Impact of Technology on Conflicts

Major General (Dr) Pawan Anand, AVSM (Retd)[@]

Abstract

The content of this article was presented at the United Service Institution of India United Nations (UN) Forum in 2024. It highlights current characteristics and the fast pace of change in modern war-fighting, accelerated by rapid technological developments. Emerging technologies such as Artificial Intelligence and quantum and the military application of commercial ones have led to multi-domain forms of conflict, blurring the differentiation between national and societal lines and leading to a constant state of contestation. UN peacekeeping operations will need to recognise these rapid changes in conflict-ridden areas and adapt to these new paradigms if they are to remain relevant.

Introduction

The first 20 years of this century have seen wars in 54 countries (of 193), and most of these are continuing even today. Around 60 states and 100 armed groups were actively in conflict in 2020, according to the International Committee of the Red Cross, with many other states supporting these wars diplomatically, financially, or by supplying arms. As of Nov 2024, data stands at over 120 armed conflicts around the world, involving over 60 states and 120 non-state armed groups.[1] Some of the unique issues characterising current-day conflicts are:

- **Stakeholder Coalitions.** Most of the conflicts since 2010 have taken the form of groups comprising a coalition of state and non-state actors. This diffused the pressure on states from the perspective of International Humanitarian Law (IHL) and rules of war.

[@]**Major General (Dr) Pawan Anand, AVSM (Retd)** is a distinguished sapper officer who was awarded the President's Gold Medal at the National Defence Academy and the Sword of Honour at the Indian Military Academy. Having seen action during the Kargil War and Counter Insurgency Operations, and commanded his unit in an armoured division, he currently heads the Centre for Emerging Technology for *AtmaNirbharta* at the United Service Institution of India, and is a mentor at the National Defence College. He is an acknowledged speaker and regular attendee at Track 1.5 dialogues.

Journal of the United Service Institution of India, Vol. CLV, No. 639, January-March 2025.

- **Duration.** Just as the belief that long-duration wars would be a thing of the past drew currency, wars have now begun to lengthen, and as they get prolonged, they tend to mutate. The Ukraine war has been ongoing for three years, and the tactics, techniques, and procedures, and strategies have undergone numerous changes as the introduction of newer technologies finds application again and again. Such wars have a tendency to degenerate into a form of national insurgency, factional civil war, Islamist terror, or forced occupation (as is expected in the Middle East).[2]

- **Restricted Spaces.** Unlike the World Wars, armies (including navies and air forces) have not fought at larger scales as they did in the 20th Century. Most wars between 2000 and 2020 involved an asymmetric struggle between relatively small government forces and armed groups supported by bigger nations who, at times, have used them as proxies. Some exceptions do exist, but none seem to even equal the scale of the Gulf Wars under the leadership of the United States (US) including the Global War on Terror with a 'Coalition of the Willing'. The areas of operations in most of these wars have been restricted to specific areas in any one or two countries, regardless of urban or rural, except the wars in Iraq, Syria, Yemen, Afghanistan, Sudan, and now Gaza, and Ukraine.

- **Diffused Outcomes and Prolonged Political Contestation.** The democratisation of technology has enabled smaller forces to achieve disproportionate results, making it difficult to crush ideologies or achieve complete victories, resulting in festering wounds on all sides. This makes way for prolonged law and order situations or gang violence internally, as seen in some South American nations and currently in Haiti.[3]

- **Computer-based Warfare.** Computerisation and Artificial Intelligence (AI) put warfare on a new trajectory—into the new domains of outer space and cyberspace involving highly complex 'Systems of Systems' that are automated with extraordinary precision and speed well beyond the understanding of their human operator. AI-based Intelligence, Surveillance, and Reconnaissance (ISR) systems can gather

extraordinary amounts of detailed information and provide decision support functions, almost in real-time. Drones are being used in attack, defence, surveillance, and supply. They can operate alone or in swarms, and operate in tandem with combatants in 'Hybrid Operations'. AI-based weapons are achieving high levels of functional autonomy, putting to test ethically-based decisions.

- **Sub-threshold Conflicts Involving Entire Populations.** The covert use of special forces, espionage, assassinations, cybercrimes, disinformation campaigns, and election tampering are often deniable and exist in a 'Grey Zone'. Mobile phones and social media platforms have reduced human misery to a spectacle, with the ancient art of propaganda, misinformation, disinformation, and hate speech taken to the next level. Weaponisation of all forms of public interaction is the dominant narrative. Allegations of Russian subversion of western elections and Chinese pressure to retake control of Hong Kong can be below-threshold conflict examples.[4]

- **Lawfare.** This has come starkly to light during the Gaza war, where states themselves or specific heads of state have been dragged to international or domestic courts debatably beyond their jurisdiction.

Impact of Technology on Warfare through Different Generations

Warfare has evolved based either on concepts and doctrines or on the evolution of technology that shapes war fighting. Today, the phenomenal speed in the evolution of technology is shaping future warfare, wherein, AI, big data analytics, cyber, militarisation of space, nanotechnology, directed energy weapons, and hyper-velocity technology portend non-contact kinetic and non-kinetic dimensions of asymmetric warfare. Table 1 below reflects the increasing speed with which warfare has morphed.[5]

Warfare	Characteristics	Weapon Systems
1st Gen	• Massed manpower, • Line and column, face to face.	• Based on 'attrition' • Use of swords, arrows, lances, cannon (Napoleonic Wars,3rd Battle of Panipat)
2nd Gen	• Massive fire power, deployment of troops • Emergence of Operational Art	• Rifled barrel, guns and indirect fire (1st WW, First Anglo-Sikh War)
3rd Gen	• Maneuver Warfare • Development of Advanced Missile technology	• Armored units replace Horse Cavalry • Military aircraft and airborne forces (2nd WW, Indo-Pak 1965)
4th Gen (4 GW)	• Product of Globalization • Insurgency, Terrorism, Guerilla warfare	• Resembles traditional low-intensity conflict (Gulf Wars, LTTE, Kashmir, Chechnya/Baluchistan)
5th Gen	• Non—contact warfare • Spread due to digitization	• Use of Networks & combat clouds (cloud computing), • Multi-domain battle (non-mil, trans-mil and mil domains) • Fusion warfare (Russia-Ukraine Conflict, Nagorno -Karabakh War, Azerbaijan)
6th Gen	• Extreme Electronic Deception • Manipulating space-time loop to own advantage.	• A mix of manned and unmanned automated platforms and systems (Chinese disinformation campaigns during Covid, Hamas/Hezbollah-Israel)
7th Gen	• Totally automated warfare • AI completely removes human interface in decision making, command and execution.	• Advancements in Nano-technology, robotics, surveillance and digital networks

Table 1

Militarisation of Commercial Technologies

Military research and development famously led the race for innovation, but recent decades have seen an interesting reversal in this order, with civilian or commercially developed technologies being rapidly adapted and integrated for military purposes. This has the advantage of such technologies being driven by necessity and a profit motive before they find military application. Recent examples are the employment of StarLink in the Ukraine war and how the Israelis seem to have won the war against Hamas but lost the television war (of narrative) to Gaza and its images of destruction, which replaced the horrors of 07 Oct 2023. Yet it raises ethical and legal questions, as well as concerns about the potential misuse of technology.[6]

Emerging Cyber Threats

Cyber threats are no more merely ransomware; they are now increasingly sophisticated, targeting critical information infrastructure, governments, and individuals across the spectrum. Cyberattacks and malware present threats via advanced persistent threats[7], phishing, data breaches, and Distributed Denial of Service (DDoS), with the potential for significant damage.[8]

As more devices become connected to the internet, the Internet of Things (IoT) presents new attack vectors for cybercriminals. Insecure IoT devices can be compromised to launch large-scale attacks, such as DDoS attacks. At the same time, the 'Internet of Battle Things' or 'Internet of Military Things' are increasingly vulnerable as attack surfaces for cyber interventions increase, especially at the interfaces of media, such as communications via 5G or 6G networks, software-defined architectures, etc. Increasingly, governments are feeling the need for indigenously developed systems.

The use of AI in cybersecurity has both positive and negative implications. While AI can enhance security measures, cybercriminals can also leverage it to automate attacks, evade detection, and launch more sophisticated phishing campaigns.

It must be noted that unlike the physical battlespace, cyberspace presents the defenders dilemma—the attacker has the advantage of initiative and surprise while the defender has endless surfaces to defend and can easily be blind-sided.

Artificial Intelligence

The use of AI is beginning to revolutionise operations. It helps analyse enormous amounts of data in real-time, detect patterns, and identify potential threats. AI systems are being employed to help detect and identify wireless communication links of interest and to deploy the appropriate technology to jam these signals or to help intercept and monitor them as needed. Sensor-shooter linked systems require high-speed data processing, but their advent has tightened up the Orient Observe Decide Act loop to unimaginable levels. Augmented/virtual reality systems provide realistic immersive training. Predictive AI analytics becomes useful in maintenance operations. Routine and repetitive tasks can now be performed by AI-driven systems, making cognitive skills gain salience.

Yet, AI poses challenges such as the need for big data storage, secure connectivity, and high-powered computing for real-time processing, analysing, and protecting it from interdiction and corruption. While India sits on and continues to generate humongous amounts of data all the time, it also poses challenges like data sovereignty, its collation, and finally, its utilisation.

While machine learning algorithms learn from new data, improve accuracy and adaptability, AI systems, which have not fully matured, tend to be vulnerable to data poisoning and hallucinated outputs. There is a dire need for edge computing and advanced graphics processing units.

Un-crewed Weapon Systems

Unmanned vehicles or 'Drones'—can be deployed in the air, on the ground, or in maritime configurations. The United Nations (UN) Secretary-General, in his policy brief on a 'New Agenda for Peace', has emphasised the proliferation of un-crewed systems in armed conflicts. When used to attack civilian targets or critical infrastructure, they border on international law infringements and have presented a threat to peace operations.[9] On one hand, these present a reduced risk to personnel but, on the other, can lead to uncontrolled escalatory actions. The employment of drones in wars is well underway, but the threat of their use by terrorists and non-state actors has become infinitely high, making things difficult for law enforcement agencies.

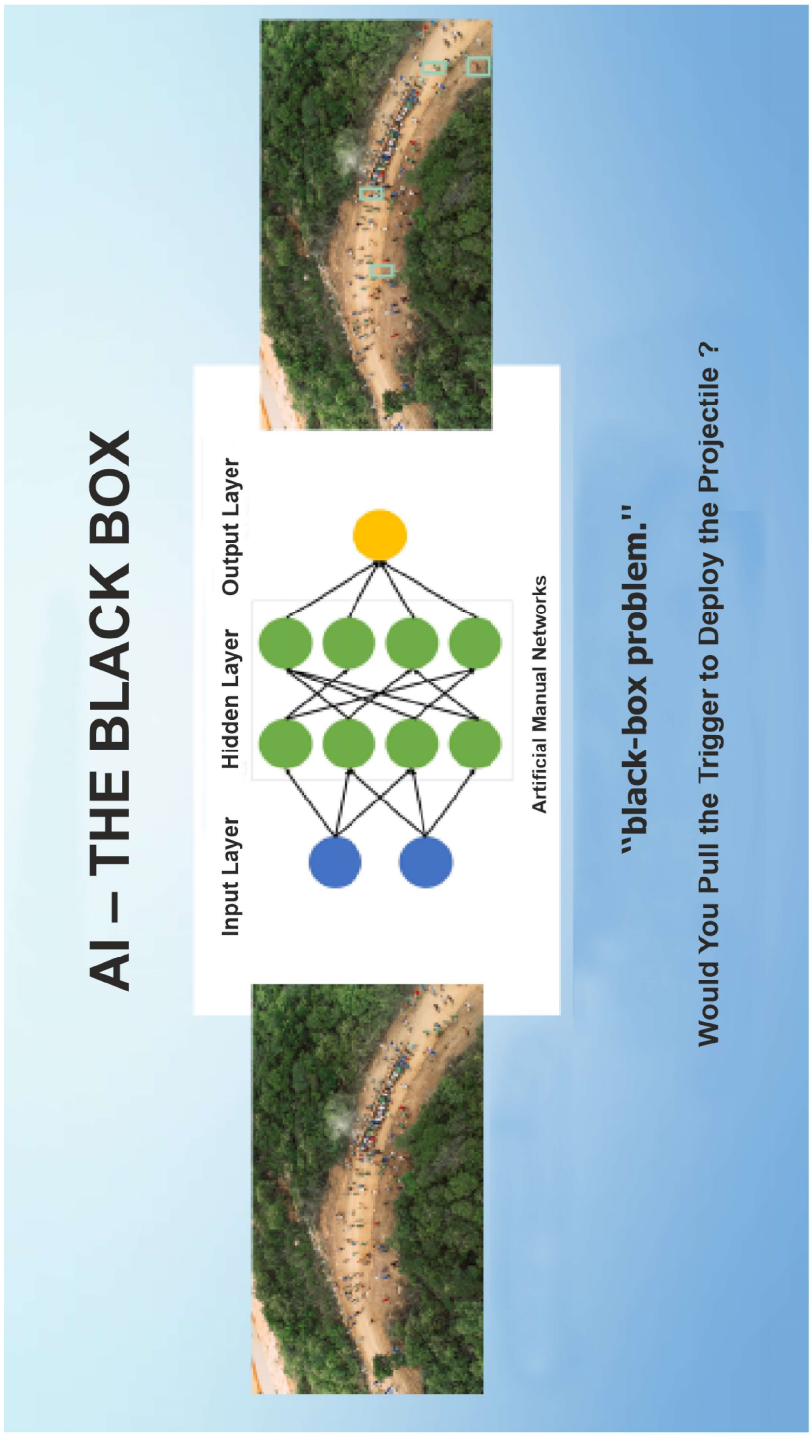
AI – THE BLACK BOX
Input Layer
Hidden Layer
Output Layer
Artificial Manual Networks
"black-box problem."
Would You Pull the Trigger to Deploy the Projectile ?

Figure 1

The defence industry has been revolutionised by lethal autonomous weapon systems, which make use of advanced robotics and AI. The speed of development has been unimaginable—the US developed an AI-based change detection system for ISR within eight months under Project Maven, which proved to be a hugely successful military-private sector enterprise.

Neural networks produce outputs based on their self-learned algorithms, and in many cases, the basis for the generation of this output cannot be understood. This is called the 'Black Box' problem of neural networks, which are based on machine learning. The fielding of such weapon systems, thus, raises the questions of IHL and responsible AI in the military domain.

These AI-based weapons will need to meet the principles of explainability, interpretability, and accountability. It is essential to build a global consensus to adhere to these principles. While nations jostle for policy and regulatory supremacy in this uncharted territory, India hopes to represent the have-nots by being the voice of the Global South in such matters. It will not fall prey to earlier discriminatory policy regimes such as the Nuclear Non-Proliferation Treaty.

Blockchain

Blockchain technology, initially developed for cryptocurrencies like Bitcoin, has revolutionised security. Its decentralised and immutable nature provides transparency, integrity, and resistance to tampering. Blockchain can be employed to secure transactions, verify the authenticity of digital assets, and ensure the integrity of supply chains. In the context of security, blockchains enhance data integrity, prevent unauthorised access, and enable secure identity management. It can be used to create secure, tamper-proof logs of cybersecurity events, facilitating incident response and forensic analysis. Another noteworthy feature of blockchain is its consensus algorithm, which keeps an eye out for any malicious activity and false positives without requiring a central authority.[10]

Quantum Technology

With quantum technology on the horizon, traditional cryptographic methods will soon be immensely vulnerable. Quantum cryptography and encryption techniques are being developed by the US and China, followed by some other advanced nations.

While the technology is not yet matured, considering its extreme requirements like high purity levels or low temperatures to make rare earths super-conductive (e.g., beryllium and aluminum oxide become superconductive at zero-degree Kelvin); once deployed, it will break blockchain algorithms in a short span of time. The need for segregated discrete data storage and high-speed retrieval methods would then be invaluable.

Quantum key distribution allows for the secure exchange of cryptographic keys, confidentiality, and data transmission with integrity. Post-quantum encryption algorithms are being designed to withstand attacks from quantum computers, ensuring long-term security.

While India has managed up to 6-14 qubits, China and the US have already achieved 1,200 qubit capability, and the former has made claims to soon achieve 6,000 qubits.

Space Race

Increased activity by many nations is driving strategic competition in outer space, posing new risks, with possibilities of collisions and the threat of hazardous debris. Satellites support tactical operations and strategic defence with enhanced capabilities for communication, navigation, and reconnaissance. They also provide a range of capabilities to existing systems, including precision targeting. Space communications, when intercepted, will enable hostile takeovers of command-and-control systems of even satellites or weapon systems—to take them off course, crash, collide, disable, change loyalties, etc., making space stations vulnerable to killer satellites. Vulnerable satellites and spacecraft computers are potential targets for cyberattacks by states, their proxies, or terrorist groups. Offensive cyber capabilities are now an integral part of anti-satellite toolboxes.[11]

Race for Resources

Just as oil is a source of conflict, critical and rare minerals, and rare earth elements pose an even greater threat to security as nations battle for resources powering advanced weapons system capabilities. In addition to this, competition over natural resources is a major driver of conflict. Often, control over valuable resources like minerals, forests, diamonds, oil, water, and the like directly cause or compound violence. Access and sale of such lucrative

resources helps finance or prolong conflicts which arise out of entirely different causes.[12] Converging national interest for capability development is forging new international groupings, even alliances.

Nuclear Revisionism

There is a perception that the unravelling of the international arms control architecture and a gradual backtracking on established arms control agreements may not support global stability, restraint, and transparency. The continued existence of nuclear weapons poses a greater threat than ever before. Indeed, when the Intermediate-Range Nuclear Forces Treaty ended in Aug 2019, the UN Secretary-General deplored the loss of 'An invaluable brake on nuclear war'. A similar situation arises for the New Strategic Arms Reduction Treaty, which may never effectively see the light of day. The Ukraine war, followed by the Middle East conflict, has already prompted Russia to revisit its nuclear doctrine, which it declared publicly. Others are following suit as the Iranian capability nears fruition.[13]

Dilemmas in United Nations Peacekeeping in High-Tech Wars

The preceding issues make it evident that the deployment of the latest tech in warfare and conflicts has raised unique dilemmas in peacekeeping. Modern armed conflicts have witnessed small-scale, lightly-armed, high-tech-enabled, mounted groups capable of inflicting great damage in short periods of time. Their form of hostility is hard to identify as they do not model or shape themselves as traditional adversaries do. There is also an evolving threat of violent extremism, transnational terrorism, and transnational organised crime, which bring about unimaginable collateral damage.[14]

Increased employment of private security organisations makes them difficult to be differentiated from terrorist groups and criminal gangs, yet assists in building the capacity of government forces. This environment is difficult for peacekeepers to operate in, until peace and stability are restored. For example, activities of Boko Haram in northern Nigeria, international terrorism in Mauritania, Mali, Chad, Burkina Faso, and the Sahel region, as well as transnational organised crime, have negatively affected peace efforts. The death toll of at least 462 UN and associated personnel who were killed in deliberate attacks in the past 11 years is evidence of this.[15]

TECHNOLOGY APPLICATIONS OVER A DECADE

Technology	Expected Advances	Potential Military Applications
Artificial Intelligence (AI)	-Advanced machine learning algorithms and neural networks. -Autonomous military systems. -Enhanced decision support systems.	-AI-driven unmanned vehicles and drones. -Improved command and control.
Quantum Computing	-Faster encryption and decryption. -Improved quantum communication. -Advanced simulations.	-Secure military communications. -Advanced military planning and research.
Hypersonic Weapons	-Faster and more maneuverable missiles. -Precision strike capabilities. -Potential for defense systems.	-Rapid and precise strike capabilities. -Enhanced strategic deterrence.
Cybersecurity	-Addressing more sophisticated cyber threats. -AI-powered threat detection. -Enhanced network protection	-Safeguarding military networks and data. -Real-time threat response.
Unmanned Aerial Vehicles (UAVs)	-More autonomous UAVs. -Improved endurance and stealth. -AI integration for autonomous missions.	-Surveillance and reconnaissance. -Swarming drone operations.
Advanced Materials	-Lightweight and durable armor materials. -Advanced energy storage. -Extreme environment materials.	-Enhanced soldier protection. -Extended mission capabilities.
Biotechnology	-Advanced medical solutions. -Bio-inspired sensors. -Soldier enhancements.	-Medical support in the field. -Improved situational awareness.
Space-Based Technologies	-Reliable satellite communication and navigation. -Advanced space situational awareness. -Potential space-based weaponary.	-Secure communication and navigation. -Monitoring potential space threats.

Table 2

Conclusion

Peacekeeping operations will need to be upgraded to the highest existing levels of existing capability to be able to meet these new challenges. This transformation will happen only when peacekeepers rapidly adapt to emerging techno-threats and challenges with agile mind-sets and organisational flexibility. Supply chains and lines of communications will need to be constantly monitored to avoid poisoning. Commercial technologies need to be used as a service, and talent acquisition and skilling need to be upgraded constantly.

Endnotes

[1] 'Warfare Today and Tomorrow - Oxford Institute for Ethics, Law and Armed Conflict', *Oxford Institute for Ethics, Law and Armed Conflict*, 7 Mar 2022, accessed 28 Feb 2025 https://www.elac.ox.ac.uk/programmes-projects/solferino-21/warfare-today-and-tomorrow/

[2] Ibid

[3] Ibid

[4] Ibid

[5] 'Indian Defence Industries', 12 Aug 2018, accessed 27 Feb 2025 https://indiandefenceindustries.in/evolution-of-warfare-1.

[6] Alvin Toffler, Heidi Toffler, Matthew Williams, Brookings Institution, Michael Boyle, and Edward Helmore, 'The Impact of Technological Progress on Modern Warfare', *Interesting Engineering* (2021) pp 1-3, accessed 26 Feb 2025 https://www.trinity.ox.ac.uk/sites/default/files/inline-files/Margaret%20Howard%20Prize%20winning%20entry%20-%20Marcus%20Heal.pdf

[7] Advanced Persistent Threats (APTs): APTs are sophisticated and targeted cyberattacks that aim to gain unauthorised access to sensitive information or disrupt critical infrastructure. These attacks are often carried out by nation-states or well-funded hacking groups.

[8] Eva Gorcsosova, 'How Technology Can Create Conflict', accessed 25 Feb 2025 https://www.paccsresearch.org.uk/blog/technology-can-create-conflict/#:~:text=Technology%20has%20shaped%20conflict%20in,used%20to%20defend%20against%20it

[9] United Nations, 'Armed Uncrewed Systems', *United Nations*, accessed 23 Feb 2025 https://disarmament.unoda.org/armed-uncrewed-systems/#:~:text=Uncrewed%20systems%20%E2%80%93%20often%20colloquially%20referred,uncrewed%20systems%20in%20armed%20conflicts

[10] 'What Is Blockchain Security? Is Blockchain Safe?', *Kaspersky*, 18 Jun 2024, accessed 28 Feb 2025 https://www.kaspersky.com/resource-center/definitions/what-is-blockchain-security

[11] 'A New Era of Conflict and Violence | United Nations', accessed 26 Feb 2025 https://www.un.org/en/un75/new-era-conflict-and-violence

[12] 'Natural Resources - Source of Income and Cause for Conflicts, *War and Peace*, accessed 24 Feb 2025 https://warpp.info/en/m4/articles/natural-resources-source-of-income-and-cause-for#:~:text=There%20are%20many%20ways%20in,resource%20wealth%20and%20civil%20wars

[13] 'A New Era of Conflict and Violence', United Nations, accessed 21 Feb 2025 https://www.un.org/en/un75/new-era-conflict-and-violence

[14] Inouye K Daniel, 'Challenges of the United Nations Peacekeeping Operations', *Asia-Pacific Center for Security Studies*, 08 Oct 2022, accessed 22 Feb 2025 https://dkiapcss.edu/nexus_articles/challenges-of-%20the-united-nations-peacekeeping-operations/

[15] Ibid