Mosaic Warfare: The March towards Interconnectivity in US, UK, and European Airpower

Anika Torruella

Senior Analyst, Janes

Information and data-sharing networks have changed the landscape of defence operations. Great-power actors have been investing in technology that enables high-speed connectivity between a growing number of warfighters, networks, and autonomous or manned machines that can interact in a highly complex and increasingly unpredictable battle environment. At the same time there is an emerging drive to link a growing number of sensors, mobile land platforms, aircraft, mission systems, unmanned systems, man-portable devices, human-wearable devices, weapons, munitions, software, and other technology to become a single information network. The overall objective is to create a dynamic and adaptive matrix that enables real-time, actionable, and predictive analytics for decision making, command and control (C2), and other in-theatre capabilities.

The end goal is to shift warfighting from linear decision making to a web of actionable outcomes to deny, deter, and defeat adversaries. The US Defense Advanced Research Projects Agency (DARPA) calls this a shift to 'mosaic warfare' as traditional asymmetric technologies, such as bespoke satellites, stealth aircraft, and precision munitions, offer reduced strategic value in modern warfare due to growing global access to commercially available advanced technology and

components. This mosaic warfare concept is intended to move beyond individual system designs and unique interoperability standards to develop processes and tools dependent on trusted connections between known entities that offer limitless possibilities for creating effects at the tactical, operational, and strategic decision-making levels.

Intelligent interaction

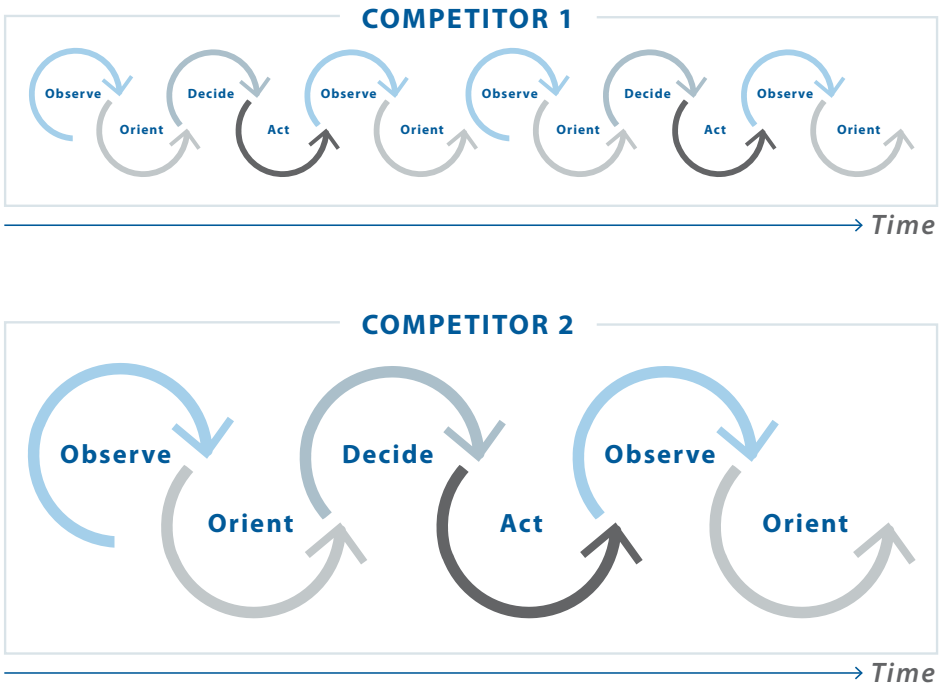
The Internet of Things (IoT) has been used to describe communication and information sharing between large numbers of 'smart' technology nodes. These can then be categorised into data-carrying devices, which are attached indirectly to physical things with communication networks; data-capturing devices, which are reader-/writer-type devices that are capable of interacting with physical things indirectly via data-carrying devices or directly via data carriers attached to physical things; sensing and actuating devices, which detect or measure information in the surrounding environment and convert it into digital signals; and general devices, which have embedded processing and communication capabilities and may include equipment and appliances for different IoT applications (International Telecommunication Union 2012).

IoT can describe city networks, industrial grids, cloud computing, and mobile networks, while its applications have boosted data and information gathering and services when introduced to biomedical, security, and commercial and industrial infrastructure systems. However, due to the relationship between the industrial-commercial complex and defence and military services, applications of IoT technology to modern warfare strategies have come under greater scrutiny. The Internet of Military Things (IoMT), or Internet of Battlefield Things (IoBT), describes technology that enables intelligent interaction among warfighters and their equipment within battlespaces.

Other defence usage of IoMT describes sets of interdependent and networked elements that not only include sensors and devices, but also infrastructure such as storage and data processing equipment, the network used to interconnect

devices and nodes, and the software and machine-learning algorithms that govern them. This incorporates a wide range of military integrated sensors, devices, and platforms capable of intelligent sensing, machine learning, and actuation via cyberspace nodes and human-machine interfaces. These interactions are intended to increase situational awareness and reduce time for processing data, risk assessment, strategic planning, actioning information, and executing objectives. Under a broad definition 'things' could include tanks, warships, aircraft, unmanned aeriel vehicles (UAVs), forward operating bases (FOBs), logistic equipment, transportation and building infrastructure systems, warfighters themselves, or anything that can be integrated with sensing, processing, and transmission capabilities (Russell and Abdelzaher 2018).

Accelerating the OODA Loop for Operational Advantage



In this way IoMT represents the convergence of warfighting domains: their networks, embedded hardware, electromagnetic emissions, communication nodes, mobile processing hardware, software architectures, information management, and data analytics. Just as digital twins mitigate the threat of equipment malfunction, failure, and cyber-based intrusion through simultaneous modelling and continuous prediction of maintenance and performance capabilities, the data collected from the pervasive sensing and communication promised by IoMT can be used for dynamic system optimisation, fault detection, and monitoring and prediction. In addition, IoMT provides the pervasive analysis, management, and C2 needed for a new type of information warfare: one that is decision centric by relying on faster and better decision making, as well as shorter actionable response times.

> ***Fault tolerance is low and failures in communication nodes are catastrophic. Back-ups, digital twins, and alternative communication pathways must be established and secured.***

Unmanned and uncrewed (optionally piloted) aircraft have entered the landscape and proven to be a force multiplier, especially for data gathering and air strikes in long-range, difficult to reach, and/or anti-access/area-denial (A2/AD) regions. They have become the workhorses for in-theatre intelligence, reconnaissance, and surveillance (ISR) and are already performing a wide range of military mission roles. A number of countries are developing future-combat air systems (FCAS) programmes that envision high-performance, network-enabled, unmanned aircraft that fly in concert with manned combat aircraft—either in swarms or as a 'loyal wingman'—to close this gap.

Loyal wingman concepts operate as an extension of the sensors and other systems of manned aircraft, with capabilities to disrupt, damage, or destroy target air-defences while surviving in contested A2/AD environments. These teamings seek to create overmatch by shifting traditional manned combat aircraft formations to new mixes of manned and unmanned platforms that create more agile, stealthy, and lethal weapons delivery. If the awareness-to-decision-to-response chain of modern warfare is to accelerate to cyber speed, machine-human team-

ing with AI-boosted analysis and edge computing in-theatre is required. The interconnected technology of mosaic warfare will leverage unmanned systems with machine intelligence self-aware enough to assess the status, goals, and vulnerabilities of missions to counteract disruptions in real time.

JADC2 and Advanced Battle Management System in the United States

The USAF the Advanced Battle Management System (ABMS) is part of a wider plan by the US military to create a Joint All-Domain Command and Control (JADC2) concept, which is looking to build an IoMT by connecting sensors from all across all US services into a single collaborative network. Previous efforts saw each service develop its own tactical network, although these were incompatible with each other. According to the US Congressional Research Service, with interoperability based on a common multi-domain IoMT the US DoD seeks to transform "the current multi-day process to analyse the operating environment and issue commands" into a process that takes "hours, minutes, or potentially seconds" for future conflicts and operating environments. The US DoD has also stated that the existing C2 architecture is insufficient to meet the demands of the US National Defense Strategy (NDS).

The US Air Force's (USAF's) IoMT programme, the ABMS, was originally envisioned to replace the USAF's E-3 Sentry Airborne Warning and Control System (AWACS) platforms. However, it took on a broader scope when former assistant secretary of the Air Force for Acquisition Will Roper stated that the contested environment envisioned by the 2018 US National Defense Strategy had forced the air force to restructure ABMS. Roper directed that ABMS become less focused on command centres and aircraft while refocusing on creating digital technologies, such as secure cloud environments, to share data across multiple weapon systems.

The ABMS IoMT is now intended to encompass a family of systems that includes hardware and software designed to improve anti-access/area denial (A2/AD) management and enable USAF elements to co-ordinate with and conduct joint

operations with the US Navy (USN), US Marine Corps (USMC), and US Army. According to the US Congressional Research Service, the USAF has performed five events to demonstrate the new C2 capabilities it intends ABMS to field. In December 2019 the air force showed the capability to transmit data from a US Army radar (an air-defence sensor and firing unit) and a USN destroyer (the Arleigh Burke-class guided missile destroyer USS Thomas Hudner , deployed in the Gulf of Mexico) to Lockheed Martin F-22 Raptor and F-35A and F-35C Lightning II Joint Strike Fighter combat aircraft, in addition to the US Space Force Unified Data Library (UDL), which is a cloud environment combining space- and ground-based sensors to track satellites.

In September 2020 ABMS detected and defeated a simulated US-bound cruise missile using hypervelocity weapons. ABMS also exhibited capabilities to "detect and defeat efforts to disrupt US operations in space". In the same month the USAF used a KC-46 tanker aircraft to perform tactical C2 by relaying data from fourth-generation fighters to fifth-generation aircraft, such as the F-22 Raptor, during Exercise 'Valiant Shield' at Joint Base Pearl Harbor-Hickam in Hawaii. In February an abbreviated demonstration was held in Europe that linked allied nations, including the Netherlands, Poland, and the United Kingdom, into combined air operations. According to General Jeffery Harrigan, commander of USAF Europe, the event tested US and allied capabilities to perform long-range strike missions with F-15E aircraft launching AGM-158 Joint Air-to-Surface Standoff Missiles (JASSMs) while using US and allied F-35s for airbase defence missions. In May the USAF stated that procuring a communications pod for the KC-46 would be the first capability release for the ABMS programme.

IoMT in the UK and Europe

Concepts for a programme similar to ABMS were published in April by the UK Ministry of Defence's (MoD's) Digital Strategy for Defence effort. This is intended to create a secure, singular, and modern 'digital backbone' connecting "sensors, effectors, and deciders across military and business domains and with partners, driving integration and interoperability across domains and platforms" by 2025.

"We have too often traded out technology refresh and have not driven sufficient integration and commonality," the MoD warned. "Continuing down this path will prevent us from exploiting emerging technologies at the pace and scale required to deliver the Defence Purpose."

The UK Digital Strategy went on to highlight that access to, and control of, the electromagnetic spectrum (EMS) is essential to all operations and the functioning of the digital backbone, adding that with the advent of 5G and IoT the cyber domain would grow "far faster and wider in the next few years. As such, data and architectural standards, as well as management of the EMS, will secure operational advantage and freedom of manoeuvre."

The UK's loyal wingman platform, Mosquito, for the Tempest optionally piloted future fighter jet is under a programme known as the Lightweight Affordable Novel Combat Aircraft (LANCA). Mosquitos will be compatible with UK aircraft carriers and will be able to perform a range of roles, such as weapons carriers and/or decoys or serve as weapons themselves. The UK FCAS programme also includes Alvina swarming drones and other legacy platforms networked together by a combat cloud, with uncrewed aircraft expected to replace UK Typhoon aircraft air-to-air combat capability by the mid-2030s.

European IoMT initiatives include the Wireless Sensor Networks for Urban Local Areas Surveillance (WINLAS) and Cloud Intelligence for Decision Making Support and Analysis (CLAUDIA) projects, which fall within the scope of the European Defence Agency (EDA). The WINLAS programme researches large sensor networks of heterogeneous devices for urban warfare, energy systems, and information management in large-scale soldier modernisation systems. The research from this project builds partly on the results of the EDA's Information Interoperability and Intelligence Interoperability by Statistics, Agents, Reasoning, and Semantics (IN4STARS) programme, which is intended to improve situational awareness in urban areas by using AI, sensors, and energy harvesting to prolong network operation.

The main objective of CLAUDIA is to develop modular software analysis platforms to support the analysis and assessment of military scenarios, especially those exercised during hybrid warfare. CLAUDIA is intended to support the needs of commanders in terms of analysis, decision making, and planning. Its platforms will collect, process, and analyse data from heterogeneous information sources to provide situational awareness and a comprehensive common operational picture (COP) to support planning, decision-making processes, and co-ordination of EU member states.

On the other hand, France, Germany, and Spain have agreed to jointly develop the Next-Generation Weapon System (NGWS) element of their Système de Combat Aérien Futur (SCAF) FCAS programme, called Remote Carriers. First flight demonstrations of the European SCAF/FCAS programme are intended to occur in 2027 and the final proposed design is slated to be frozen in 2030 ahead of a proposed in-service date of between 2040 and 2045. The programme will include the Eurodrone (also called the EuroMALE—European Medium-Altitude Long-Endurance [MALE] Remotely Piloted Aircraft System [RPAS]), an ultra-low observable unmanned combat aerial vehicle (UCAV), future cruise missiles, and legacy platforms operating in the future battlespace.

Operational vulnerability

Implementing IoMT is not without substantial challenges. Complexity arises from the increasing scale, functionalities, and interdependence of the networked elements, as well as from the speed and volume of data collection and production of new information. The new speed of war—driven by automated battle networks and increased computing power—is cyber speed, where network attacks and electronic warfare dominate the information landscape. In addition, despite the capabilities that IoMT offers to defence applications, operational vulnerability is the most critical concern.

Another challenge presented by interconnecting different types of weapons and warfighters is that battlefield scenarios require real-time decisions and re-

sponses. Fault tolerance is low and failures in communication nodes are catastrophic. Back-ups, digital twins, and alternative communication pathways must be established and secured. In addition to 'things' and IoMTs that forces own and control, they may also need to use military, commercial, industrial, or adversary IoTs that they do not own or fully control. Authentication would need to accommodate deceptive data and counter advanced persistent threats (APTs). New elements would need to be secured and updated regularly to prevent APT incursions, which are increasingly frequent, complex, and subtle.

> *If the awareness-to-decision-to-response chain of modern warfare is to accelerate to cyber speed, machine-human teaming with AI-boosted analysis and edge computing in-theatre is required.*

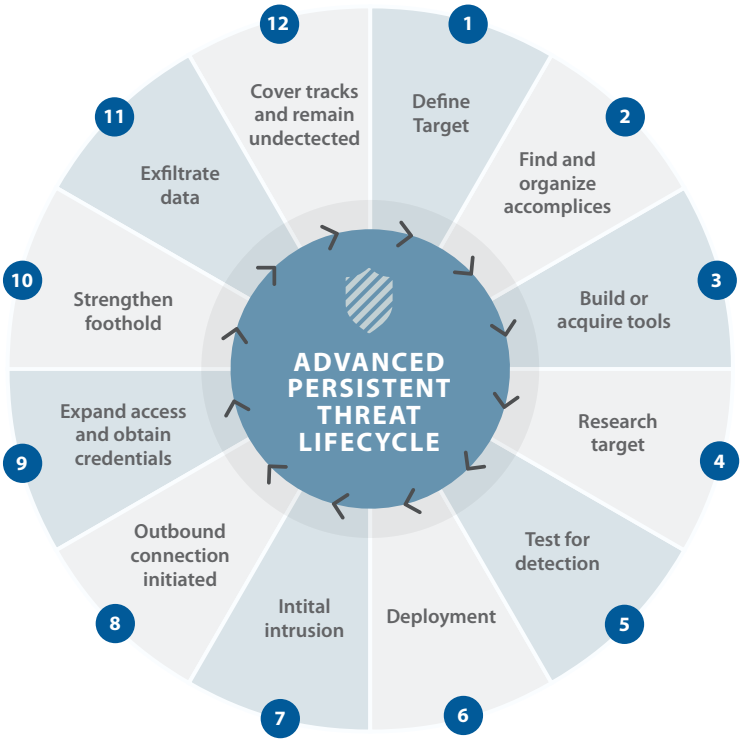
In addition, with IoMT implementation the number of battlefield interactions between constituent things will increase over time. Commercial and industrial protocols that are useful for scaling are unlikely to be effective in the resource-restricted environment of a battlespace where throughput may be limited. The processing and computational requirements are also likely to increase, which makes real-time responses and outputs more unlikely.

Interoperability, energy efficiency, and quality of service are also considerations. The dynamic nature of interoperability—whether between US forces or EU member states—is challenged not only by the different applications and devices used in the battlefield, but also the diverse operational and equipment standards that stem from the devices of different manufacturers of various allies, all of which may not be operating at the same level of technological advancement.

Developing a small form factor for wearable devices without degrading user experience is another challenge, especially since reducing size and weight generally also reduces battery capacity as well as charging and cooling capabilities. The US Army has noted its interest in IoMT for diverse and dynamic missions that will require rapid deployment and adaptation in environments with high mobility, resource constraints, and extreme heterogeneity in very dense and

sparse environments. Degraded transmission quality or drops in real-time analysis would indicate a failure of the entire matrix.

Advanced Persistent Threat (APT) Lifecycle



Conclusion

Despite all the challenges, the march towards interconnectivity seems inexorable. Such disruptive shifts in military thinking coincide with the offset strategy that drove nuclear superiority in the 1950s (First Offset) or the military overmatch provided by guided munitions and battle networks during the 1970s and 1980s (Second Offset). When the US DoD started to think about a Third Offset strategy in 2014, AI, autonomous systems, and human-machine teams were recognised as critical to gaining tempo. As strike velocities and ranges

increase alongside the speed and volume of accessible data, pervasive interconnectivity, interoperable networks, and improved standards of unmanned/manned coordinated behaviour will set new foundations for achieving air power superiority.

References:

International Telecommunication Union. 2012. Series Y.2060: *Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks: Next Generation Networks—Frameworks and functional architecture models: Overview of the Internet of things* [online]. Y.2060. Available from: *https://www.itu.int/rec/TREC-Y.2060-201206-I* [accessed 26 October 2021].

Russell, S, and Abdelzaher, T. 2018. The Internet of Battlefield Things: The Next Generation of Command, Control, Communications and Intelligence (C3I) Decision-Making In: *MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM)*. Oct 29-31, Los Angeles. IEEE.

Anika Torruella is a Senior Analyst at Janes, covering naval electronic warfare, C2 systems, and sonar technology, with extensive further expertise in artificial intelligence, robotics, naval warfare, space, future computing, nanotechnology, and new materials. Over the past two decades Anika has also worked with the World Bank, Access Intelligence, and National Geographic. Anika graduated with a BA in Physics from Bryn Mawr College in Pennsylvania, where she studied Mathematics and Astronomy and was a Research Fellow.