

# Are we doing enough to **derisk** the defence supply chain?



**D**efence ministries and major contractors would be at a loose end without vast global supply chains to provide the equipment needed to undertake operations in a timely, cost-effective manner. However, as these chains add more links, the complexity of managing them has steadily increased, while the risk of a single vulnerability – and its potential to disrupt – becomes inevitably more severe.

A critical supplier may suffer financial failure or be found in violation of labour or environmental standards. Just as worrying, foreign infiltration into critical systems for the purposes of disruption is becoming a significant concern given recent attitudes towards cyber and corporate espionage. It is therefore vital that governments and agencies do what they can to better understand the risks and press contractors for transparency and accountability.

**‘In a six month period, 40% of deliveries were a month or more overdue, demanding emergency expenditure on commercial air freight services’**

## The ‘good’ news

As with most western states, there is some respite for the British Government in that there is currently no major ground conflict requiring British land forces. Aside to deterrent/support deployments to Eastern Europe and peacetime operations, the risk to the lives of personnel is minimal. However, this situation could of course change at any time, and recent inefficiencies should serve as a warning.

During intense operations in Afghanistan and Libya, the UK was met with [fears](#) that its supply chain of equipment to the frontline was at a serious risk of ‘critical failure’ and could result in shortages of essentials within weeks. This anxiety reportedly stemmed from a delay in securing the appropriate tracking system and had seen the military forced to stockpile equipment in the event of such a shortage – which in itself drained life out of the budgets.

In that situation, a Commons public accounts committee released a report that had found in a six month period, 40% of deliveries were a month or more overdue, occasionally demanding emergency expenditure (totalling £347 million) on commercial air freight services alone. At the time, the government played down the severity of the report, claiming that it in the midst of supplying to a conflict zone, it had placed greater demands on the industry to meet its delivery schedules and for the MoD to reform with emphasis on cost control. →

### The 'not so good' reality today

Years after the withdrawal from Afghanistan, the UK Government found itself in another costly quandary, with a 2015 report [emerging](#) from the Policy Institute of King's College, London, suggesting that a lack of official data on the value of the UK defence industry to the economy could lead to 'substandard' procurement choices. The aim of the report was to examine how a domestic defence industry underpins the country's security and whether, as in most other countries, its contribution to the wider economy should be assessed in how it selects its equipment and its business partners.

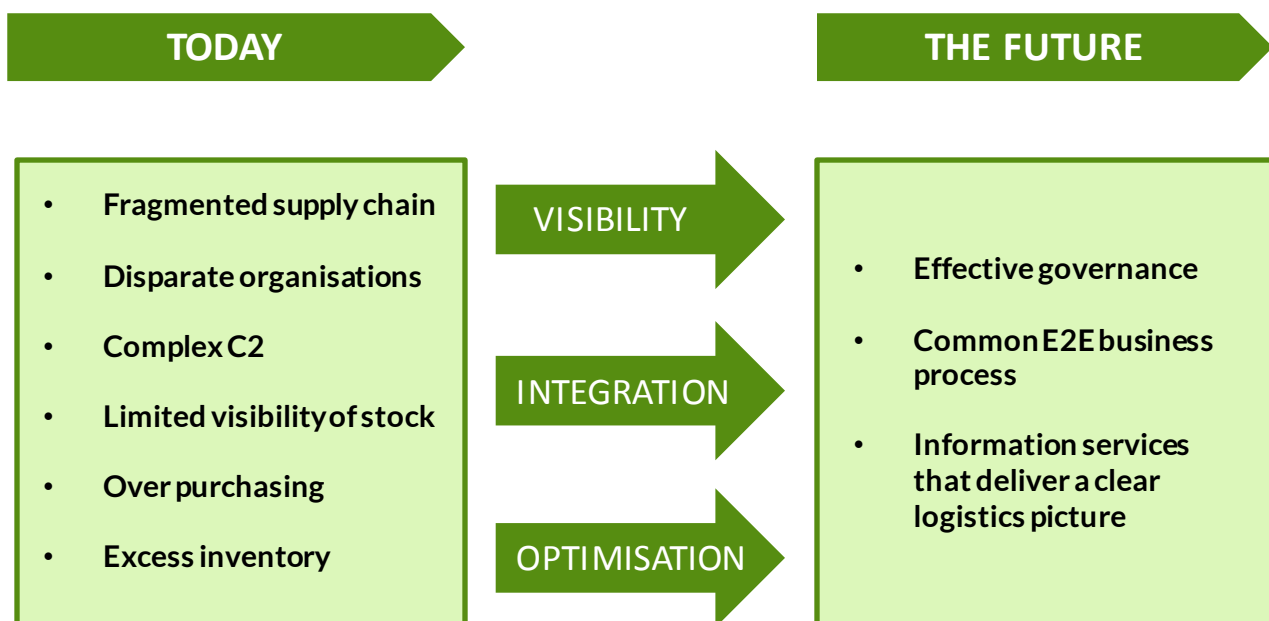
The critique came amid concerns in the industry and the armed forces that an already constrained defence budget would be stricken worse by further cuts, particularly as geopolitical tensions appeared to be on the rise. It is impossible for the MoD to afford to source all its equipment domestically, but criticism was levelled at claims that purchasing decisions – alongside those relating directly to logistical supply chain – were being made in a 'data vacuum', potentially putting operations in jeopardy. The apparent solution to this was to make efforts to improve both the robustness and the flexibility of the supply chain in tandem.



### Digital anxieties

New dimensions to the supply chain include the increasing use of digital solutions and the new pressures this places on logistics and procurement decisions. The MoD cannot lock away information entirely and hope to have efficient process – there must be room for information sharing that can be stored and transferred by digital means. Yet, this means security along the supply chain needs stronger oversight than ever.

Likewise, with a booming cyber industry ready to meet a booming demand for cyber solutions for military and government, there is undoubtedly strong opportunity for business, but equally, there is significant chance of budget holders making hasty decisions based on limited evidence of reliability, and perhaps even being seduced by a plethora of promises some businesses make (the type insiders have been known to refer to derisively as 'magic box' solutions). →



***Wider MoD supply chain concerns and three proposed improvements that can aid transformation, as suggested by the Assistant Chief of Defence Staff (Logistic Operations)***

As of 2016, all suppliers bidding for new MOD requirements which include the transfer of 'MOD identifiable information' must first achieve a Cyber Essentials Scheme (CES) certificate by the contract start date and some suppliers to ensure additional cyber security controls beyond that. The Defence Cyber Protection Partnership (DCPP) is a joint MOD/Industry initiative tasked with improving the protection of the defence supply chain from the cyber threat. Alongside MOD, the Partnership consists of defence primes; SME trade associations and other governmental departments. The DCPP model undertakes new risk assessments that rank companies on a 1-5 scale. Based on the outcome, specific cyber protection measures can then be issued to fit the category.

### A transatlantic concern

Naturally, derisking the supply chain is not a uniquely British problem. The United States Department of Defense is acutely aware of the need to improve efficiency and security, issuing [a new rule](#) to the Defense Federal Acquisition Regulation Supplement (DFARS) this year that clarifies the scope of Washington's ability to evaluate and exclude contractors that may represent supply chain risk, primarily where it pertains to IT systems, services and software used for national security programmes. This would include the likes of sabotage and subversion (such as by an adversary, a foreign state or an opportunistic insider), which was confirmed to have been a [real threat](#) in recent years. ➔

Under Section 806, action to preclude can be approved by high-ranking officials, such as the secretaries of the military departments or the most senior procurement officials within those departments, where written notice is provided to congressional defence and intelligence committees and other agencies responsible for procurement of similarly risk-prone assets.

The rule also requires that contractors commit to mitigate supply chain risk and consider the action of imposing government consent for all subcontractors in addition to thoroughly documenting all processes undertaken to vet those third parties.

Problematically, while the new ruling will assess contracts on a case-by-case basis, analysts are concerned that contractors are not safeguarded with appropriate procedural protections from being unfairly disqualified from DoD business should assessment or oversight be

flawed. This could be frustrating for many businesses as the DoD is often restricted from communication with contractors, leaving some doors to explanation, clarification or appeal all but closed from the offset.

Until DFARS releases further guidance on how contractors (and subcontractors) should be vetted, or until this rule is reviewed for assessment itself, it remains unclear what impact this development will have on overall risk levels to Pentagon procurement.

Meanwhile, DFARS has also issued a new ruling for DoD contractors to adhere to cyber incident reporting requirements, which broadens previous rules and clauses by encompassing all agreements from “contracts, grants, cooperative agreements, other transaction agreements, technology investment agreements, and any other type of legal instrument or agreement”. →



**‘Analysts are concerned that contractors are not safeguarded with appropriate procedural protections from being unfairly disqualified from DoD business’**

## Wider issues

US actions to advance its oversight of the supply chain come at a time when opportunities for DoD contract work continue to [prove strong](#) in spite of an ongoing downturn in demand for weapon systems. In October, the nation's biggest contractors reported positive third-quarter results, with sales and earnings widespread and strong projections continuing for the near future. Analysts have said that the thriving nature of the industry today can be pinned on a number of factors including major cost-cutting, share buy-backs and low-interest rate policies.

But again, much of this growth remains reliant on effective supply chain management and continued efforts to ensure nothing falls through the gaps. Where anxiety arises is in a reliance on outside control, particularly in the abundance of manufacturing and supply from

overseas. A report in 2013 from the Alliance for American Manufacturing [highlighted](#) the fact that some defence platforms could be derailed and operations severely hampered if single-source supply suddenly fails.

As one example, it was found that, due to the product being discontinued domestically, the US relied solely on one Chinese company for its buta-netriol (BT) needed to produce solid rocket fuel for Hellfire air-to-ground missiles, used across multiple airborne assets. Reliance on sole providers is one matter – the other is in the reliability of sourcing from potentially unpredictable nations or those that may be prone to political disagreement. However, there is strong argument that without the use of these providers, it would not be possible for the Pentagon to afford the variance and volume of its procurement needs. →




**‘Reliance on sole providers is one matter – the other is in the reliability of sourcing from potentially unpredictable nations’**

**Knowledge + Networking = Simply Less Risk**

Clearly there are significant questions that must be asked of governments and of all companies involved in defence supply chains today. Equally, there can be no room for miscommunication or a lack of dialogue. If these are issues close in your wheelhouse, *Defence IQ* encourages you to attend the International Defence Logistics conference (February, 2017; Brussels, Belgium) so that you can arm yourself with the latest knowledge and methodology to approach any future



changes to supply chain management by meeting the experts in this field.

The forum will include opportunity to network with the likes of the Director of Logistics Delivery Operating Centre at Defence Equipment and Support (UK MoD) and the Assistant Chief of Defence Staff (Logistics Operations), as well as with senior defence logistics representatives from across the world, including the US, Norway, Germany and Jordan. The full agenda can be downloaded from the [conference website](#). 



## Australian DoD awards supply chain contract to Rheinmetall

Rheinmetall Defence Australia signed an agreement with the Australian Department of Defence (DoD) on 20 October 2016, committing the company to assisting local industry in gaining access to the Rheinmetall group's international supply network.

Christopher Pyne, Defence Industry Minister, said the global supply chain agreement will provide Australian defence companies with opportunities to enter Rheinmetall's subcontracting network as well as "help break down barriers that may otherwise deter local firms from doing business in overseas markets".

The deal makes Rheinmetall the seventh international corporation to enter a global supply chain agreement with the nation's Defence Department. Other companies include BAE Systems, Boeing, Lockheed Martin, Northrop Grumman Raytheon, and Thales.

Source: [IHS Jane's](#)

## SAIC receives \$1.4bn US DLA deal

Science Applications International (SAIC) has received a \$1.4bn logistics and supply-chain-management services contract from the US Defense Logistics Agency (DLA).

Under the contract, the company will provide chemicals, packaged petroleum, oils and lubricants to the US Army, Navy, Air Force, Marine Corps, federal civilian agencies and foreign military sales customers.

The indefinite-quantity contract has a five-year base period of performance, one three-year option, and one two-year option.

SAIC Department of Defense Agencies and Commands Customer Group general manager and senior vice-president said: "SAIC has supported DLA with multiple logistics and supply chain solutions for more than 30 years in their mission to provide products and services to American troops and others to accomplish their missions.

"We are proud to continue these critical services to DLA for the next decade under this contract." DLA manages logistics on behalf of all US military branches and federal civilian agencies. The agency supports more than 2,300 weapon systems and provides a range of logistics, acquisition and technical services.

With more than 25,000 civilian and military employees, DLA operates in 48 US states and 28 countries. In the past decade, SAIC has delivered more than 42 million packaged petroleum products, oils, lubricants, and chemicals to DLA's customers worldwide.

Source: [Army-Technology](#)

## SEKO joins JOSCAR ranks

SEKO Logistics has earned a place on the Joint Supply Chain Accreditation Register (JOSCAR), which enables companies in the Aerospace, Defence, Security & Space sectors to identify qualified suppliers.

ADS has formed a Governance group of buying organisations and representatives from the supplier community to work with Hellios Information, the third party service provider, to develop and administer JOSCAR. ADS Group promotes the importance of the four sectors to the UK economy and works to create an environment that allows its members to invest in productivity, exports and growth.

Aerospace, defence, security and space currently generate over £50 billion of revenue a year for the UK economy.

ADS says JOSCAR demonstrates to clients and other stakeholders that a supplier is 'fit for business'. The Register holds common supplier data in a central system that can be accessed by all participating buying organisations, saving time, cost and resources.

For SEKO Logistics, the accreditation reduces the processes associated with pre-qualification, assurance and ongoing compliance, and will provide easier access to business opportunities. Attaining JOSCAR status has meant that customers can have confidence knowing SEKO Logistics have passed this stringent process.

Source: [ADS](#)



# INTERNATIONAL DEFENCE LOGISTICS

21st - 23rd February 2017  
Brussels, Belgium

## Optimising logistics in the age of rapid deployment

The procurement, transport and replacement of military supplies continue to pose considerable challenges for logisticians. Today's operations demand a lighter, more efficient supply chain, with the capacity to deliver resources to isolated theatres at speed. February's conference will be an invaluable opportunity for military and industry alike to confront the difficulties of logistics supply in the post-Afghanistan era. With no major theatres of war ongoing, the event will consider the demands of a return to contingency, examining the need to develop a logistical framework suitably robust to deal with rapid deployment, and suitably uniform to encompass joint international efforts.

### By Attending Defence Logistics 2017 you will have the opportunity to:

- Leverage long-term relationships with industry to simplify the supply chain and to discover how outsourcing the logistical process to a third party can deliver on a product, service or programme more effectively in support of contingency operations
- 
- Examine the sophisticated programmes that allow you - the logistician- to better manage your assets and their availability by integrating the supply chain at the joint operational level
- 
- Improve your ability to deliver assets and equipment to hard-to-reach conflict zones by sourcing partnerships with other infrastructure owners
- 
- Benefit from avenues of outsourcing that can reduce the supply chain burden so that you can concentrate on sustaining the equipment or technology itself and supply your product or service reliably to the user

[www.defencelogisticsevent.com](http://www.defencelogisticsevent.com)

Tel: +44 (0) 20 7368 9737

Email: [enquire@defenceiq.com](mailto:enquire@defenceiq.com)