BIPSS Commentary
www.bipss.org.bd June-2026
BIPSS Towards a Secure World

Smart Tech or Hot War: The Future Space of Conflict

Farhana Rashid[1]

Source: iStockphoto

Introduction

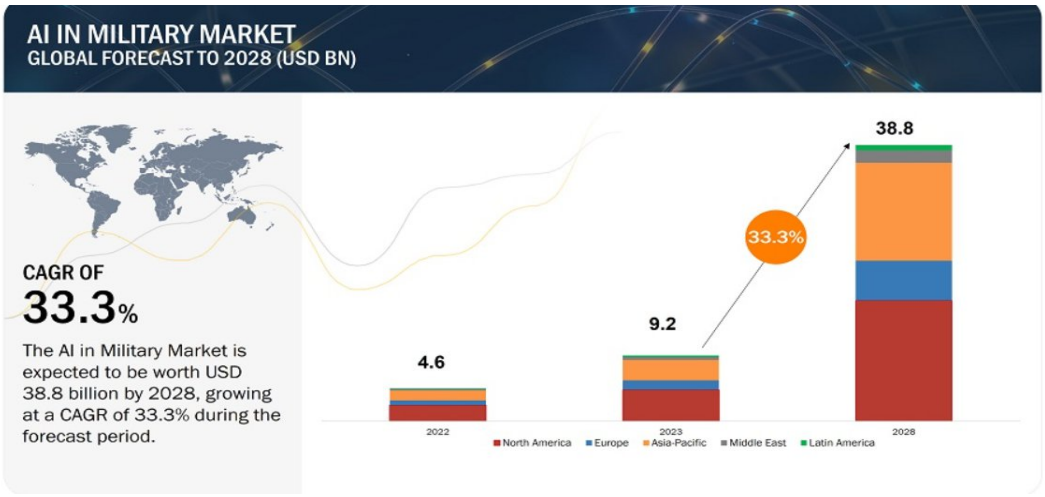
The character of warfare has always evolved alongside technological progress. From the invention of gunpowder to the development of nuclear weapons, every technological breakthrough has fundamentally altered how states project power and pursue security. Today, the pace of transformation is unprecedented. Artificial intelligence (AI), autonomous weapons, quantum computing, cyber capabilities, biotechnology, and space technologies are converging to create an entirely new battlespace where algorithms, data, and digital infrastructure have become as strategically significant as tanks, aircraft, and missiles. These emerging technologies are replacing conventional military power. They're blurring the boundaries between peace and war, civilian and

[1] Farhana Rashid is a Research Assistant at the Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS & MSS in International Relations from the University of Chittagong. She has a keen interest in Geopolitics & Non-Traditional Security discourses.

military domains, and physical and virtual battlefields. Consequently, the future of conflict is increasingly defined not only by military strength but also by technological superiority and control over information ecosystems. From the Iran-Israel-US confrontation in early 2026 to the India-Pakistan crisis of May 2025, recent events suggest that the future space of conflict will be hybrid by default, which contested simultaneously in the air, on the ground, in cyberspace and inside the software.

The Evolution of Warfare: From Industrial Wars to Algorithmic War

For much of modern history, military power was measured by mass: soldiers, tanks, aircraft, ships, and the industrial capacity to sustain them. The First and Second Industrial Revolutions transformed warfare through mechanization, railways, machine guns, and aircraft, while the Cold War introduced nuclear deterrence. That logic is changing as warfare becomes increasingly data-driven, networked, and software-intensive. AI systems can process huge volumes of sensor data, support target recognition, and accelerate command decisions, which gives militaries a speed advantage but also creates new vulnerabilities if the data, model, or network is compromised. Military scholars increasingly describe this transition as the shift from "information warfare" to "intelligence warfare." Nations capable of integrating AI, cloud computing, and real-time battlefield intelligence are likely to enjoy decisive operational advantages.



Source: MarketsandMarkets

The ongoing Russia–Ukraine war vividly demonstrates this transformation. Commercial satellites, artificial intelligence-assisted intelligence analysis, open-source intelligence (OSINT), drones, cyber operations, and social media have become integral components of military strategy. Small, inexpensive unmanned aerial systems have successfully destroyed armored vehicles worth millions of dollars, while satellite internet services have maintained communications despite extensive attacks on conventional infrastructure.[2] These developments indicate that future wars will increasingly reward technological adaptability over sheer military size.

This is why Smart tech is not any separate domain, rather it is becoming the main infrastructure of conflict. The expansion of AI in conflict has shown that national militaries have an immense appetite for the technology, despite how unpredictable and ethically fraught it can be.[3]

The Algorithmic Battlefield: AI as the New Force Multiplier

Artificial intelligence has moved from being a background analytical tool to an operational feature of the battlefield itself. The United States has pursued an explicitly AI-first military posture, with the Pentagon reportedly requesting billions of dollars for autonomy and unmanned systems in its 2026 budget and signing agreements with major technology firms to integrate AI models into classified networks used for intelligence analysis, targeting, and logistics.[4] Their goal is clear; to transform the United States into an "AI first" military force which is capable of maintaining decision superiority in battlefield. On May 1, 2026, the US War Department announced agreements with eight of the world's leading frontier artificial intelligence companies to deploy

---

[2] Zabrodskyi, Mykhaylo , Jack Watling , Oleksandr Danylyuk , and Nick Reynolds. 2022. "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022." Www.Rusi.Orghttps. November 30, 2022. https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022.

[3] Robins-Early, Nick. 2024. "AI's 'Oppenheimer Moment': Autonomous Weapons Enter the Battlefield." *The Guardian*, July 14, 2024, sec. Technology. https://www.theguardian.com/technology/article/2024/jul/14/ais-oppenheimer-moment-autonomous-weapons-enter-the-battlefield.

[4] Paganini, Pierluigi. 2026. "AI, Cyberwarfare, and Autonomous Weapons: Inside America's New Military Strategy." Security Affairs. May 8, 2026. https://securityaffairs.com/191842/cyber-warfare-2/ai-cyberwarfare-and-autonomous-weapons-inside-americas-new-military-strategy.html.

capabilities on Pentagon's classified networks.[5] AI is moving directly into their military chain of command, intelligence analysis, logistics, targeting, and operational planning.

Meanwhile, China has openly pursued "intelligentized warfare," integrating AI into command structures, unmanned systems, and military planning. a January 2026 broadcast reportedly showed a single operator commanding a formation of some two hundred autonomous drones, underscoring Beijing's ambitions in mass-produced, AI-coordinated swarming systems.[6] Ukraine's experience adds a third data point. Kyiv's defence ministry has acknowledged that while fully autonomous lethal systems do not yet exist in its arsenal, elements of autonomy have already been partially implemented in some drone and ground-robot systems, born of necessity on a resource-constrained battlefield. What's common in these cases is a shift in the function that technology performs in war: no longer merely supporting human decision-makers, AI is increasingly compressing the time between detection and lethal action.

Synchronized AI Drone Swarm flight demonstrates coordinated battlefield movement. Source: AICERTs News

---

[5] "Classified Networks AI Agreements." 2026. U.S. Department of War. 2026. https://www.war.gov/News/Releases/Release/Article/4475177/classified-networks-ai-agreements/.

[6] "China's AI Drone Swarm Test Redefines Battlefield Autonomy - AI CERTs News." 2026. AI CERTs News. January 24, 2026. https://www.aicerts.ai/news/chinas-ai-drone-swarm-test-redefines-battlefield-autonomy/.

Cyber Warfare and Digital Battlefields

Digital revolution has transformed cyberspace into one of the most contested areas of modern conflict. Cyber warfare transcends geographical boundaries and enables states and non-state actors to disrupt critical infrastructure, steal sensitive information, manipulate public opinion, and undermine national security without deploying conventional military forces. Financial institutions, power grids, communication networks, healthcare systems, and transportation infrastructure have all become potential targets. Consequently, many strategists say that cyberspace has evolved into the "fifth domain" of warfare alongside land, sea, air, and space. The low cost of launching cyber operations, combined with the difficulty of attributing attacks to specific actors, has made cyberspace an attractive battlefield for both major powers and smaller states seeking asymmetric advantages.

Cyber operations accompany conventional military campaigns rather than replacing them. Russia's invasion of Ukraine demonstrated how cyberattacks against government ministries, satellite communication networks, financial institutions, and energy infrastructure were coordinated with missile strikes and ground operations. Before the invasion, malware such as WhisperGate and HermeticWiper targeted Ukrainian government systems, while attacks on satellite communications temporarily disrupted military and civilian connectivity.[7] Although many of these operations achieved only limited military success, they illustrated that future conflicts will likely combine cyberattacks, electronic warfare, disinformation campaigns, and kinetic operations into a single integrated strategy. This convergence complicates military planning because commanders must defend both physical territory and digital infrastructure simultaneously. A single cyber operation may serve multiple objectives, such as gathering intelligence while also laying the groundwork for future disruptive attacks or conducting espionage while simultaneously stealing intellectual property.[8]

The interconnected nature of digital systems means that the impacts of cyber warfare often extend far beyond the intended targets. The NotPetya attack, while initially targeting Ukraine, caused

[7] Fierro, Christopher Del, and John Dwyer. 2022. "New Destructive Malware Cyber Attacks Ukraine." Ibm.Com. February 24, 2022. https://www.ibm.com/think/x-force/new-destructive-malware-cyber-attacks-ukraine.

[8] Rahimi, Nick, and Henry Jones. 2025. "Cyber Warfare: Strategies, Impacts, and Future Directions in the Digital Battlefield." *Journal of Information Security* 16 (02): 252–69. https://doi.org/10.4236/jis.2025.162013.

widespread collateral $10 billion damage to companies and institutions worldwide, demonstrating the unpredictable nature of cyber weapons and the challenges in containing their effects.[9] The Israeli-US strikes on Iran launched on 28 February 2026, Operation Epic Fury and Operation Roaring Lion, combined air and missile strikes with a parallel cyber campaign that reportedly collapsed Iranian internet connectivity to as little as 1 to 4% of normal levels, which disrupted official media and security communications.[10] The same campaign produced spillover effects far from the immediate battlefield, including disruptions to fuel distribution in Jordan and interference with navigation systems affecting over a thousand vessels near the Strait of Hormuz.[11]

The growing role of private technology companies such as Microsoft, Google, Amazon Web Services, Starlink, CrowdStrike, and Cloudflare have become indispensable in defending national digital infrastructure. During the Ukraine conflict, commercial satellite imagery, cloud computing services, cybersecurity firms, and satellite internet providers supported military resilience in ways traditionally expected only from state institutions. This reflects a significant shift in international security: technological corporations increasingly possess capabilities comparable to those of many governments, making public-private partnerships an essential component of national defence.

Autonomous Weapons and the Ethics of Machine Combat

Perhaps no technological innovation has generated greater ethical and strategic debate than autonomous weapons systems (AWS). These systems employ artificial intelligence and advanced sensors to identify, track, and engage targets with varying degrees of human intervention. While fully autonomous weapons remain relatively limited, many militaries already employ semi-autonomous systems capable of independently navigating, selecting routes, detecting threats, and executing defensive actions. The increasing deployment of loitering munitions, autonomous naval vessels, robotic ground vehicles, and AI-assisted drones indicates that autonomy is gradually becoming a defining characteristic of modern military operations.

---

[9] Ibid

[10] "Middle East Cyber Warfare Escalates In 2026 Conflict." 2026. Cyble. March 17, 2026. https://cyble.com/blog/middle-east-cyber-warfare-2026-hybrid-conflict/.

[11] "Hybrid Warfare 2026: Cyber & Kinetic Threats Converge." 2026. Cyble. March 30, 2026. https://cyble.com/blog/hybrid-warfare-2026-cyber-kinetic-threats/.

FPV drones attacking a tank. Source: Istockphoto

The wars in Ukraine and the Middle East have highlighted the growing military value of autonomous and semi-autonomous drones. First-person-view (FPV) drones, loitering munitions, AI-assisted target recognition systems, and swarm technologies have dramatically altered battlefield tactics. Compared with traditional missiles, these systems are significantly cheaper while maintaining considerable destructive capability. Small drone swarms can overwhelm sophisticated air defence systems, conduct persistent surveillance, and attack armored formations with remarkable precision. Military planners increasingly anticipate that future wars will involve coordinated swarms of autonomous aerial, maritime, and ground systems operating simultaneously across multiple domains.

Despite their operational advantages, autonomous weapons raise profound ethical and legal concerns. Delegating life-and-death decisions to machines challenges fundamental principles of international humanitarian law, including distinction, proportionality, and accountability. If an autonomous system mistakenly targets civilians, determining legal responsibility becomes difficult. Existing legal frameworks were developed with human decision-makers in mind and therefore struggle to address these emerging problems. Human rights organizations and numerous states have consequently called for legally binding international regulations governing lethal

autonomous weapons before their widespread deployment becomes irreversible. For example, Human Rights Watch has founded a civil society coalition called Stop Killer Robots, that calls for a new international treaty to prohibit and restrict autonomous weapons systems.[12]

Quantum Computing and the Next Military Revolution

Implementation of China's carrier-grade quantum communication networks over 10000 km. Source: Nature.com

Quantum computing, quantum sensing, and quantum communication have the potential to alter intelligence gathering, cybersecurity, navigation, and strategic competition. A sufficiently advanced quantum computer could potentially challenge widely used encryption methods, threatening the security of military communications, financial networks, government databases, and critical infrastructure. They can therefore do things that conventional technologies can't, such as precisely measuring location while entirely offline and, in theory, cracking encryptions that are widely used today.[13] This possibility has already encouraged governments to invest in post-

[12] Human Rights Watch. n.d. "Killer Robots." Human Rights Watch. Accessed July 14, 2026. https://www.hrw.org/topic/arms/killer-robots.

[13] Neuberger, Anne. 2026. "The Coming Quantum National Security Crisis: China and Russia Are Harvesting Encrypted Secrets—and Getting Closer to Cracking Them." Foreign Affairs. Foreign Affairs Magazine. June 17, 2026.

quantum cryptography and quantum-resistant security systems. At the same time, quantum sensing could improve the detection of submarines, aircraft, and other military assets, while quantum navigation may reduce dependence on vulnerable satellite-based positioning systems. Although many military applications remain experimental, the strategic competition surrounding quantum technology has already begun.

So far, when it comes to quantum, the United States maintains a technical edge in hardware, and much of its progress is driven by private companies, including IBM, Google, and various startups. China, by contrast, has identified quantum as one of its top priorities in its five-year plan for 2026–30 and centralizes most of its research and development under state-directed hubs, such as Hefei National Laboratory.[14] The United States has joined leading quantum allies such as France, Japan, and the United Kingdom to form the 13-nation Quantum Development Group, with the aim of securing global supply chains and protecting national security interests from emerging quantum threats. Meanwhile, China, is already collaborating with BRICS countries, most notably Russia, which is home to world-class physical science, math, and cryptography capabilities. Russia is focused on developing military tools for war in Ukraine. Since its full-scale invasion of Ukraine, in 2022, Russia has forged closer ties with China. In late 2023, the two countries demonstrated what they called "a secure quantum link," transmitting information instantly between Chinese satellites and Chinese and Russian ground stations 2,400 miles apart with ostensibly zero risk of eavesdropping. In October 2024, China conducted a similar demonstration with South Africa linking stations that were over 8,000 miles apart. The connection spanned a remarkable 12,900km: the longest intercontinental quantum communication link established to date.[15]

---

https://www.foreignaffairs.com/china/coming-quantum-national-security-crisis.

[14] Ibid

[15] Ismail, Yaseera. 2025. "South Africa and China Set up a Quantum Communication Link: How We Did It and Why It's Historic." Edited by Wale Fatade, August. https://doi.org/10.64628/aaj.gh37xjg57.

At a cyberdefense exercise in Kalkar, Germany, April 2026 Source: Reuters

The strategic importance of quantum technology lies not only in its potential capabilities but also in the uncertainty surrounding when those capabilities may become operational. States fear that adversaries could collect encrypted information today and decrypt it in the future once sufficiently powerful quantum computers become available. This creates an immediate security challenge even before large-scale quantum computers exist. The United States, China, the European Union, and other technological powers are therefore investing heavily in quantum research, making it another arena of geopolitical competition. As with artificial intelligence, the countries that establish technological leadership, secure critical supply chains, and develop highly skilled scientific workforces may gain significant strategic advantages.

Will Smart Technology Lead to Hot War?

The central paradox of emerging military technology is that the same systems designed to strengthen deterrence may also increase the risk of conflict. AI-enabled surveillance, predictive analytics, and precision weapons can improve situational awareness and potentially prevent

miscalculation. Yet they can also accelerate the pace of military decision-making to a point where political leaders have less time to evaluate uncertain information. During a crisis between major powers, an AI system that incorrectly identifies an attack or recommends an aggressive response could contribute to rapid escalation. The danger becomes particularly severe when AI is integrated into nuclear command, early-warning, or strategic decision-support systems.

The concept of an "algorithmic arms race" further complicates strategic stability. States may fear that delaying the adoption of AI or autonomous systems will leave them vulnerable to technologically superior adversaries. This pressure can encourage rapid deployment before systems are adequately tested or appropriate regulations are established. Similar dynamics have historically characterized arms races, but digital technologies evolve considerably faster than conventional weapons systems. Software can be updated almost instantly, while autonomous capabilities can proliferate through commercial markets. The result may be a security environment in which governments constantly fear technological surprise and therefore become more willing to act pre-emptively.

Another danger is the growing ambiguity between civilian and military technologies. Artificial intelligence, drones, satellites, cloud computing, semiconductors, and communication networks are overwhelmingly dual-use. A commercial satellite may support civilian internet access while simultaneously enabling military communications. A civilian drone can be modified for reconnaissance or combat. Cloud infrastructure operated by private corporations can host government and defence-related data. In a future conflict, adversaries may therefore consider civilian technological infrastructure to be strategically relevant, potentially expanding the range of targets and increasing risks to civilian populations. The boundary between the battlefield and everyday life is consequently becoming increasingly difficult to define.

technological innovation does not make major war inevitable. Emerging technologies can strengthen deterrence, improve transparency, enhance early warning, and enable more precise military operations. AI-powered monitoring systems could help verify arms control agreements, while satellite imagery can expose military mobilization and reduce strategic uncertainty. Autonomous systems can perform dangerous tasks such as mine clearance and reconnaissance without placing soldiers at immediate risk. The future impact of technology will therefore depend largely on political choices, international norms, and the institutions created to govern its use.

Technology changes the instruments of warfare, but political leaders still determine whether those instruments are used for deterrence, coercion, or conflict.

Implications for South Asia and Bangladesh

The transformation of warfare has particularly significant implications for South Asia. This region is characterized by nuclear rivalries, unresolved territorial disputes, political instability, and rapidly expanding digital economies. India, Pakistan, and China are investing in artificial intelligence, drones, cyber capabilities, missile technologies, and space systems. The strategic competition between India and China, combined with the enduring India-Pakistan rivalry, means that technological innovation could influence regional deterrence and crisis stability. AI-assisted surveillance and precision-strike capabilities may improve military effectiveness, but they could also compress decision-making time during crises and increase the danger of miscalculation between nuclear-armed states. For Bangladesh, the future of conflict presents a different but equally important set of challenges. Bangladesh is unlikely to compete technologically with major military powers, but its growing digital economy, strategic location in the Bay of Bengal, critical infrastructure, financial networks, and increasing dependence on digital services create new vulnerabilities. Cyberattacks against banking systems, energy infrastructure, telecommunications networks, ports, or government databases could generate significant national security consequences without involving conventional military confrontation. The growing availability of inexpensive drones and commercially accessible AI tools also lowers the technological barrier for non-state actors and criminal networks. Bangladesh should therefore approach emerging military technologies primarily through the lens of resilience, capacity building, and responsible adoption. Strengthening cybersecurity institutions, protecting critical infrastructure, developing skilled human resources, improving civil-military technological cooperation, and establishing clear policies for artificial intelligence should become national priorities. The country can also play a constructive diplomatic role by supporting international discussions on responsible AI, autonomous weapons, cyber norms, and the peaceful use of outer space. For middle and smaller powers, technological security does not necessarily require participation in an expensive arms race; instead, strategic resilience and effective governance may provide the most sustainable form of protection.

Conclusion

The future space of conflict is neither purely digital nor purely kinetic. It is a layered environment in which algorithms, autonomous systems, cyber operations, satellites, drones, and human judgment interact under conditions of stress and uncertainty. Smart tech may deliver tactical advantage, but without restraint it can also make hot war easier to start, harder to contain, and more difficult to end. The evidence from Iran, Ukraine, and South Asia over the past eighteen months points toward a future space of conflict in which algorithmic targeting, autonomous drones, and cyber-physical sabotage do not replace conventional force but accelerate, extend, and sometimes provoke it. Ultimately, technology itself will not determine whether the future is characterized by smarter deterrence or more destructive warfare. That outcome will depend on how states choose to develop, regulate, and deploy emerging capabilities. International cooperation on responsible AI, meaningful human control over lethal force, cybersecurity norms, space security, and technological arms control will become increasingly important. In an era where machines can act at unprecedented speed, preserving human judgment may become the most important security technology of all.