The Connected Battlefield

A Military Internet of Things is emerging

pwc

Introduction

A new military force multiplier is emerging. This is the Military Internet of Things (MIoT), a world where digital data is drawn from an ever-expanding range of networked sources and integrated to create a multi-dimensional world of intelligence and operations. The MIoT is enabled by many technologies, some familiar, some new, but all converging thanks to advances in device interoperability and improved information processing power. The MIoT is becoming a new military front-line, bringing extraordinary advances in capability but also challenges in terms of planning, management and deployment.

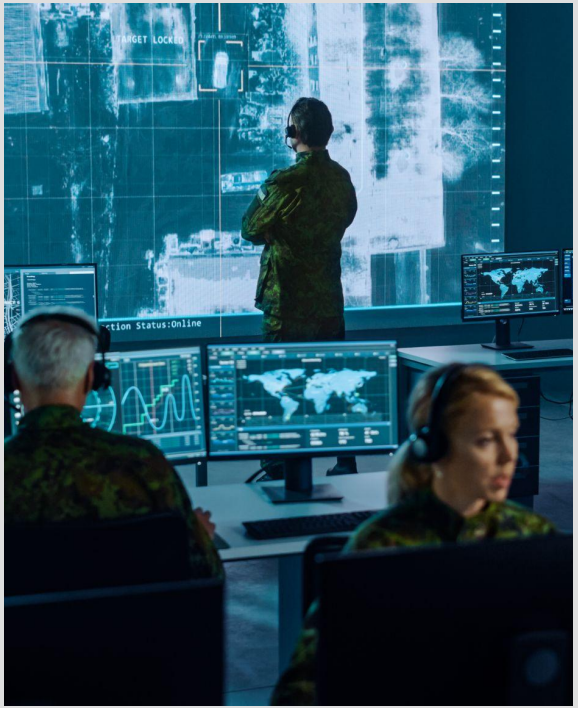
We live in a connected world. It is a world where any kind of device or machine, whether digital or analogue, can be connected to a network, using wireless sensors and switches that can be very small, lightweight and inexpensive. The networks that are created may be limited by design (the so-called ‘edge computing’ model), or may be components of a global data cloud. But everything can, in principle, connect with everything else. **For the military, this creates possibilities for intelligence and real-time control of situations ranging from traffic or infrastructure management to kinetic battlefields.**

Sensing technology comes of age

Intelligence derived from sensing technology is not new. In a military context it is more than a century old. Consider for example the tunnelling sensors devised by the British Army in the First World War. As tunnelling became a critical offensive tactic in otherwise static trench warfare on the Western Front, the Army ran short of personnel to listen for enemy tunnelling activity; in their place, remote sensors (Tele-geophones and Seismo Microphones) were installed, allowing 36 locations to be monitored by just two soldiers at a central listening exchange.

In the Second World War, radar came to the fore, a sensing technology that was first patented by German researchers in 1904 but ignored until it became a vital tool. That was followed by the deployment in the 1950s of the US Sound Surveillance System to detect Soviet submarines, and the acoustic and seismic sensors used by the US Army to detect enemy movement on the Ho Chi Minh Trail in the Vietnam War.

All of these sensor technologies used remote devices in a network to integrate and thus enhance the value of data in conflicts. But they were costly, sometimes unreliable and most often wired devices, pre-dating the internet age with its near-unlimited bandwidth, data storage capacity and processing power.



The MIoT is different. Today's sensors are ubiquitous and mobile. They are operable within a wide range of communication networks, from mobile telephone cellular networks to secure point-to-point communications. They can operate at low power over wide areas (such as WLAN networks already widely used in building management systems) and persist for years without service. They can report the location and status of machines and equipment, execute commands, or use biometric data to identify people and monitor life functions. Above all they are potentially **interoperable, able to feed data into a wide range of networks and machine intelligence capabilities.**

The challenges that come with realising the potential of MIoT are considerable. It requires a high level of organisational skill and data processing capability to integrate pervasive sensing, pervasive computing, and pervasive communication. Military organisations must be able to embrace signals from a diverse and dynamic set of sensors such as static ground sensors and soldier-worn sensors, as well as data from fixed and mobile equipment including intelligence from drones and satellites. They need the agility to keep up with constantly changing technologies, while concealing their capabilities and knowledge from potential adversaries.

In five or ten years time, for example, there is a real possibility that **MIoT technology will allow soldiers to hold up a palm-sized device and know the identities of everyone around them within seconds, at the touch of a button and even in the dark.** However, achieving this means having the capability to link multiple databases and bring together a range of detection technologies. The benefits of this level of situational awareness must also be balanced with citizens' rights to privacy and data protection.

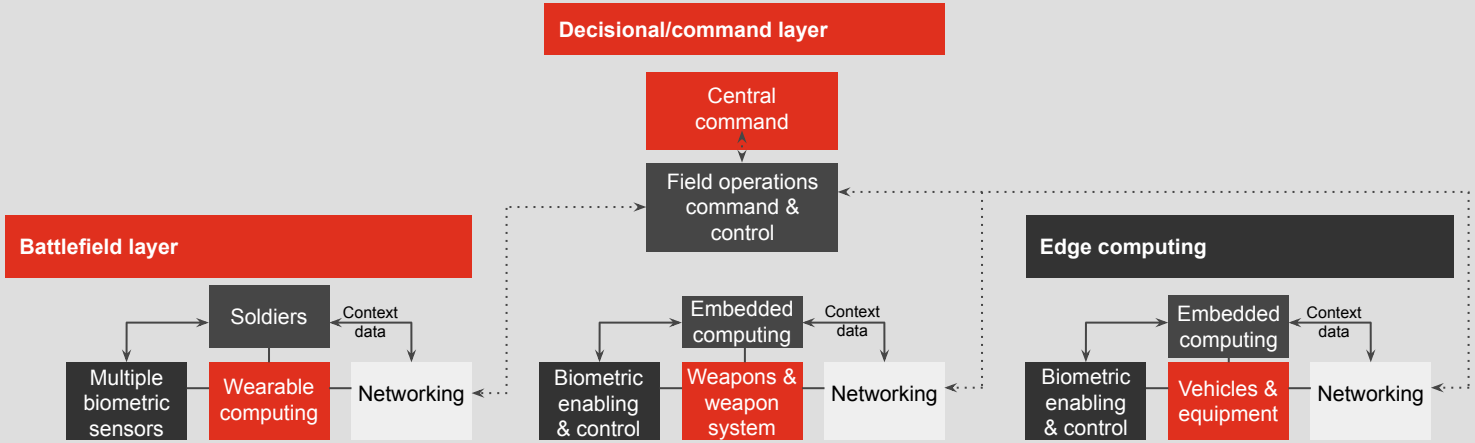
Security is the key

The MIoT also requires a rigorous approach to the integrity of technology deployed and the security of communication through multiple channels.

In a recent paper, the NATO Communications and Information Agency identified security as the leading challenge for MIoT deployment. The authors point out that there have been several instances in recent years of relatively unsophisticated armed groups successfully taking control of unsecured communication channels such as data streams from unmanned surveillance drones. They add that many connected devices such as RFID tags and software-enabled vehicles have proved to be vulnerable to hacking or unauthorised data capture.

To prevent the MIoT becoming another 'attack surface,' whether at the level of connected devices or through back-end data storage and processing systems being compromised, adopters will have to make decisions both on how to secure the physical integrity of devices and sensors, and on how to implement encrypted communications. This is a complex task in a network that may contain many devices with varying levels of encryption capability, and may also include 'Bring Your Own Device' technology such as military personnel's privately owned cell-phones which may create points of vulnerability.

Figure 1: The network of command



Where such challenges as these can be met, there is opportunity to create a sphere based on an unparalleled richness of information, with high-speed, high-bandwidth networks that are secure and un-jammable, where interconnected and self-healing networks and databases support AI-enabled real-time decision-making, and where rich data is fully integrated with military organisations and their doctrines.

Five real-world use-cases

MIoT applications can run through every dimension of military operations, from the planning room to defensive action. The connected military world will embrace data from human and machine sources, crossing over into the world of civilian networks and infrastructure and back again. The use cases generated by MIoT technology will include:

Predictive maintenance

1

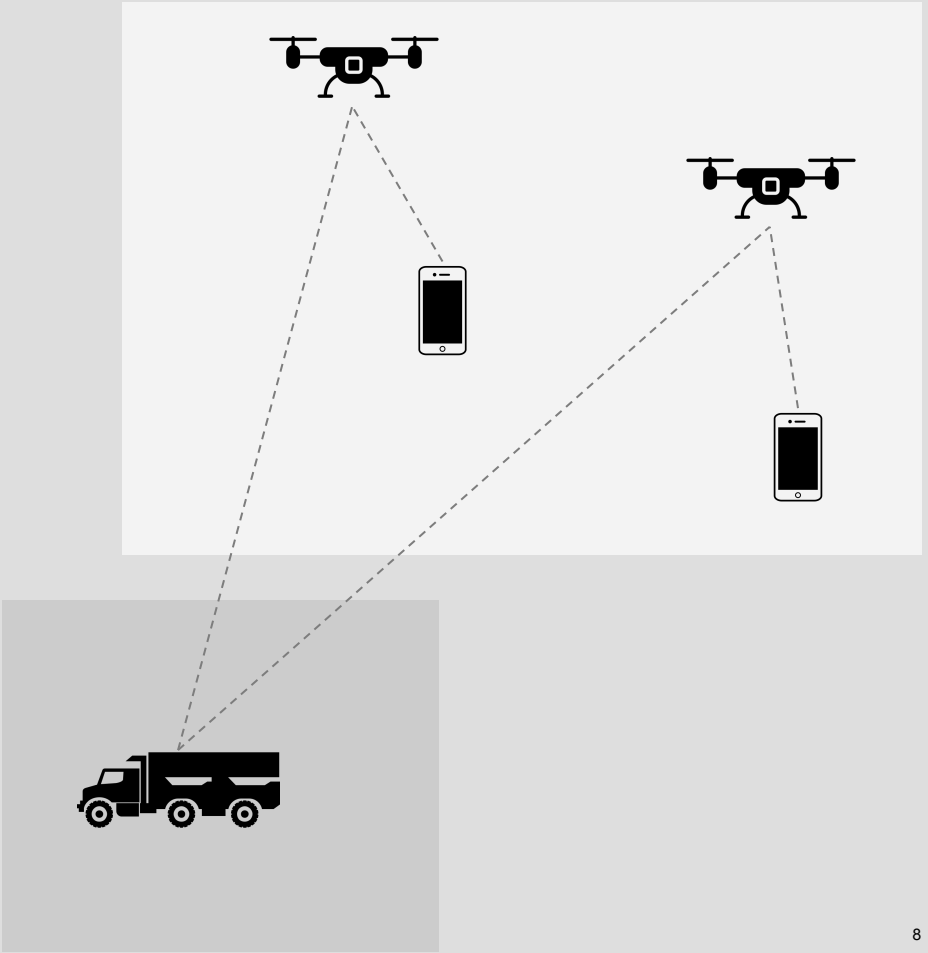
Industrial companies worldwide are already using artificial intelligence (AI) and ‘digital twin’ virtual recreations of machines and processes to create a predictive maintenance model that prevents failure before it is detectable by conventional means, and lowers the maintenance costs. **Military applications will extend to many critical operations all the way to the front line.**

For example, the US Army implemented predictive maintenance for its AH-64 Apache helicopter fleet as early as 2005. **To date, it is believed to have avoided at least four serious air crashes.** In 2015 the Royal Navy implemented the Systems Information Exploitation predictive maintenance package that detects anomalies across 16 different critical systems in the Type 45 Destroyer. In 2019, the US Navy implemented the predictive Hornet Health Readiness Assessment Tool on the F/A-18 multi-role combat aircraft to detect and forestall pressure abnormalities that could disrupt pilot performance. In 2021 the French Army began a trial of an oil flow predictive maintenance system for its latest third-generation Leclerc Main Battle Tank.

2 Civilian infrastructure hijack

In combat it is possible for MIoT-equipped forces to use civilian data networks for offensive purposes, just as in previous eras armies used conventional infrastructure such as roads and waterways.

One example is the cell-site simulator, a wireless devices that can be sent into hostile battlefields by land or drone, picking up the signals of nearby cell-phones and spoofing the signals of a phone mast, thereby ‘tricking’ cell-phones into self-locating by measuring the strength and direction of signals from nearby phone masts (as smartphones routinely do to establish location). These responses locate the cell-phones on the ground and create targets that can be located precisely.

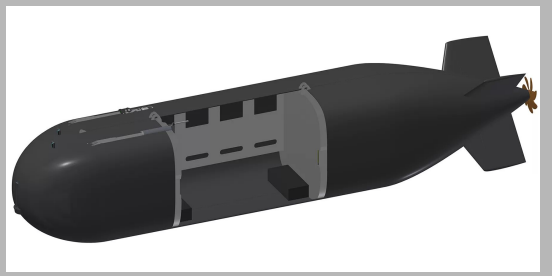


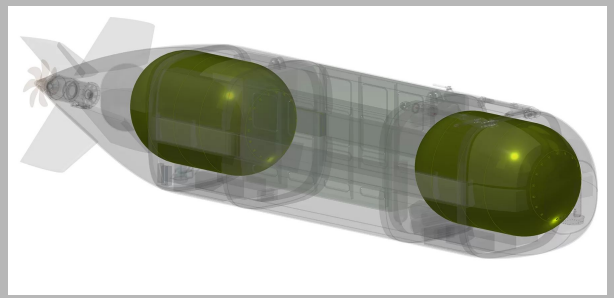
Autonomous systems

3

Unmanned autonomous systems go hand-in-hand with MIoT either in conjunction with one another or complementing each other. Navies worldwide, for example, are increasingly turning to autonomous vehicles for both surface and submersible operations, cutting the large cost of maintaining crewed sea power.

The Royal Navy has been an early adopter of autonomous vehicles. Autonomous mine hunters are already in operation, Pacific 24 autonomous surface boats are undergoing testing, and the Navy is shortly to take delivery of the battery-powered CETUS un-crewed submarine, an autonomous submersible capable of carrying mines, sensors or smaller unmanned submersible vehicles, with a 1,000-mile single mission range and the capacity to dive deeper than any existing submarine.





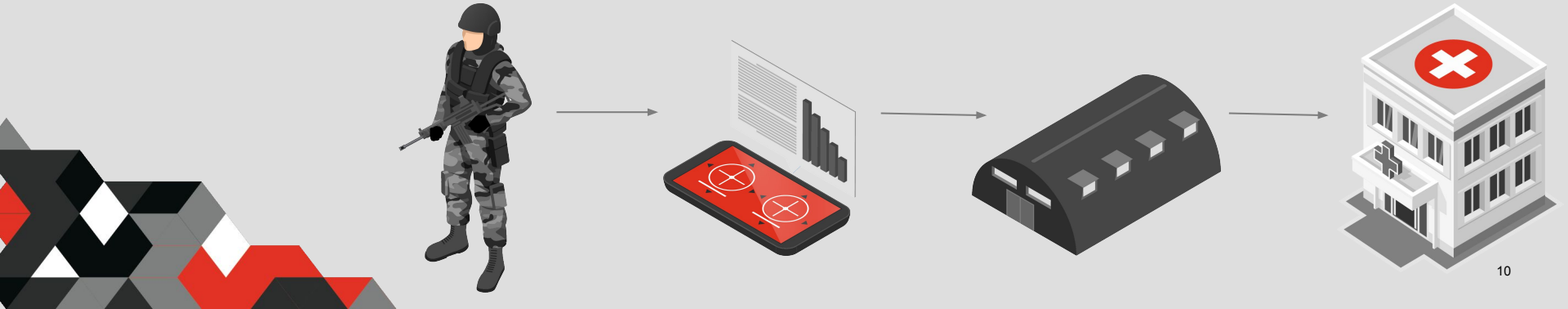
Connected battlefield health

4

The time between injury and treatment is the most critical factor in dealing with battlefield wounds – but one reason that time is critical is lack of information and preparation. The MIoT in medical contexts can change that.

Soldier-worn body sensors, wrist straps or ear trackers that measure heart rate, temperature and location can send automatic alerts to medics and treatment centres equipped to track devices. Combat medics can use ruggedised tablets to log situation details and initial treatment. Field hospitals receive real-time updates on arriving cases and match these with individual medical records.

Fixed hospitals receive full background and current status data, building a record that will be used after discharge to civilian services. The Health Readiness and Performance System (HRAPS), for example, is tailored for field deployment and can track 150 types of health data, from vital signs to dehydration to blast pressures that could lead to brain injuries, and is currently on trial with the US Special Forces.

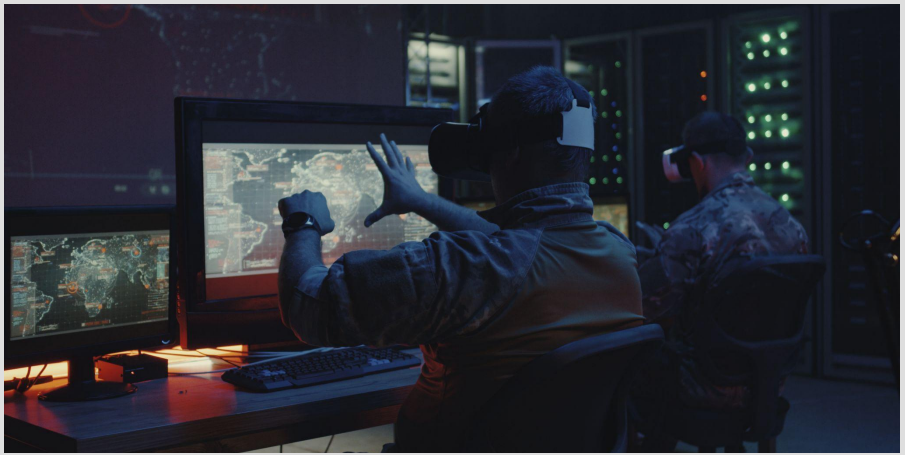


5 Smart bases

The smart military base uses the technologies of networked surveillance, automated building controls for energy management and continuity in the event of attack, and automated logistics management including smart vehicle deployment.

Smart bases using connected sensors and integrated data processing have the potential to revolutionise military effectiveness, especially in temporary settings where fixed and hard-wired conventional infrastructure is prohibitively costly, and where 24/7 security is critical.

Smart bases include surveillance and response technologies that are vital to military security, allowing complex logistics and human resource deployments to be achieved quickly and cost-effectively. Smart security networks and autonomous vehicles have already been deployed in US smart bases at Fort Carson, Tyndall Air Force Base and Maxwell-Gunter Air Force Base.



What next?

Implementing MIoT is a complex organisational challenge. In addition to the difficulty of adapting networked sensing to some of the most complex machines in the world, such as present-generation fighter aircraft, militaries must grapple with challenges of structured evaluation and training, storage and analysis of data, integration of automated and manned resources, and adapting to the speed of operation that the connected world implies.

Security may be the greatest challenge. This includes not only solving the technical problems of access versus encryption, but also the challenge of integrating military assets with networks and devices that may be widely used in the civilian world. The evidence shows that conventional armies have consistently underestimated the capacity of informal and irregular enemies to capture or disrupt networked military assets or lines of communication using technologies widely and cheaply available in the civilian world.

Yet these are the challenges of any significant technological shift. The world is transforming at pace, and if military forces refuse to adapt and evolve, put off by the costs and conceptual difficulties of the MIoT transition, they may find their defences vulnerable and exposed to future MIoT threats. **As society becomes increasingly more digitally connected and devices interoperable, militaries must take stock and look ahead, pro-actively preparing for the battlefields of the future**.

Contact us

Sascha Rodenberg
Partner
PwC Middle East

sascha.rodenberg@pwc.com
+971 56 603 4010

Jay Edwards
Director
PwC Middle East

jay.edwards@pwc.com
+971 54 793 3244

http://pwc.com/me/the-connected-battlefield-MIoT