IOT TECHNOLOGIES ARE PLAYING AN INCREASINGLY IMPORTANT ROLE ON THE BATTLEFIELD.

OMNETICS
CONNECTOR CORPORATION

How Military Uses of the IoT **for Defence Applications are Expanding**

BY SALEEM KHAWAJA

The Internet of Things (IoT) has changed the operational paradigm of many sectors, not least the defence industry, and military applications and devices are on the rise.

The internet has been the backbone for computing and communication devices to exchange information, with rising speeds, volumes, and complexity. But for all its ubiquity, most users aren't aware of how it is delivered. Here are three basic components of how everyone connects and communicates through the internet.

The Last Mile

The last mile consists of the cables that connect homes and businesses to the internet. It includes towers that enable people to use their mobile phones to access the internet, and a significant and increasing portion of all usage is now made up of wireless internet access.

Data Centres

Servers housed in data centres host online applications and content as well as store user data. They can serve multiple users at once thanks to their incredibly fast internet connections. Although they can be found anywhere in the world, they are frequently found in isolated locations where land and energy are affordable.

Internet Backbone

Long-distance networks, typically on fibre optic lines, are what make up the internet's backbone. They move data between data centres and users. Internet exchange points (IEPs), which are frequently found in major cities, are where backbone service providers frequently link their networks.

The current state of the internet is increasingly in flux with the introduction of the concept of the Internet of Things (IoT). The number of devices that use it to 'talk' to each other is mind-numbing. Fridges, vehicles, vacuum cleaners, domestic heating systems, and even doorbells, are connected.

The IoT is connecting countless physical devices that are transmitting, getting, gathering, and sharing data on a global scale. With the reduction in the cost of computer technology and the widespread use of wireless networks, anything can become a component.

From digital sensors swallowed by a human or animal to monitor medical conditions in real-time, to commercial and military vehicles across the world sending and receiving vast amounts of data, fast interconnectivity between a huge number and variety of applications and devices is increasing exponentially. By fusing the real and digital worlds, it is shrinking the world around us while also making it smarter and more responsive.

IoT is spawning as many sub-divisions as innovators can think of. The main ones increasing in size and reach are Consumer and Commercial IoT, Industrial and Infrastructure IoT, and Medical and Military IoT. We will discover how Military IoT is enabling defence forces across the globe to become smarter, and more responsive, allowing them to plan for and neutralise physical and cyber threats.

IoMT Market

IoT systems and equipment are being used more and more by military organisations to improve operational efficiency and security. The ability to manage logistics and people virtually while on a base, a battlefield, or even in transit, as well as monitor assets anywhere in the world, has given command staff a near-divine real-time view of their current states.

According to a 2022 GlobalData research paper titled 'Internet of Military Things', it is not possible to estimate the precise size of the IoMT market as many devices and applications being researched and developed are sensitive, but it provides overview numbers using the global IoT market and gleaning those civilian solutions that can be used by defence environment.

This includes wearables and hearables, electro-optical/infrared systems, and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems and infrastructure.

The report estimates this market to have been valued at $439bn in 2019, rising to $486bn in 2020, and will grow to $807bn by 2025, at a compound annual growth rate of 11% over the period.

Military Applications

Both IoMT, and the Internet of Battlefield Things (IoBT), use edge architecture that communicates data swiftly and makes use of biometrics, environmental sensors, and other connected devices, enabling military people to react and perform better on the battlefield.

There is general acceptance that technology and artificial intelligence will dominate future conflicts and military activities that may occur in urban settings. For this reason, having as much knowledge and information as you can is essential to making wise choices that will maximise human safety and save lives.

Below are just a few uses for IoMT and IoBT applications.

Advance Battlefield Awareness

Armed forces can scan the battleground using unmanned aerial drones that are fitted with cameras and sensors thanks to IoT. These drones can transmit real-time data to the command centre, capture live images, and track the terrain and locations of the enemies. Officers can monitor the battlefield and quickly make judgements using this data.

Perimeter Security of Smart Bases

Using stolen credentials or posing as civilians, bad actors can gain entry to military installations. Active and passive IoT sensors can collect fingerprints, iris scans, and other biometric data to identify people to single out those who might be a danger.

Soldier Health Monitoring

Knowing a soldier's health condition is another use of IoT in defence and the military. Sensors can track behavioural traits by analysing speech patterns, and physical metrics like pulse rate, body temperature, and thermal distribution.

Real-time Equipment and Vehicle Management

Vehicle maintenance is critical to successful military operations, and tracking battlefield supplies is made easier by gathering data with vehicle sensors. Location, fuel efficiency, mechanical state, damage level (if any), and other parameters, make it possible to spot problems and solve them quickly.

Training with Augmented and Virtual Reality Environments

Using historical real-world data, automated battlefield action models can be developed, and then a virtual training simulation setting is created. The VR/AR gear is attached to the trainees, who are then placed in a simulated environment that records and evaluates the accuracy, emotional state, movement speed, and other metrics to enable commanders to adjust parameters on the fly.

Omnetics Connector Corporation has long been supplying specialist design and fabrication services in this growing field, and it has worked with a combination of micro-miniature sizes, ruggedised reliability, and multiple designs using power inside miniaturised connectors. It has a wide range of products that can handle both power and digital signal in one connector, and further provide data on signal integrity and test capabilities. Its system designers ensure that the design and manufacturing services meet MilSpec test requirements and quality assurance standards.