Support providers need to do more to ensure that components are mission ready

Picture credit: IFS

WORKING EFFICIENTLY

Evan Butler-Jones *examines the latest technical, tactical and political developments in defence logistics for 2018*

A lot has changed in a short amount of time in the defence industry. Next-generation equipment, such as the HMS Queen Elizabeth aircraft carrier and the F-35 Joint Strike Fighter, is growing in scale and complexity, requiring new and intensive support methods to keep them operationally available. For instance, the autonomic logistics information systems (ALIS) onboard the F-35 is the first tactical aviation system to have sustainment and maintenance systems installed for efficiency and cost effectiveness.

Meanwhile, changing attitudes to defence spending in terms of GDP have also lead to slowing expenditure in the West, especially in the UK and US, but a sharp increase in spending in the Middle and Far East – both China and the UAE have more than doubled their defence spending over the past 10 years.

Alongside this, new frontiers are arising. There has been a continued increase in the number of cyber attacks across the world. Cyber threats are becoming more frequent, sophisticated and damaging, and defence forces will need to ensure they are prepared to defend networks and operations against threats, which could land from around the world at a moment's notice.

Military organisations are having to constantly stay on top of technical, tactical and political developments happening in the defence sector. Moving in-sync with advances in all three can be the difference between fielding an effective fighting force or being caught out. All military stakeholders, from department officials to equipment manufacturers and in-service support providers, will need to watch out for and respond to movements on these three fronts in 2018.

TECHNICAL CONCERNS

Due to overarching constraints around security, slow government investment and natural conservatism, the defence industry has traditionally lagged in the adoption of IT developments. The cloud is the latest being debated for military use, which comes with its own concerns over cyber security, data assurance and export controls.

Cyber security and data assurance are closely linked.

PROCUREMENT WILL MOVE TOWARDS AN INCREASINGLY COMPLICATED MODEL

Due to the sensitivity of military information, defence organisations and defence departments are wary of critical data stored in the cloud being accessed by unauthorised personnel. Can its safety be guaranteed if it is held on a server owned by a commercial company?

On top of these concerns is the issue of export control and how organisations navigate frameworks and rulesets that they are bound by in the countries they operate in. According to Tech UK, export control not only applies to export of physical goods, "but also of software or technology by any means including the key point relevant to cloud computing – giving access to software or technology in electronic form to someone overseas".

The US Military has been working on refining its cloud strategy to address information assurance and security concerns. In 2017, IBM announced it was working with the US Army to build and manage a secure private cloud data centre. The DoD has also begun discussions with commercial information technology leaders around updating the rulebook that's governed its security demands for firms that have provided it with cloud computing services.

In 2018, I expect to see more defence organisations follow the lead of the US DoD and look to the quick implementation, efficiencies and lean principles the cloud offers. This will be contextualised by the individual requirements of each organisation. Organisations must find a solution that allows them to operate and adhere to country-specific frameworks and decide whether a commercial or private cloud offering will be able to provide the appropriate level of security.

TACTICAL DECISIONS

In recent years, mature defence forces have been moving from either the traditional 'buy an asset and lots of spares' model or repairs done by the Original Equipment Manufacturer (OEM) model, toward an end goal of contracting for capability with assets delivered on a service basis. In this scenario, the OEM owns and maintains the asset and the organisation pays via a lease model.

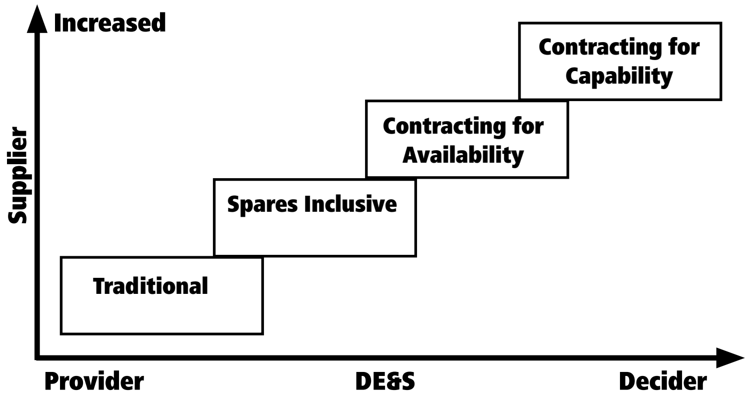
There are several factors that explain this transformation, including changes in defence and security policies, reductions in defence expenditure, and participation in peace support operations. Alongside these, IT developments such as health usage monitoring systems (HUMS) and the autonomic logistics information system (ALIS) have revolutionised asset management and – at least in industry environments – servitisation models have shown huge efficiency improvements.

Moving from a traditional model to contracting for capability has not been framed as a one-step process. The UK MoD sets out a 'transformational' staircase model, which includes four steps: traditional, spares inclusive, contracting for availability, and contracting for capability (see diagram, below left).

Contracting for availability is the third step on the transformational staircase. The defence organisation owns the asset and the OEM or in-service support provider guarantees the asset is available. But the question many organisations may come to ask as they begin new projects and renew agreements in 2018 is if this model is a viable option.

Both axes on the staircase graph are about sharing risk between support provider and the defence organisation. At the bottom of the staircase, the risk is mostly placed on the defence organisation, which can quickly become unsustainable given the high cost and complexity of next-generation assets such as the F-35 or the HMS Queen Elizabeth.

It is in the best interest of military decision makers to push risk as far as possible to the OEM or in-service support provider – meaning assets are always ready for operations without using military resources to keep them that way. Contracting for availability becomes a potential halfway house, with substantial risk still being placed on the military. This is hardly an ideal situation for a military officer who needs his force to be mission-ready at all times – how this is achieved should be the concern of support providers.



▶

We are witnessing this rising trend among our own defence customers and expect to see a steady progression to new models as programmes are put in place and contracts renewed during 2018.

POLITICAL DEVELOPMENTS

One aspect out of the defence industry's control is the triangular dynamic between the US, NATO and the EU. The last two decades have seen a period of stability between the three. Most of the world uses NATO common standards at present, but changes are taking place in the Northern hemisphere, which will have knock-on effects to defence forces, OEMs and in-service support providers on a global scale.

There were high-profile recommendations from the US on NATO member defence spending in 2017, and there have been notable new equipment strategy changes from the UK and the European Union. BAE Systems signed an agreement with Turkey Aerospace Industries to collaborate on a development programme for the TAI TFX, a new twin-engine aerial superiority jet, set to be introduced in 2023.

With the UK forging its own path as a dominant European defence power after Brexit, other European defence powers are looking to collaborate with each other. In the summer of 2017, France and Germany announced plans to work together on a project to produce unmanned fighter jets that will eventually replace French-made Rafale Jets and the Eurofighter Typhoon.

Defence organisations will decide which equipment best fits their strategic requirements, while in-service support providers will realise the need to stay competitive by providing services that help new, often unexpected partnerships. The support of IT systems designed to cope with this change and adapt to multi-stakeholder environments becomes even more important.

The buying map in the defence industry is clearly shifting. As NATO spending continues to divide opinion and new equipment development programmes evolve through 2018 and the following years, procurement and support will move towards a different, and increasingly complicated model.

Military decision makers must make choices throughout the year ahead that will directly affect their fighting force. More organisations will consider the cloud as a viable option as cyber security fears are eased. The industry that has so far lagged behind its commercial counterpart will no doubt be looking closely at developments in and adoption of cloud technology throughout the year, but only within the parameters and frameworks set out by each country they operate in.

> I EXPECT TO SEE MORE DEFENCE ORGANISATIONS LOOK TO THE EFFICIENCIES THAT THE CLOUD OFFERS

The procurement of equipment and maintaining it via the right support model will see firm developments as it starts to effect mission success. IT developments have helped transform this, and the promise of reducing risk on the operator will open up significant opportunities and benefits for both sides. As new and unexpected partnerships emerge and contractors adapt to an ever-changing political landscape, the support of IT systems will be elevated from a transactional tool to a strategic enabler to help military, contractors and suppliers function more efficiently ●

Evan Butler-Jones is Director, Defence Product Line, Aviation & Defence Business Unit at IFS and is responsible for ensuring that products and services meet the needs of defence customers around the globe.

The risk between support provider and defence organisation must be shared more equally

Picture credit: IFS