaponising the Narrative: Social Media Propaganda Post-Pahalgam Attack," *ORF*, May 13, 2025

[16] Peter W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*

AI as the strategic inflection point

By analysing five verticals—decision dominance, algorithmic targeting, governance divergence, autonomous swarming, and generative cognitive systems—this section demonstrates how AI restructures not only capability but also control. It accelerates tempo, expands operational reach, and blurs accountability across public and private actors. As decision cycles compress and human cognitive latency becomes the bottleneck, reliance on AI becomes both operational necessity and strategic risk. The strategic question is therefore not whether AI enhances power, but whether states can retain authority, transparency, and restraint within systems optimised for speed. In the convergence age, stability depends less on automation itself than on governance frameworks capable of aligning machine performance with human responsibility.

Space: The Final Fragile Frontier

Space has become the enabling infrastructure of converged warfare. It is no longer a discrete domain but the connective system that sustains artificial intelligence, unmanned platforms, cyber operations, and real-time command networks. Orbital assets provide the data, timing, and connectivity that allow cross-domain integration to function at machine speed. Without assured access to space-based systems, convergence falters: AI loses data fidelity, drones lose coordination, and cyber operations lose temporal coherence. As a result, control of space increasingly shapes operational tempo on Earth while simultaneously introducing systemic fragility.

Scientific sanctuary to strategic high ground

For much of the Cold War and post–Cold War period, space was framed as a domain of exploration and cooperation under the 1967 Outer Space Treaty.[17] That paradigm has eroded. Dual-use satellites now support civilian connectivity while simultaneously guiding missiles, synchronising forces, enabling drone operations, and feeding AI-driven decision systems. Space has become the strategic high ground, not just a discrete domain, but the infrastructure that binds all others. Without assured access to space, convergence collapses: AI loses data, drones lose coordination, and cyber operations lose timing. Emerging technologies further reinforce this shift. Quantum communication and sensing threaten long-standing assumptions about concealment and survivability. Demonstrations of satellite-based quantum key distribution signal a race to secure communications through physics rather than computation.[18][19] More destabilising is the

[17] United Nations. *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (Outer Space Treaty).* 1967
[18] U.S. Department of Energy. *Quantum Networking and Security Roadmap*. 2023
[19] China Academy of Sciences. *Micius Quantum Science Satellite Experiments*. 2017

prospect of quantum sensing, which could undermine the survivability of submarines or stealth platforms by eroding secrecy itself.[20] When concealment erodes, warning times compress and escalation dynamics destabilise, reinforcing how space now shapes not only connectivity but strategic stability.

The age of anti-satellite weapons

The contemporary ASAT era is often dated to 2007, when China destroyed its defunct Fengyun-1C satellite, generating tens of thousands of debris fragments that continue to endanger spacecraft today.[21][22] Subsequent demonstrations reinforce the message. Russia's 2021 destruction of Cosmos-1408 produced a debris cloud so extensive that astronauts aboard the International Space Station were forced to shelter.[23][24] These events shatter assumptions of orbital invulnerability and reveal a deterrence dynamic rooted in mutual vulnerability. In space, even limited conflict produces persistent debris that degrades the domain for all actors. This is mutually assured disruption without the bomb, a form of deterrence driven by shared exposure to catastrophic externalities rather than moral restraint. Hypersonic glide vehicles and manoeuvrable missiles further compress geography into minutes. Systems under development by Russia, China, and the US destabilise deterrence through speed, manoeuvrability, and payload ambiguity.[25][26] Leaders who once had time to interpret warning data may soon have only moments. In such an environment, misinterpretation becomes as dangerous as malice. Strategic stability therefore depends not only on deterrence in orbit but on crisis communication, shared early-warning mechanisms, and doctrines calibrated for compressed timelines.

Invisible warfare: Jamming, spoofing and cyber intrusions

Kinetic destruction is only the most visible threat to space systems. More prevalent are non-kinetic attacks, such as jamming, spoofing, dazzling, and cyber intrusion, which disrupt satellite services without creating debris or triggering clear attribution. Russia's 2022 cyberattack on Viasat's KA-SAT network disabled tens of thousands of terminals across Ukraine and Europe, degrading military communications at the outset of the conflict.[27][28] Such operations reveal the deep convergence of space and cyber domains.

[20] Stockholm International Peace Research Institute, "Military and Security Dimensions of Quantum Technologies," July 3, 2025
[21] NASA Orbital Debris Program Office. *Fengyun-1C ASAT Test Debris Assessment*. 2007
[22] Secure World Foundation. *Global Counterspace Capabilities: An Open Assessment*. Latest annual edition
[23] Roscosmos and NASA. *ISS Emergency Procedures Following the Cosmos-1408 ASAT Test*. 2021
[24] Weeden, B. "Russian ASAT Test and Orbital Debris Risks." Secure World Foundation, 2021
[25] RAND Corporation. *Hypersonic Weapons and Strategic Stability*. 2022
[26] U.S. Army. *Long-Range Hypersonic Weapon (Dark Eagle) Program Overview*. 2023
[27] Viasat Inc. *KA-SAT Network Cyber Incident Statement*. February 2022
[28] UK National Cyber Security Centre. *Cyber Operations Observed During the Ukraine Conflict*. 2022

Malware targeting ground infrastructure or electronic interference against space-based links can paralyse AI-driven command networks and unmanned systems as effectively as kinetic attacks—while remaining deniable. Space superiority therefore depends as much on cybersecurity, spectrum resilience, and redundancy as on orbital mechanics.

Private space power and commercial dependence

Modern militaries increasingly rely on commercial constellations for communications, imagery, and situational awareness. SpaceX's Starlink network proved decisive in Ukraine by sustaining connectivity after terrestrial networks were degraded.[29] However, reports that service access was curtailed during a Ukrainian operation expose a new vulnerability: corporate decisions can shape battlefield outcomes.[30] While the proliferation of commercial constellations enhances resilience through redundancy, it also blurs civilian and military functions, complicating accountability, neutrality, and control. In a converged battlespace, governance frameworks must ensure that commercial space power reinforces collective security rather than undermining sovereign decision-making.

Space power as a battlefield enabler

The Ukraine conflict demonstrates the democratisation of space power. Commercial imagery providers supply intelligence, shaping both operational planning and public understanding of the war.[31] Near–real-time satellite data is no longer monopolised by superpowers. In a converged environment, AI ingests open-source orbital data, drones exploit persistent coverage, and narratives form in real time. Commanders therefore operate under constant observation, where concealment is fleeting and missteps propagate rapidly across military and cognitive domains.

Governance and the future of orbital stability

Despite its strategic centrality, space is weakly governed. The Outer Space Treaty prohibits weapons of mass destruction in orbit but offers limited guidance on non-kinetic attacks, cyber operations, or debris-generating tests.[32] As low Earth orbit grows increasingly congested, states are advancing voluntary norms, including initiatives on responsible space behaviour and national space policies.[33][34][35] Yet these efforts

[29] Reuters. "Starlink Keeps Ukraine Online Amid Russian Attacks." 2022
[30] Isaacson, W. *Elon Musk*. Simon & Schuster, 2023
[31] Maxar Technologies and Planet Labs. *Commercial Satellite Imagery and Open-Source Intelligence in Ukraine*. 2022–2023
[32] United Nations. *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (Outer Space Treaty).* 1967
[33] Government of India. *Indian Space Policy 2023*. Department of Space, 2023
[34] China Academy of Sciences. *Micius Quantum Science Satellite Experiments*. 2017
[35] U.S. Department of Energy. *Quantum Networking and Security Roadmap*. 2023

remain fragmented and non-binding. In a converged battlespace, fragmented governance is itself a vulnerability. Long-term stability depends on transparency, redundancy, rapid reconstitution, and confidence-building measures that prevent technological advantage from triggering strategic panic.

A crowded sky

This section demonstrates the transformation of the space domain across six interrelated dynamics: its erosion as a scientific sanctuary and emergence as strategic high ground; the proliferation of anti-satellite capabilities; rise of non-kinetic interference including jamming, spoofing, and cyber intrusion; expanding dependence on commercial constellations; democratisation of space-enabled intelligence and surveillance; and persistent governance gaps in orbital stability. Together, these strands reveal a central paradox: space enables convergence across domains, yet its disruption can cascade through every connected system. Preserving stability in the convergence age therefore depends on resilience, redundancy, and governance mechanisms capable of managing shared vulnerability in orbit.

Drones and Unmanned Systems

Drones and unmanned systems represent one of the most visible manifestations of convergence in contemporary conflict.[36] They compress the interval between detection and action, integrate real-time intelligence with strike capability, and reduce the cost of aerial and maritime access. In doing so, they shift the grammar of power away from mass and distance toward speed, precision, and accessibility. Their proliferation challenges traditional deterrence frameworks while simultaneously creating new forms of transparency and vulnerability.

Loitering munitions and tactical drones

Recent conflicts demonstrate that drones are no longer auxiliary assets but integral actors across the tactical spectrum. The 2020 Nagorno-Karabakh conflict showed how the integration of armed drones and loitering munitions dismantled entrenched air defences and armour formations within days.[37][38] Parallel developments in Ukraine continue to reveal how commercial quadcopters, rapidly adapted at the front, enable reconnaissance, targeting, and strike missions at low cost.[39][40] The 2025 India–Pakistan crisis following the Pahalgam attack further illustrated how unmanned aerial systems can serve as

[36] P. W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009)
[37] Secure World Foundation. *Global Counterspace Capabilities: An Open Assessment*. Latest annual edition
[38] Center for Strategic and International Studies, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," December 8, 2020
[39] Kofman, M., et al. *Military Lessons from the Ukraine War*. CNA, 2022
[40] Watling, J. and Reynolds, N. *Meatgrinder: Russian Tactics in the Second Year of the Ukraine War*. Royal United Services Institute, 2023

instruments of signalling and pressure in a nuclearised environment.[41] Cross-border drone activity, including surveillance and reported interdictions, unfolds alongside heightened political tension, reinforcing how low-cost aerial systems can complicate escalation management without crossing conventional thresholds. Together, these cases illustrate drones as force multipliers that grant smaller actors disproportionate capability at minimal cost. The strategic implication is clear: deterrence by accessibility increasingly supplements, and in some contexts, replaces deterrence by exclusivity.

Innovative drone tactics and countermeasures

The evolution of drone warfare has been as cultural as technical. Improvised, field-level fabrication workshops, rapid iteration cycles, and frontline innovation have become decisive advantages. Russian Lancet loitering munitions and Ukraine's modified racing drones exemplify a battlefield ecosystem where adaptation outpaces procurement cycles.[42][43] This proliferation compels a doctrinal rethink. Survival depends not only on counter-drone technologies such as jammers, lasers, interceptor drones, and increasingly directed-energy systems but also on dispersion, deception, and camouflage. Directed-energy weapons, including high-energy lasers and high-power microwaves, operate at the speed of light and offer instantaneous, repeatable engagement against drones and missiles.[44] While often framed as defensive stabilisers, such systems also compress engagement thresholds and introduce ambiguity into escalation dynamics when effects are rapid and attribution uncertain. The 'drone gap' is therefore both technological and cognitive. Forces must relearn how to operate under persistent aerial observation without triggering escalation through indiscriminate countermeasures.

Naval drones and maritime disruption

Unmanned surface and subsurface vehicles are transforming maritime security. Ukrainian naval drones demonstrate the ability to strike high-value targets without conventional fleets.[45] Similarly, Iranian-supplied and Houthi-operated systems in the Red Sea have showed how disproportionate economic and security costs can be imposed.[46] These developments invert naval cost equations: inexpensive unmanned craft can threaten capital ships and global trade. Maritime deterrence now hinges on distributed sensing,

[41] International Institute for Strategic Studies, "India–Pakistan Drone and Missile Conflict: Differing and Disputed Narratives," May 15, 2025
[42] NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Operations and Escalation Management*. 2023
[43] Swedish Defence Research Agency (FOI), "Usage, Effectiveness and Recent Trends of FPV-Drones in the Russian Invasion of Ukraine Based on Published Combat Footage," March 25, 2025
[44] U.S. Government Accountability Office, "Science & Tech Spotlight: Directed Energy Weapons," May 25, 2023
[45] U.S. Navy. *Unmanned Surface and Subsurface Vehicle Programs*. 2024
[46] Reuters. "Houthi Drone and Missile Attacks Disrupt Global Shipping." 2024

rapid interception, and cooperative threat awareness rather than sheer tonnage.

Robotic ground forces and man–machine teaming

Unmanned ground vehicles and robotic combat systems are transitioning from experimental prototypes to operational testing. Major militaries experiment with robotic mules, remote weapon stations, and quadruped systems designed to extend endurance, reduce exposure, and support infantry operations.[47] While still immature, these systems represent a doctrinal inflection point. By lowering casualty risk, they promise humanitarian and operational benefits; yet they may also reduce political thresholds for force deployment. Man–machine teaming therefore demands robust ethical and legal guardrails to ensure that human command remains central to lethal decision-making. The objective should be protection rather than detachment by using machines to preserve human life rather than normalise its loss.

The persistence of instability

This section demonstrates transformation across four interrelated developments: the operational integration of loitering munitions and tactical drones into frontline combat; adaptation of commercial systems for reconnaissance and targeting; expansion of unmanned platforms into maritime and ground domains; and the strategic implications of low-cost aerial proliferation in nuclearised environments. Together, they illustrate how unmanned systems accelerate decision cycles while lowering entry thresholds for force projection. Their affordability and visibility may introduce elements of mutual surveillance that complicate surprise, but without governance frameworks and countermeasures, proliferation risks entrenching persistent instability across air, sea, and land.

Cyber and Cognitive Warfare

Cyber and cognitive operations extend convergence into the informational and perceptual domains, dissolving traditional distinctions between battlefield and society. This section demonstrates that shift across four interrelated dynamics: state-led cyber intrusions as pre-kinetic instruments of disruption; exploitation of zero-day vulnerabilities and compromised supply chains; digitally amplified information operations that shape legitimacy and public perception; and the emergence of synthetic media that blurs authenticity in crisis environments. Together, they show how connectivity itself becomes a vector of both coercion and influence. The same interdependence also creates space for restraint. Strengthened attribution, hardened infrastructure, and credible information governance can mitigate escalation without kinetic force. In the convergence age, stability

[47] People's Liberation Army Academy of Military Science. *System Destruction Warfare*. Translated excerpts, 2020

increasingly depends on securing both networks and narratives.

State-led cyberattacks

Cyberspace has become the de facto opening theatre of contemporary conflict. The Russia–Ukraine war demonstrates that initial salvos are frequently digital, ranging from malware deployments, wiper attacks, and coordinated intrusions designed to disrupt command-and-control networks before or alongside kinetic operations.[48] What distinguishes cyber as a strategic instrument is its ambiguity. Attribution remains complex, timelines are compressed, and escalation thresholds are blurred. Similar dynamics were visible during the 2025 India–Pakistan crisis following the Pahalgam attack. In the days surrounding heightened military signalling, cybersecurity advisories in both countries reported increased probing activity, distributed denial-of-service attempts, and information operations targeting public-facing platforms. While public attribution is contested, the episode underscores how cyber activity can operate as both signalling and pressure in a nuclearised environment below the threshold of overt force, yet be capable of shaping perception and preparedness. This deniability complicates deterrence by obscuring responsibility, weakening retaliation credibility, and increasing escalation uncertainty, rendering cyber operations both a low-cost entry point and a high-impact multiplier of state power.

Targeting command networks and critical infrastructure

Modern militaries are inseparable from civilian digital infrastructure. Fibre networks, cloud services, and satellite links carry both tactical orders and essential civilian services. Cyber campaigns increasingly exploit this convergence, as illustrated by the 2022 attack on Viasat's KA-SAT network, which disrupted military communications while affecting civilian users across Europe.[49] In the ongoing Russia–Ukraine conflict, electronic warfare operations target GPS signals and data links, severing drone coordination and degrading AI-driven targeting. Spectrum denial does not merely blind sensors but desynchronises convergence. When data flows collapse, AI loses coherence, drones lose coordination, and precision warfare fragments. The Internet of Military Things extends this vulnerability. Dense networks of sensors, autonomous platforms, and command nodes feed real-time data into AI-driven architectures. Concepts such as Joint All-Domain Command and Control (JADC2) aim to synchronise operations across every echelon at unprecedented speed.[50] Connectivity, however, is exposure. Each additional node is both a sensor and a

[48] NATO Cooperative Cyber Defence Centre of Excellence. *Cyber Operations and Escalation Management*. 2023

[49] Carnegie Endowment for International Peace. *Attribution Failure and Escalation Risk in South Asia*. 2024

[50] U.S. Army. *Long-Range Hypersonic Weapon (Dark Eagle) Program Overview*. 2023

vulnerability. Cascading failures can propagate faster than human intervention. In such an environment, deterrence hinges less on invulnerability than on continuity i.e. the ability to absorb, isolate, and recover faster than an adversary can disrupt.

Psychological and information operations

If cyber operations target networks, information operations target legitimacy. Social media platforms, real-time video, and algorithmic amplification have transformed perception into a decisive battlespace. Russia and China invest in coordinated influence architectures employing bots and narrative flooding to shape opinion at scale.[5152] Conversely, Ukraine demonstrates how digital transparency galvanises international support and sustains domestic morale. The 2025 India–Pakistan crisis following the Pahalgam attack similarly reveals how rapidly digital narratives shape public perception during escalation.[5354] Competing hashtags, edited visuals, and emotionally-charged content circulate widely across platforms, often outpacing official clarification. In such environments, information cascades amplify domestic pressure, constrain diplomatic manoeuvring, and compress decision timelines. Credibility, earned through timely communication and transparent attribution, becomes both reputational capital as well a stabilising instrument in crisis management. In an era of synthetic media and automated amplification, credibility itself becomes a form of deterrence.

Zero-days, supply-chains, and trust

The most destabilising cyber threats increasingly exploit trust rather than force. Zero-day vulnerabilities (software flaws unknown to vendors at the time of exploitation) and compromised supply chains, in which attackers infiltrate systems through trusted third-party providers, have become the preferred vectors for state-led intrusion. The SolarWinds compromise revealed how a single software supplier provided persistent access to thousands of government and defence systems worldwide.[5556] Such operations undermine traditional deterrence logic: they are difficult to detect, hard to attribute, and are often discovered only after damage has occurred. Emerging technologies further extend this convergence. Advances in synthetic biology and genome editing lower barriers to manipulation, while machine-learning systems model protein-folding and simulate pathogen behaviour. The same algorithms that defend public health could, in theory, be repurposed to design novel biological threats.

[51] People's Liberation Army Academy of Military Science. *System Destruction Warfare*. Translated excerpts, 2020

[52]

[53] *Observer Research Foundation*, "Weaponising the Narrative: Social Media Propaganda Post-Pahalgam Attack," *ORF*, May 13, 2025

[54] ABC News (Australia), "Misinformation War Rages Online amid India-Pakistan Crisis," May 23, 2025

[55] U.S. Cybersecurity and Infrastructure Security Agency. *SolarWinds Cyber Supply-Chain Compromise*. 2021

[56] OECD. *Global Frameworks for Artificial Intelligence Governance*. 2023

Preparedness in this domain therefore depends less on punishment than on resilience based upon early detection, rapid attribution and international transparency. Consequently, national security now demands technological sovereignty: secure hardware, vetted codebases, zero-trust architectures, and governance mechanisms capable of managing both digital and bio-digital convergence.

Risks, Regulation, and the Road Ahead

The above sections have traced how artificial intelligence, space systems, cyber operations, unmanned platforms, and emerging technologies are converging into a single operational continuum. This convergence multiplies capability as much as it multiplies risk. Distance, detection, decision, and delivery are collapsing into near-simultaneity. Automation, speed, and opacity compress decision time, blur attribution, and strain the stabilising mechanisms on which deterrence has traditionally relied. As speed erases distance and sensing erodes secrecy, the human cognitive loop becomes the bottleneck. The central challenge of the convergence age therefore is governance. Preparedness must reinforce restraint rather than accelerate escalation. Below are four risks and potential pathways to address them:

1. Escalation risks in a machine-paced environment

Technological acceleration erodes the temporal buffers that once separated tactical action from strategic consequence. Hypersonic weapons compress warning windows from tens of minutes to mere minutes.[57] Cyber operations enable pre-emptive disruption of command networks before leaders can even recognise a crisis. Autonomous and semi-autonomous systems introduce the possibility of machine-speed interaction without deliberate human intent. In a converged battlespace, these risks don't accumulate independently but compound. A cyber intrusion can blind space-based sensors, disrupt AI-driven targeting loops, and trigger automated defensive responses across domains. Escalation thus becomes nonlinear: small incidents propagate rapidly across systems, generating strategic effects disproportionate to their origin. Conflict increasingly becomes a contest not of mass or manoeuvre, but of decision advantage under compressed timelines. Deterrence in this environment depends less on punishment than on predictability by restoring time for judgment through transparency, crisis communication channels, shared early-warning mechanisms, and confidence-building measures adapted to machine-paced conflict.

2. Ethical and legal challenges

Automation challenges accountability embedded in international humanitarian law. Converged

[57] U.S. Army, "Long-Range Hypersonic Weapon (Dark Eagle)," program overview

warfare is driven less by discrete weapons than by processes such as data ingestion, algorithmic inference, and human–machine interaction. Governing the convergence age therefore requires shifting from regulating tools to regulating workflows, ensuring data integrity, auditability, and enforceable human control. Ethical restraint is not a moral abstraction but a strategic asset that sustains legitimacy and deterrence.

3. Civil–military fusion and private-sector dependency

One of the most destabilising features of convergence is the redistribution of strategic influence beyond the state. Modern military operations depend on private infrastructure ranging from commercial satellites, cloud platforms, analytics software, and global supply chains. In several conflicts, corporate decisions shape outcomes as decisively as battlefield manoeuvre. This diffusion of power blurs sovereignty and accountability. Resilience therefore requires structured public–private compacts and institutionalised liaison mechanisms between governments and technology firms.

4. Converged governance frameworks

If warfare has converged, governance cannot remain siloed. Separate regimes for space law, cyber norms, AI ethics, and arms control are increasingly mismatched to the reality of integrated operations. Fragmented regulation is itself a vulnerability. A converged battlespace demands converged governance that comprises adaptive, modular, and iterative frameworks capable of matching technological speed with institutional control. These can include:

- **AI arms control dialogue:** Bilateral and multilateral mechanisms to define testing standards, safety benchmarks, and human-control thresholds for autonomous systems, particularly those linked to strategic weapons.
- **Space and quantum stability norms:** Transparency measures, debris-mitigation commitments, and shared situational awareness to reduce miscalculation in orbit and prevent quantum advantage from destabilising deterrence.
- **Cyber accord 2.0:** The extension of humanitarian principles to digital infrastructure, reinforcing prohibitions on attacks against hospitals, power grids, financial systems, and emergency services.
- **Bio governance charter:** Mandatory transparency and verification for genome-editing research with military relevance, paired with rapid-response public health cooperation and AI-assisted monitoring.

Conclusion: Governance as Deterrence in the Convergence Age

This Issue Brief has argued that contemporary conflict is defined not by traditional asymmetry but by the collapse of boundaries between domains. AI accelerates decision-making and operational integration; space systems sustain the data, timing, and connectivity that enable that integration; and cyber and cognitive operations extend competition into networks, perception, and legitimacy. Across these verticals, convergence accelerates the interaction between sensing, analysis, and response, reshaping how the battlefield is perceived and how deterrence is conceptualised.

Across Ukraine, Gaza, Nagorno-Karabakh, the Red Sea, and South Asia, a consistent pattern emerges: adaptability outperforms mass; integrated systems trump numerical superiority; civil–military fusion enhances resilience; and information dominance shapes legitimacy and coalition support. These cases confirm that convergence is not a future condition but the present reality of conflict.

The cumulative effect is structural rather than incremental. Advantage increasingly derives from integration, speed, and adaptability rather than mass alone.[58] Civil–military boundaries blur, attribution becomes contested, and escalation timelines narrow. In such an environment, miscalculation can propagate at machine pace. The war of milliseconds is not defined only by faster machines but also the ability to preserve judgment within acceleration. The strategic challenge therefore is more than what is understood primarily as technological competition; it extends to the preservation of control within accelerating systems.

Deterrence in the convergence age can't rely solely on retaliation. It depends on credible governance as also demonstrable assurance that automation, integration, and connectivity remain subject to institutional oversight and human judgment. Stability rests on resilience, transparency, and mechanisms that prevent speed from overwhelming restraint. In a battlespace measured in milliseconds, governance is not peripheral to power but its most enduring safeguard.

Lt Col S Anirudha Rao is an officer in the Indian Army serving with the Army Cyber Group, where he leads cyber defence and incident response functions within CERT-Army.

Aran Hooda created *Nuro*, a series of discussions with CEOs and global leaders on innovation, leadership, and governance.

[58] Lawrence Freedman, *The Future of War: A History* (New York: PublicAffairs, 2017)