MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Commentary

Military Applications of Edge Computing

Vivek Reshi

July 30, 2026

Summary

Edge computing can be combined with other technologies like AI, 5G/6G, and Internet of Things to build a smart military ecosystem.

Modern military operations are no longer restricted to a specific arena or domain. They are being increasingly carried out in environments defined by rapid technological changes. This is compounded by the continuous flow of data generated on the battlefield via sensors, devices, and operators across air, land, sea, space, cyber, and the electromagnetic spectrum. Well-oiled military machinery and the defence ecosystem are expected to match these technological developments. They must be able to act swiftly and decisively on data being generated from the battlefield.

Many high-value and analytical military tasks, such as object detection, signal classification, anomaly detection, route optimisation, and predictive maintenance, can be performed more precisely and quickly with Artificial Intelligence (AI)/ Machine Learning (ML) models than by any human military analyst, provided the requisite compute power and data pipelines are available where the mission happens.

Whilst Cloud computing has been a major driver of compute power and data storage, it has several limitations in military/defence scenarios. For starters, it relies on high-quality and reliable network infrastructure between the Cloud and the client device(s). This is not a guarantee in case the military's operational environment lies on the border or in a remote area with little internet coverage—surroundings that represent a large chunk of a military's combat habitat. On the other hand, storage facilities and computational power are both centralised in a cloud computing environment. Critical data storage and high-level data analysis are routed via a central data centre, causing latency or delays in data processing. This is where 'Edge Computing' comes in.

What is Edge Computing?

In technical terms, edge computing is a networking philosophy. Central to this philosophy is bringing computing as close to the source of generated data as possible to reduce latency and network/data pipeline bandwidth usage.[1] Put simply, edge computing decentralises processes of compute, storage and application services from the cloud and transfers the execution of these processes to local places—places closer to where decisions and actions must occur, such as an 'edge' server.

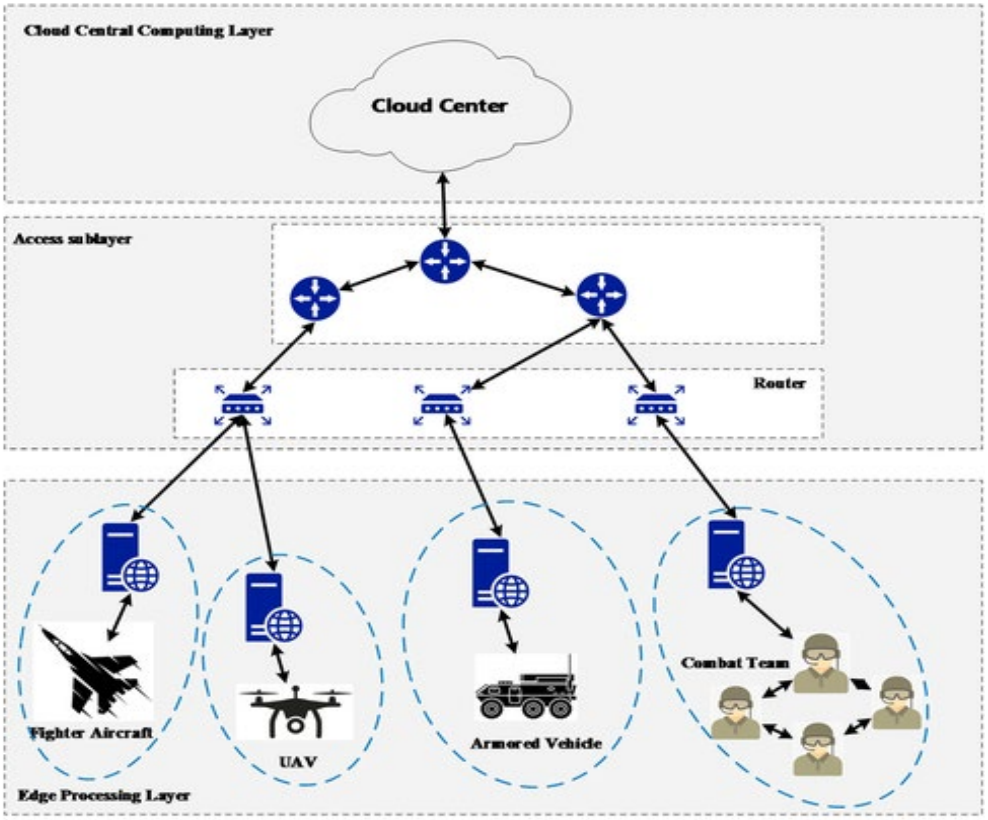
The term 'edge' is considered fuzzy and refers to a combination of different locations. In the military context, it can refer to either a ruggedised compute on platforms (vehicles, ships, aircraft, unmanned systems), or forward-deployed command posts and mobile 'mini-datacentres' or even the processor on a sensor or drone or any other

[1] **"What is Edge Computing?"**, Cloudflare Learning Center.

military tool of its kind operating in the battlefield.[2] For example, the BLADe-S is an indigenously developed, AI-integrated wearable language translator that uses edge computing combined with a built-in neural network processor, offering real-time translation of audio, visual and textual intelligence data.[3]

TurbineOne's Frontline Perception platform is another recent example powered by edge computing and AI. It is used to process complex, multi-source sensor data in environments where communications, bandwidth and cloud access are limited.[4] American frontline forces have tested this platform in ongoing battlefield operations in West Asia.[5] Thus, a key takeaway is that the network edge is geographically closer to the end devices than origin or cloud servers, which are often located much further away.

Figure 1. Edge Computing Architecture



Source: **"Analysis of Key Technologies in Edge Computing and Practical Applications in U.S. Military Operations"**, Association for Computing Machinery (ACM), 19 December 2025.

[2] "Massimiliano Claps and Alan Webber, **"Taking Technology and Data to the Edge: Edge Computing and Data Management for Military and Defense Agencies"**, IDC Technology Assessment Guide, Red Hat, April 2026.

[3] **"The New Age of Defence: Presenting AI Preparedness of the Country in Defence"**, Department of Defence Production, Ministry of Defence, Government of India, 2022.

[4] **"Frontline Perception: Turn Raw Sensor Data into Real-time Detection, Classification, and Targeting at the Edge"**, *TurbineOne*.

[5] **"U.S. Army Airborne Forces Employ Edge AI in Current Operations"**, *Yahoo Finance*, 8 July 2026.

This effectively brings data processing and storage in proximity to the source of data generation, enabling nearby terminals, sensors, or even military operators to access communication and computational services more efficiently. Its decentralised design preserves operational functionality in challenging or limited-bandwidth environments while reducing latency. In the military context, these features enhance combat performance and situational awareness through real-time processing of data from weapon systems, monitoring soldier status, and managing battlefield information.

Military Applications and Challenges

Edge computing, by virtue of its design, can work in remote and disconnected locations—areas that most militaries generally work in. This enables continuous operation and vital data analysis in combat, with little to no network availability. It can also survive in harsh working conditions and needs very little added space to operate. It can also withstand electromagnetic interference, dust, vibration, explosions and current/voltage fluctuations, making it a robust military application on the battlefield.[6] An example case is the Sentry-X2 Mini, a MIL-SPEC certified rugged edge AI system, developed by the firm Connect Tech Inc. (CTI) for critical and autonomous aerospace and defence missions in harsh environments.[7]

Since data processing happens in proximity to the source of the data, edge computing helps reduce both latency and decision response time.[8] During wartime, when military leaders must make decisions efficiently and in real-time, edge computing expedites decision-making by drastically reducing the time between initial data capture and resultant action. The United States Air Force has incorporated edge computing on its F-35 Lightning II fighter jets and localised data processing through an on-board heterogeneous computing unit.[9] In doing so, it has drastically reduced sensor data processing latency.

Edge computing also reduces the risk of sensitive military data leakage by reducing the attack vector/attack surface that a malicious actor can exploit.[10] This is because data does not travel to the centralised cloud servers unless needed. Data can be gathered from edge servers, encrypted and cleansed before being transmitted

[6] Yunna Li, Deyun Yang, Haipeng Lu, Jian Wu and Lu Peng, **"Analysis of Key Technologies in Edge Computing and Practical Applications in U.S. Military Operations"**, In Proceedings of the 2025 8th International Conference on Computer Information Science and Artificial Intelligence (CISAI '25), Association for Computing Machinery, USA, 12 September 2025, pp. 1183–90.

[7] **"Connect Tech Launches Deployment-Ready Tactical Edge AI System, Sentry-X2 Mini, MIL-SPEC Certified for Aerospace and Defense Autonomous Applications"**, *Connect Tech*, 12 May 2026.

[8] Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie Young, **"Mobile Edge Computing: A Key Technology Towards 5G"**, White Paper No. 11, European Telecommunications Standards Institute (ETSI), September 2015.

[9] Jamie Whitney, **"Sensor Fusion Meets Edge Computing for Real-time Ops"**, *Military + Aerospace Electronics*, 15 April 2026.

[10] Sameer Patil and Dhruv Banerjee, **"Edging Ahead: The Importance of Tactical Military Edge Computing"**, Observer Research Foundation (ORF), 16 September 2025.

elsewhere. Thus, edge computing makes data interception harder and improves data privacy and security. Additionally, edge computing also supports network defence applications. The 'Persistent Cyber Hunter' (PCH) project of the United States Cyber Command has demonstrated this capability in real combat during the ongoing conflict in Ukraine in 2024 using a network of intelligent AI agents mounted on frontline communication devices, satellite terminals and shipboard systems.[11]

New developments in the field of edge computing have given rise to the concept of 'digital soldier'.[12] Slightly different from the established notion of soldiers participating in cyberwarfare, the idea of a digital soldier is about utilising small, connected sensors attached to soldiers, ensuring rapid and synchronized local operational data sharing and processing across the network of participating soldiers, giving them a fuller picture of the battlefield from different perspectives.

Commercial technological lifecycles are short, whereas military machine systems are usually designed to last for tens of years.[13] These legacy military systems also lack the processing power essential for edge computing during operations, and some use older communication protocols that transmit data too slowly or too insecurely.[14]

Despite the apparent advantage of applying edge computing in military systems in challenging environments close to the frontline, physical capture of the edge device by the enemy risks exposing sensitive data.[15] These grim operational environments also lack power connectivity or have very little access to it. As such, many edge computing devices have batteries or portable generators fitted on them. But these are temporary fixes to a larger power challenge associated with edge devices.

Conclusion

It is becoming increasingly clear that in the rapidly advancing and digitalised battlefield, quick and informed decisions will hold the key to military success. Therefore, the incorporation of edge computing in military systems is no longer a technological upgrade necessity but a definite requisite from a strategic point of view. It can also be combined with other technologies like AI, 5G/6G, IoT (Internet of Things), etc. to build a smart military ecosystem. Such an integrated network will significantly improve situational awareness, accelerate response times, and support overall decision-making. All this points to the capability of this technology to not only shape the future of warfare, but also improve the current state of military operations.

[11] Yunna Li, Deyun Yang, Haipeng Lu, Jian Wu and Lu Peng, **"Analysis of Key Technologies in Edge Computing and Practical Applications in U.S. Military Operations"**, no. 6.

[12] Greg Dupier and John Pisano, **"How the U.S. Military is Using Edge Computing"**, *Booz Allen.*

[13] **"Edge Computing in the Military – Challenges and Solutions"**, Maris Technologies, 3 April 2025.

[14] **"Top 5 Challenges in Edge Computing"**, *Invenia*, 1 March 2025.

[15] Greg Dupier and John Pisano, **"Key Obstacles to Edge Computing Adoption"**, *Booz Allen.*

About the Author

Mr. Vivek Reshi is Research Analyst at the Manohar Parrikar Institute for Defence Studies and Analyses, New Delhi.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses