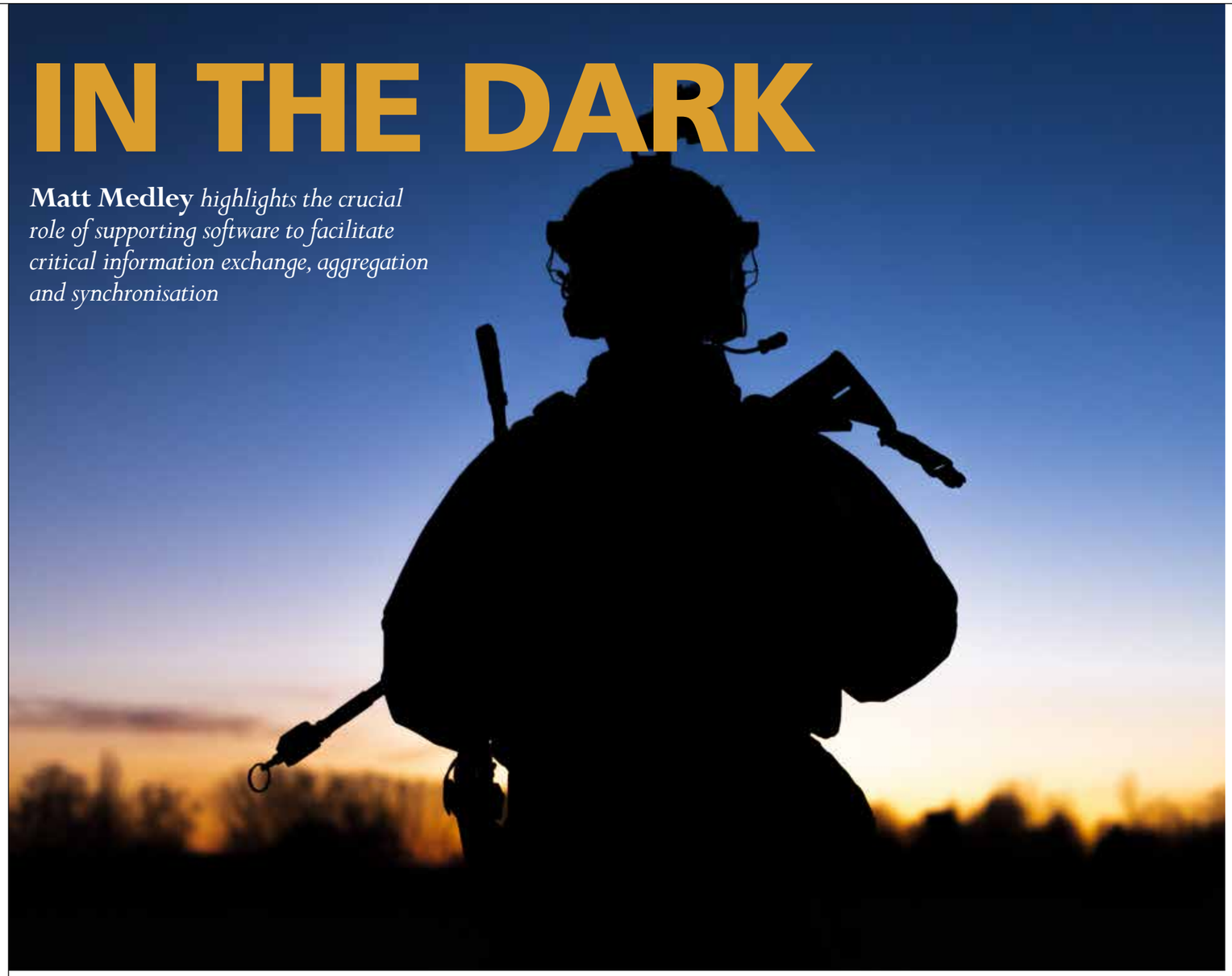
IN THE DARK

Matt Medley *highlights the crucial role of supporting software to facilitate critical information exchange, aggregation and synchronisation*



Picture credit: US Dept of Defense

As military operations across land, air and sea become increasingly distributed, keeping an up-to-date view of equipment status requires a robust digital backbone. This backbone has certainly grown over the last 12 months, as more organisations progress on the journey to maintaining Total Asset Readiness through a connected network of equipment and personnel, which feeds crucial data into an overarching software system. But any break in this connectivity can pose a serious threat to this force-wide view and impact mission success.

The importance of supporting access to organisational information from anywhere is reflected in the business world too. Gartner listed 'anywhere operations' as one of its top strategic technology trends for 2021, defined as: "an IT operating model designed to support customers everywhere, enable employees everywhere and manage the deployment of business services across distributed infrastructures."

A recent study from RAND Corporation, an American non-profit global policy think tank created by the Douglas Aircraft Company to offer research and analysis to the United States Armed Forces, illustrates this move to 'distributed operations' perfectly in the context of the Air Force. The study focuses on a set of emerging concepts for 'distributed operations' that call for a larger number of airbases to complicate enemy targeting and use a more decentralised command and control approach.

In direct response to increased air and missile threats posed to larger main bases, the study notes that the US Air Force is shifting toward concentrating on conducting missions from smaller forward operating locations or bases (FOBs). In order to maximise visibility, there needs to be consistent connectivity between a main operating centre or base (MOB) and these distributed FOBs. RAND then rightly highlights that any disruption to this connectivity by enemy attack on long-distance communications systems, including satellites and long-distance fibre, can seriously compromise mission success.

There are also planned instances where units will be conducting operations in 'dark mode'. A small percentage of top-secret military operations will, by their sensitive nature, take place in a disconnected environment, without outside-world connectivity and with a purposely minimised electronic signature. For some military units, planned instances of disconnected operations is part of the normal day-to-day business. Think a navy frigate sailing in the South Pacific where it operates in a disconnected, intermittent and limited bandwidth mode for much of its detachment unless using satellite.

A small percentage of operations take place in a disconnected environment with a purposely minimised electronic signature

The key requirement in both of these planned or unplanned disconnected operations scenarios is the ability to aggregate, update and re-sync data back to a MOB as soon as connectivity is re-established – mitigating the impact of any outage.

When units are deployed in limited forward operating environments, it can become challenging to bring full software systems such as those designed for asset maintenance onto the frontline – thankfully most military organisations are now able to do that when network connectivity is robust. But any break in connectivity can hinder communications among units (think requests for resupply) and possibly compromise the integrity of databases, maintenance software and decision support systems.

Militaries need the ability to continue operating a network at a moment's notice, even when all outside connectivity is lost, and then incrementally re-sync information such as engineering & maintenance data, technical records and more. Although this may sound simple, this is a very complex undertaking from a data architecture perspective.

Let's take an aircraft as an example. When transferring an aircraft from a MOB to a new forward operating node it is not only the physical asset which is being sent! Its logistics support material needs to move with it, from up-to-date technical records to physical spare parts.

During operations, the aircraft's systems will probably be connected via internet, radio, satellite internet, VoIP etc. 99 percent of the time – but it's the 1 percent of time it may spend disconnected which opens potential problems in data consistency. Without consistent information on what has taken place in the field, such as maintenance, the MOB or home station cannot gain a single version of the truth on the aircraft's status and availability – limiting a commander's ability to make decisions, particularly if they're making decisions about a mission from the other side of the world.

This scenario of course applies to many military assets, you only have to look at naval equipment, which commonly operates at huge scale and in disconnected environments. This scale is only set to increase, as current US Navy plans highlight a force-level goal for an even more distributed fleet architecture, including 382 to 446 manned ships and 143 to 242 large UVs by 2045.

Flipping the scenario around, there will also be key equipment updates that will be communicated out from an MOB and need to be received by personnel in a FOB. Entire assets come with an allowable baseline configuration, which will be subject to change and updates on a regular basis. In defence operations, the Central Engineering Authority (CEA) creates and maintains the maintenance and equipment baselines, and baselines at autonomous bases must remain as up-to-date as possible.

Continuing the aircraft example, any changes to its allowable configuration or critical technical bulletins must be 'pushed' outwards to all operational nodes. Depending on its current status, certain airworthiness updates may directly impact an individual aircraft's safety and ability to carry out a mission, so they must be accessible for the personnel operating the aircraft on the front line.

ANY BREAK IN THIS CONNECTIVITY CAN POSE A SERIOUS THREAT TO A MISSION'S SUCCESS

Two-way data exchange ensures all parties are viewing timely and accurate information, and this data-driven approach directly translates into better strategic decision-making. The answer to Total Asset Readiness in distributed operations doesn't lie in "quantity" – for example more maintenance personnel to keep assets running – it lies in "quality" data – consistent, accurate and timely information to drive more efficient asset management.

To effectively manage disconnected operations, the underlying software infrastructure requires the capability to aggregate, consolidate and store data, while providing physical and software-based hardening against attack. Incremental reconsolidation from supporting software is the most effective way to facilitate a two-way information exchange between a MOB and FOB.

Once an asset returns to connected status, supporting software must sync information both ways, establishing a feedback loop to ensure there is an accurate and up-to-date single version of the truth down to the individual asset level. The other critical requirements to keep all parties updated when information is resynced are scale, security and user experience.

This is where containerised architecture is key and involves bundling an application together with all of its related configuration files, libraries and dependencies required for it to run in an efficient and bug-free way across different computing environments. Containerisation meets the challenges of scale, rapid deployability and being self-contained as secure, standalone software.

Military operators require purpose-built software to address the unique challenges of operating from remote and austere environments in the following focus areas:

- Asset compliance and baseline updates
- Supporting software should be able to address the core requirement needed to transfer

assets between nodes for military operations, including asset transfers (air vehicle and loose inventory), baseline transfers along with the asset, and technical records transfers along with the asset. Workflow management functionality should prepare deployments and imports of assets from MOBs to FOBs and inversely from FOBs to MOBs. When assets are transferred, baseline updates and a portion of their technical records are automatically transferred. Conversely, bases can view the batch number their location is using and request an update from MOB or CEA.

TECHNICAL RECORDS REPOSITORY

In situations where technical records for an asset are created in multiple internal or external systems, command or central maintenance management requires an aggregated view of an asset's technical records. A Technical Records Repository (TRR) should enable planners, reliability departments and others to view the full set of historical records for maintenance performed and usage accrued on an aircraft or component. Bases that perform maintenance can keep the central TRR up-to-date by sending technical record updates through the built-in workflow manager feature.

INTEGRATION WITH CORE MAINTENANCE SYSTEM

This disconnected operations functionality should be fully integrated into core maintenance management software, eliminating the need for data duplication. This integration delivers a complete spectrum of military equipment maintenance management in a single integrated business platform.

In the January issue I highlighted how a robust digital backbone had revolutionised military equipment readiness, giving commanders, maintenance personnel and frontline operators better insights into force-wide asset status than ever before. But this digital backbone can be compromised if supporting software cannot cope with planned or unexpected connectivity disruptions.

Underlying software has to be able to be able to collect, analyse and re-sync data from disconnected operations to ensure all stakeholders have a completely accurate picture of their military assets, wherever and however they may be deployed. Only then can military organisations truly be able to maintain that all important Total Asset Readiness

Matt Medley is Senior Product Manager, IFS

Operatives need to be able to continue operating a network at a moment's notice, even when all outside connectivity is lost

Picture credit: US Dept of Defense