Picture credit: US Air Force

The US Air Force is currently 1,800 maintenance personnel short

HUMAN-MACHINE COLLABORATION

Rob Mather *explains why military logistics and manufacturing are on a trajectory driven by industrial-grade artificial intelligence, I5.0, and maritime innovation*

We are entering a significantly technology-oriented era across air, land and sea domains. These crucial developments include in the hangar: the increasing adoption of artificial intelligence supported maintenance designed to augment the skills of human technicians and address critical workforce challenges. In the factory: the integration of I5.0 principles into defence manufacturing places human well-being and collaboration at the centre of advanced production processes. At sea: there is the transformative impact of autonomous systems, especially the emergence of sea-based drones, which is poised to revolutionise naval warfare strategies and fleet composition. Underlining these technology developments is growing urgency for defence organisations to implement comprehensive cyber security frameworks in response to evolving digital threats.

The ever-present skills gap in defence MRO continues apace in 2025. The defence industry is seeing an influx of next-gen platforms, as more global defence forces adopt the F-35 and completely new aircraft, such as the B-21 Raider (a more technologically advanced subsonic strategic bomber) enter the fray, bringing the need for an entirely new maintenance knowledge base.

The workforce numbers are plain to see. According to War on The Rocks, the US Air Force alone is currently short 1,800 maintenance personnel, with the US Government Accountability Office highlighting continuing challenges meeting aircraft readiness targets. To help mitigate these issues, Deloitte views 2025 as a pivotal year for defence organisations to consider the role AI technologies could play in enhancing traditional talent strategies.

One obvious application of AI is Optimisation, which offers several key Industrial AI use cases that can directly help organisations accomplish more with existing resources including:

Schedule Optimisation: Increasing the maintenance yield by scheduling all activities to as close to their deadline as possible. Overall, this means over the lifetime of an asset, less total maintenance will be done, actually reducing the total work for technicians.

Task Order Optimisation: AI can analyse data to ensure the order in which tasks are performed is optimised to make the most of the resources and technicians available and perform maintenance in the most efficient order, minimising unproductive time.

Optimisation of Technician Assignment: MROs can even optimise the assignment of the technician to the task, dependent on the technician's skills, availability of assets requiring maintenance and even geography/location on the aircraft, again, lowering unproductive time and maximising utilisation of the most valuable personnel.

Beyond optimisation, giving technicians access to specialised AI agents through mobile devices can help them quickly navigate complex technical information and manuals, particularly those for new and less familiar aircraft types, as well as reduce time spent troubleshooting by providing root cause and repair suggestions, while enhancing data entry –thereby empowering a single technician to accomplish more.

But it's not just in the hangar where technology is directly helping human workers in the defence industry. Defence manufacturing in 2025 will see increasing adoption of the core principles of Industry 5.0 – and its humanising influence on factory processes, including how workers train for and execute work on the factory floor and beyond.

MEET THE META-OPERATOR

Some schools of research describe a "Meta-Operator", defined an industrial worker that follows the principles of Industry 5.0 and interacts with Industrial Metaverse applications and with his/her surroundings through advanced Extended Reality (XR) devices.

XR is already being used as part of training, allowing them to encounter scenarios that are very rare in the real world and therefore take much more time to accrue experience against in conventional programmes. Deloitte flags in its A&D Outlook for 2025 with: "emerging technologies such as extended reality, the industry will likely begin to enhance the training environment and shorten the time it takes to bring employees up to speed." The use of XR is already making its way onto the floor though as well. Digital overlays comparing final product to spec, instructions overlayed on the product itself providing visual next steps, accessing the health information of the manufacturing machinery being used in their field of vision and even gesture control to access technical documentation, are all examples of XR empowering a more efficient and effective worker.

New forms of interacting with systems extends into the aftermarket as well, once assets are manufactured and deployed in the field. Companies including BeastCode are developing 3D models of assets, such as in-service Naval ships. So, when technicians are executing maintenance on the ships, they can navigate straight to the part in question via the 3D model to look at it, investigate, manipulate it, and understand how it interfaces with other parts. It forms an intuitive navigation model – where technicians are able to move around the 3D model to easily navigate the system and access all the pertinent information, taking digital twins to the next level for an experience straight out of science fiction.

THE DEFENCE OUTLOOK FOR 2025 IS OF DYNAMIC ADAPTATION AND STRATEGIC FORESIGHT

The impact of drones and uncrewed systems on naval warfare is clear to see. We have no further to look than the conflict in Ukraine to see that no longer are multi-billion-dollar aircraft fleets or submarines required to disable large ships. Ukraine has disabled up to one-third of the Russian Black Sea fleet largely utilising small remotely piloted sea drones. As a result, the make-up of naval fleets and the design of naval vessels is changing. More of the ships being developed in the future will be autonomous or have minimal crews based on the capability of automated systems available today. Conventional Aircraft Carriers are being joined by UAV carriers, exemplified by recent orders and testing of UAV carriers from Portugal, Türkiye, and the UK. These carriers provide the ability to launch drone-attacks from sea. We are learning that bigger does not necessarily mean better.

Uncrewed systems are also high priority in the US DoD Replicator initiative to augment "the way we fight, using large masses of uncrewed systems which are less expensive, put fewer people in the line of fire and can be changed, updated or improved with substantially shorter lead times."

Autonomous capabilities will be in high-demand IFS customer Austal is working closely with the United States Navy and Royal Australian Navy and was recently awarded a $44-million autonomous design and construction contract by the US Navy, to deliver autonomous capabilities to the Expeditionary Fast Transport (EPF13).

This ship is a multi-use military platform capable of rapidly transporting troops and their equipment, supporting humanitarian relief or operational efforts, and can operate in shallow waters. But supporting this level of autonomy means being able to collect and analyse vast amounts of data from sensors and other sources and produce actionable insights that improve mission success. As such, while capital ships will continue to form the core of large navies worldwide, more and more of the fleet mass will begin to shift to ships with minimal crews and smaller, faster, cheaper, uncrewed vessels.

With increasingly digitised assets come increasingly tightened digital compliance requirements across the defence industrial base – and cyber security is top of mind for defence departments – none more so than the US Department of Defense. In October 2024, the Cybersecurity Maturity Model Certification (CMMC) Program Final Rule was published and is expected to come into effect in mid-2025, with the Five Eyes nations aligning their own cyber security programs to the CMMS framework.

THE IMPACT OF DRONES AND UNCREWED SYSTEMS ON NAVAL WARFARE IS CLEAR TO SEE

The US DoD outlines: "The purpose of CMMC is to verify that defence contractors are compliant with existing protections for federal contract information (FCI) and controlled unclassified information (CUI) and are protecting that information at a level commensurate with the risk from cyber security threats, including advanced persistent threats." With the Five Eyes nations looking to align to CMMC requirements, organisations in the defence supply chain who have not prioritised compliant levels of cyber security run the risk of losing contracts and their place in the defence industrial base.

Imposing more stringent requirements across the defence industry is needed to harden digital defence against external threats such as IP theft can seriously erode hard won technological advantages on the battlefield. Alongside the CMMC requirements is the need for cloud-based solutions to adhere to the Federal Risk and Authorisation Management Program (FedRAMP) that provides a standardised approach to security assessment, authorisation and continuous monitoring. Although not necessarily a true requirement for all cases, FedRAMP is fast becoming a de facto security standard for doing business in the US defence supply chain, but defence organisations need to make sure they are supported by manufacturing software architecture that adheres to military regulations now and into the future. With a secure managed cloud or hybrid enterprise software environment for critical compliance areas such as CMMC, FedRamp or ITAR, defence organisations can operate knowing compliance is assured.

It's clear the defence industry is embracing a future defined by intelligent integration and moving to meet increasingly digitised threats. AI is stepping up not to replace humans, but to amplify their capabilities in critical areas such MRO, directly addressing skills gaps and boosting efficiency. Alongside this, Industry 5.0 is injecting a human-centric approach into manufacturing, leveraging advanced technologies to create more intuitive and effective work environments. The maritime domain is witnessing a significant shift, with the rise of autonomous systems and smaller naval platforms challenging the make-up of traditional fleets. Underpinning all these advancements is the cyber security imperative, as stringent regulations and the escalating threat landscape demand a proactive and robust defence of digital assets.

Ultimately, the defence outlook for 2025 is one of dynamic adaptation and strategic foresight. Organisations that proactively embrace human-machine collaboration, prioritise digital resilience, and understand the evolving nature of warfare will be best positioned to navigate the complexities and capitalise on the opportunities ahead ●

Rob Mather is VP Aerospace & Defence at IFS.

Ukraine has disabled up to one-third of the Russian Black Sea fleet largely utilising small remotely piloted sea drones