The Chartered Institute of Logistics and Transport

Second Defence Logistics Master Class

30th April 2014

A paper to capture the thought leadership demonstrated during the event

Stronger Together

Supply Chain | Transport Planning | Rail | Active Travel & Travel Planning | Bus & Coach | Ports Maritime Waterways | Freight Forwarding | Aviation

The Chartered Institute of Logistics and Transport

Addressing delegates at the master class (top to bottom): Sir Brian Burridge; AVM Graham Howard; Chris Markey FCILT

Event context

Whilst the title of the event was: *Logistics Information Systems in a New Defence Era*, the master class discussion ranged far beyond the bounds of Log IS[1], and highlighted some fundamental issues that are worth further investigation, research and action in order to meet the challenges that the new defence era is offering. It looked at three specific areas of interest: developing intelligent customer capability; managing support chain partners in the Defence Support Network (DSN); and managing the extended defence supply chain risk that realising the DSN might bring. These areas are looked at individually in subsections of this paper and could be considered separately. However, it will be seen there are some themes that run throughout each section, and consideration of these will be more effective if a wider perspective is taken.

This paper draws on the presentations and discussions that took place during the master class. Where additional material was provided by speakers and delegates, this is also considered. However, to comply with the Chatham House rules that were agreed for the event, attribution has not been made unless the originators have specifically requested it.

Information systems: business context

Business drivers of information systems

There is a generally agreed list of the business drivers in information systems, all of which can be identified at the defence/industry interface. The first two are closely aligned and could be considered as one: globalisation of the economy, and the rapid advance and use of e-commerce. There is an uneasy tension between the next two sets of drivers: security and privacy, and collaboration and partnership. The ability to build relationships across the supplier-customer borders is greatly enhanced by shared data and information, but keeping sensitive information within the bounds of that relationship, and building sufficient trust and understanding to share enough data to enable innovation are challenges. These drivers could be considered as base drivers that shape the environment within which the IS must operate. The next three drivers could be seen as shaping how business is actually done, and are key to highlighting the opportunities that management of information can offer. Prime amongst these is knowledge and asset management, which is vital for defence and its contractors. This introductory piece will look further at some examples of how this is handled in some current integrated support contracts. Equally important, but not covered in depth during the master class, were the final drivers of continuous improvement and business process redesign – potentially a topic for a further event.

External drivers of defence information systems

Taking these business drivers and applying them to the public sector, we see there are significant external environmental drivers that will have an impact on Log IS. Government departments have a legacy background of policy formulation, but this has developed into a role of implementation and delivery of high-quality public services. The MoD has always aspired to have a command role and, despite new ways of working and the effective rustication of the Chiefs of Staff, it arguably has much more influence on operational and even tactical operations than it used to. As a department of state, it has to contend with a politically savvy and vocal public, a cynical media corps and social media acting as an accelerator for perceptions and emotions. All of this is combined with a difficult financial climate. Defence therefore needs to have high levels of confidentiality within its systems and processes.

Mutual trust must, however, be generated and maintained across the defence/industry partnership in order to manage the challenges these environmental factors give to the business drivers at each side and across their interfaces. In terms of logistics information, this trust is borne out of consistency, accuracy, transparency, cost-effectiveness and innovation. Innovation is a major driver that will be further explored below.

Challenging issues for defence logistic information systems

Given the external, environmental and business drivers of Log IS, the following issues can be seen to be key to the successful partnering of defence and industry.

The human dimension

In relative terms, the arrival of the first PC-based word processors in the MoD was not that long ago. Serving officers can remember when they had to send their typing to Glasgow or Brighton in the late 1980s, and so acceptance of office automation, soon followed by early intranet communications, was generally welcomed. As the home PC with its Windows operating system became ubiquitous, consumer expectations vastly increased and acceptance of the necessary security requirements in public sector systems hardened enormously. Managing expectations in today's connected world is at least an order of magnitude more challenging.[2] Translating these expectations across to defence logistics, if we look at each of the aspects of consistency, accuracy, transparency, cost-effectiveness, and innovation in political, policy, operational and industrial context, then we begin to get a feel for the challenges that both defence and industry face. As we shall see, the human dimension reaches across and heavily influences each of the specific themes the master class addressed.

Cost-effectiveness: cost and performance

Defence has embarked on a major ICT transformation encapsulated in the Defence Core Network Services Programme. The programme mission is that, by 2020, there will be a greatly improved user experience through enterprise-wide, end-to-end MoD ICT services delivered at the cost and agility of industry best practice. The lifetime cost is an eye-watering £5.5 billion. Defence has, however, arguably learned from the costly mistakes made with previous large ICT programmes in that it recognises that a migration to market-standard commercial ICT should reduce cost, complexity and rollout time.

Essentially, the programme is a multi-vendor model across the whole spectrum from a mobile phone to a satellite, but competitively contracted in smaller packages for shorter periods. This has the virtue of acting as a brake in the throwing of good money after bad that has beset so many public sector ICT projects. It also opens the marketplace to innovative SMEs, and we will look at some of the factors that enhance and constrain innovation.

The human dimension above has an intimate effect on the success of these projects. Turbulence within defence and industry (the transfer of projects between DE&S and Joint Forces Command overlaid on the usual rotation of staff and SMEs in defence, and mergers and acquisitions in industry having a similar effect) are a contributory factor to recent poor performance with some areas of these projects. The drivers here are self-evident, with cost being at the forefront, but with alignment with commercial standards coming a close second.

Innovative approaches

Defence has often been accused of procuring yesterday's technology tomorrow, at the day after tomorrow's prices. Industry has called for early consultation from the public sector on complex procurement projects for decades, no more so than from the aerospace and defence sector. The MoD is one of the most sophisticated departmental customers, and has demonstrably improved in this area in recent years with Niteworks and Bluelightworks. Such collaboration may seem to be at odds with the principles of open competition, but have helped the public sector in areas such as: assessing the realism of the requirement; understanding the art of the possible; recognising what has been done before; understanding where COTS applies; in the case of the MoD generally understanding export potential; most importantly, stimulating rather than attenuating innovation.

Consistency and accuracy: turning ambition into reality

Commanders have had challenging experiences using ICT during military campaigns, notably in Iraq and Afghanistan. The current challenge (in 2014) is the redeployment from Afghanistan.[3] A major defence support programme for a front-line aerospace platform will be used as an example to demonstrate where industry engagement was also subject to significant constraints from existing Defence Log IS.

Back in 2003/04, when an industrial imperative to implement availability contracting was starting, the MoD Support IT landscape was fragmented, disparate and had no clear ownership. Key systems were often bespoke, standalone and developed locally with no formal support infrastructure. These systems often only surfaced during the due-diligence process – and sometimes later. This architecture was unable to produce coherent data, and it took significant investment by industry to reconcile the data to make information usable in a Contractor Logistic Support (CLS) environment. Most significant was the lack of understanding that industry was now a customer of the MoD. In other words, the MoD had become a key supplier of data necessary to enable a CLS environment.

Industry had a requirement to use the RAF's legacy Unit Supply and Accounting System (USAS) in the aerospace environment, but could not get hold of the specifications in order to build interfaces; nor could it find the right person within the MoD to provide access to the subject matter experts to discuss functionality. User training was available, but largely only up to competent operator level. Industry needed to get to the level of super-user understanding to design its own systems and processes. That level of knowledge on the MoD's systems was difficult to find and access.

Collectively, we were applying pressure on the MoD to provide additional data and functionality. That prompted the formation of an agreement (via MoU and NDA) between BAES, R-R and AWL which later expanded into the Green Box today and that, jointly with the emerging LogNEC programme, developed an integrated set of industry logistics data requirements. This combined schedule was used to de-conflict the individual requirements of multiple demands from industry to the single and overworked community within the MoD, which was not resourced to handle the onslaught of industry demands on its time. In summary, 10 years ago, within the information space, the MoD needed to recognise that it had become was a data user, a data provider and a data decider.

The Front Line Commands now use a single system to log hours and aircraft availability (Aircraft Serviceability Record (ASR)) and the discipline of data entry on to that system is becoming consistent and meaningful, not only reputationally critical to industry for assessing the fleet health and performance at the forward level of maintenance, but also in that the achievement of flying hours and sortie completion is a key performance indicator that drives the IOS payment mechanism. As for the future, the development and evolution of CLS and IOS programmes across the defence platform base is now taking some interesting turns. As industry develop support models that best suit its operational models, particularly as the international markets start to demand output based contracts, as the pace towards delivering capability quickens, and as the boundaries between industry and end-user become optimised, the requirements for data and information across CLS industry players may be diverging. The MoD and industry need to be able to respond and adapt to this changing environment. The one certainty is that this evolution will not stop, and the pace of change is liable to increase in future.

Cyber security

The biggest challenge to successful partnering in the digital space is probably cyber security. This was mentioned in passing, but not explored in detail during the master class. Significant work is going on with the Defence Cyber Protection Partnership, a group of major MoD suppliers, along with the Department for Business, Innovation and Skills (BIS), MoD, the Centre for the Protection of National Infrastructure (CPNI) and the UK National Technical Authority for Information Assurance *(CESG, part of GCHQ)*.

Defence context

At the time of the master class, defence continued to work its way through turbulent waters. Operationally, the Department was focused on completing the transition of security responsibilities in Afghanistan to the Afghan National Security Forces (ANSF), and the redeployment of UK forces from the theatre. At the same time, it was adjusting its posture from direct support to a decade of high-intensity expeditionary operations to generate and deliver a joint expeditionary force that is properly enabled, trained and resourced to succeed on contingent operations.

Moving away from enforced and sometimes ad hoc coalitions of the willing, the UK was re-engaging with more structured alliances in NATO and the UK/French Combined Joint Expeditionary Force. It was engaged in delivering the Defence Transformation Programme, and moving towards the longer term establishment of defence authorities. Closer at hand was preparation for the 2015 Strategic Defence and Security Review, which was always likely to change priorities and resource allocations.

Notwithstanding these uncertainties, the defence logistic priorities were to deliver the Whole Force. In practical terms, this means that by 2017, over 70% of all platform support solutions will be delivered through contractor-led arrangements. There would be increased provision of hard and soft facilities management by contractors, and increased numbers of contractors deployed on operations. Turning to corporate processes, one of the greatest immediate challenges was to align Log IS with financial systems, and this was encapsulated in an overarching, Government-wide Policy Transformation to provide simpler, clearer and faster process and results using Log IS.

Defence support capability would, therefore, be delivered through a Defence Support Network – see Figure 1 – comprising the Whole Force, and the Defence Support Chain reaching from suppliers through the strategic base to deployed forces. Log IS would have to enable and support the Defence Support Network across the whole spectrum of likely operational and threat scenarios.

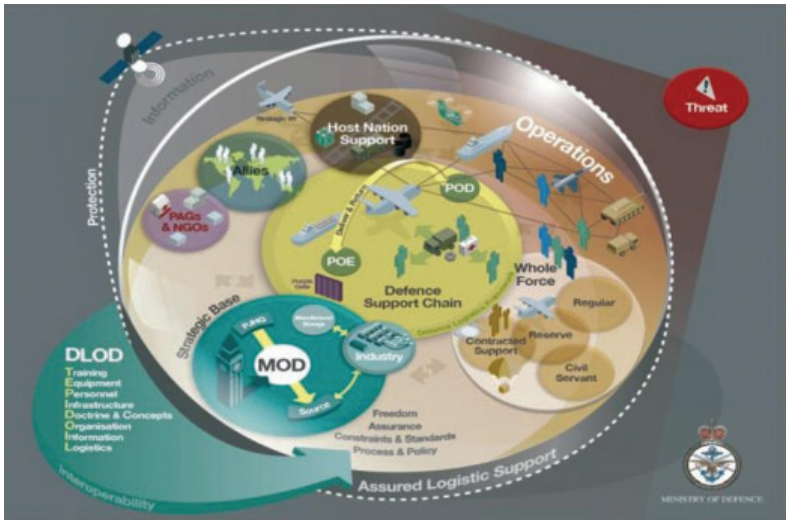

Figure 1: Defence Support Network

Theme 1: Intelligent customer capability

The master class looked at the challenge of how defence can maintain (or perhaps that should be grow) intelligent customer capability against the background of these tectonic shifts in the delivery of support capability. There was a general consensus that the whole defence community should be building inherent customer intelligence by giving military logisticians more professional credibility and through-life development. One way of doing this would be to expose practitioners to cross-sector best practice at a much earlier point in their professional development. It was not clear, however, how defence can capture, articulate, understand and demonstrate the value of professionalisation. This might provide fertile ground for further research and development.

Professional credibility and development

Professional logistics training existed within UK defence and a growth path was now defined for officers and NCOs. A route to MSc level now existed on top of vocational development. The nature of the relationship across the military/private sector boundary needed to be better understood; the military still did not understand the civilian perspective. One retired senior officer highlighted that had he understood the industry perspective while in the military, he would have behaved differently in senior defence logistic roles. The German Armed Forces had set up a unified logistics school 12 years ago, managing to harmonise single service requirements. Officer/NCO training was believed to be good, but more focus on lifelong learning was required. A major problem with the traditional career structure was that it did not recognise non-command specialists; better incentives were required for those with more technical and professional skills or the services would lose people and, more importantly, their hard-earned skills. The military needed software engineers, as well as company and brigade commanders, but there needed to be a reward system in place to recognise their value. Currently, in the UK, the only way individuals can be rewarded is by promotion to higher rank, and this is tied too rigidly to command positions. Industry, in contrast, promoted within specialisation after long periods in post; defence needed to consider the same but how this was achieved in a military hierarchy was unclear. More collaboration was needed between defence and wider commercial logistics, personnel and reserve staffs to consider this issue.

There was a perception that the logistics profession is not taken seriously enough at senior levels in defence and is often regarded as secondary and too specialist. This is reflected to a lesser extent in the commercial sector, but the value that logistics professionals bring to business is being recognised up to board level by more successful enterprises. There was too much wastage of skills and talent with people leaving defence for the private sector, and lack of recognition and being valued may be one of the drivers of this exodus. Professional development was also needed and while military engagement with CILT was reasonable, more effort was needed to generate engagement from younger personnel with their professional body.

The lack of intelligent customer and wider professional logistic skills should be mitigated where possible by proactively and systematically seeking out and using the professional skills of reservists, who will make up an increasing proportion of the Whole Force.

Defence/industry placement

Could private sector placements be a solution? More engagement was required, but placement needed to be part of in-service training for more junior staff rather than an exit route from the military. Professional engagement with wider commercial best practice was needed for younger personnel, and while this can be gained through CILT activity, a more formal model was also needed including placement and mentoring. Germany, which had a mature industry placement programme, believed it was a valuable facility for growing customer intelligence, but needed a

significant long-term commitment from the highest levels. Military personnel needed to be kept in industry posts for greater lengths – up to three years for officers and potentially nine years for NCOs – and oversight of contractor activity was important. Personnel did not have to stay in one job for this entire period, but needed to move in and out consistently and be able to get promoted. Currently, good opportunities existed in the NATO support agencies for military personnel, but were underused. If working with consultants, defence needed to define closely the outcomes and desired paths for contracted work, and this should include greater engagement with their military counterparts.

Defence training was perceived by some in UK industry not to be fast enough for the modern world. Industry's view was that personnel exchanges were vital and needed in greater volume. Industry in general would benefit from military expertise, from SNCO upwards, perhaps at a 2:10 ratio with other tours for logisticians to bring commercial expertise into the military. Industry needed to support this by mentoring of personnel and opening up real jobs, rather than just observer slots. This could form part of CLS/IOS contract requirements.

Earned value of the support chain

Whilst defence logistic training was seen by many to be outstanding, the support chain seemed to have been gradually and incrementally dismantled without an overarching plan. This may have been because defence may once have been on a holistic path, considering an end-to-end perspective, but that was now derailed, with a largely unregulated transfer of capability to the private sector. Defence needs to understand the earned value of the support chain and as a result struggles to generate business cases that justify retaining and developing in-house support chain functions in the face of criticism from external consultants. Defence needed a clear view on what the end-to-end chain needed to deliver and understand its earned value. In order to achieve this, it first has to implement systems to capture that value. This capture is the critical missing element. To be an intelligent customer, defence therefore needs to understand the earned value of its support chain

Managing supply chain risk: speakers at the Defence Master Class

Keeping pace with transformation

The pace of defence transformation was recognised, but there was a danger that the logistic element would not keep pace with it unless there was a coherent structure and plan underpinning the outsourcing of support capability, and the maintenance of the components that enable an intelligent customer. It was mooted that unless intelligent planning for military personnel existed, maintaining pace and vision would be difficult, and in this respect, three-year roulements of key officers were frustrating. The Supply Chain Blueprint had identified the requirement for a tri-service model, but the subsequent loss of the JSC blueprint illustrated the problem of sustaining coherent change. Defence was at its worst here in maintaining consistency of its aims. There were too many personal agendas diverting the department from its original aims, and this was a fundamental issue. Conversely, individuals who tried to stay the course and remain in one place or specialist role too long had their careers blighted.

Defence and industry needed to work together positively to understand the business landscape and use of terminology – but must avoid speaking different languages. Private sector partnership, including using partners to provide leadership and acting as a repository for source knowledge, could be part of the solution for coherency. These factors and options need to be considered in a focused piece of work that could identify a structure and plan to create intelligent customer capability, and offer proposals to identify ways to change training, culture, systems and people to enable that plan.

Theme 2: Managing performance in the Defence Support Network

The second part of the master class discussed whether defence and industry could bring to the table successful approaches to enabling joint enterprise. This discussion was focused on partnership-based contracting and intelligent business operations. But what is the definition of a collaborative contract? Is it just a standard contract with just more terms and conditions? The use of information technology to drive efficiency in contractor logistics support programmes has always been at the front of defence requirements, whether that is using the latest platform technology, taking the systems out into operations or collaborating with users and vendors over data to drive improvements. The master class looked at some examples of how commercial enterprises working in partnership (a Middle Eastern airline is outlined below) have contracted complex maintenance, infrastructure and information solutions, and key to their success was they were delivered in extremely short order.

It was suggested that software and information systems are no longer the challenge to such contracts because there are strong IS solutions available. The greatest challenges came from business change, process and governance, the contracting approaches to enable them, and the ability to change with intelligent business operations.

The biggest contracting mistake government departments make is being overly reliant on strict methodologies – for example, PRINCE. To try to define to a set of backed-off user requirements is expensive and complex and agreements then need iterative management over years, sometimes driving programmes off course. However, agile incremental development of requirements is deemed to be too risky and is unlikely to be accepted by traditionalist defence commercial staffs, who are bound by public sector regulation. Looser framework arrangements are therefore vital to achieving successful early project implementation. Such agile management is dependent on several factors:

- Can the business provide a single, high-level requirements focus?
- Can the parties contract flexibly in order to release joint innovation at minimum bureaucratic costs?
- Can they work together within a joint information enterprise reliably and effectively to deliver long-term IS solutions to the MoD

Intelligent business operations

Defence contracts have changed dramatically since the 1990s, which has shifted the way that industry and customer need to operate together to drive efficiency. The question was asked: *What type of contracts does the MoD think it manages: adversarial, co-operative or collaborative?* On balance, the view was that defence has sought in many cases to build co-operative arrangements, albeit in the past and again now, there are examples of projects that seek true collaboration or partnerships.

Traditional business information (BI) solutions that underpin current PPP/PBL arrangements are typically built from the bottom up, aligned to organisation or function. Day-to-day transactions in the information system are typically designed and implemented before having any understanding of a common strategy, business process or how success is measured. Information systems need to be designed and constructed from the top down, where strategy is directly linked to operations delivering a common process and data performance picture.

Industry best practice often shows software providers working collaboratively to deliver an information capability (IC) from industry as part of a Joint Enterprise partnership. However, MoD has a direct relationship with the system integrator (SI), not the software vendor, and often requirements are passed down second or third hand. This is not the norm outside Western Europe and North America – for example, in the Middle East the software vendor is typically contracted first in a partnership arrangement, and then it subsequently brings the SI into the arrangement to address any complex infrastructure aspects; it places the SI and the software vendor in the position where they can deliver greatest value and accept similar responsibility.

Example: a Middle East airline

An exemplar contract delivery of an IC was discussed. The contract was based on partnership between SI, vendor and customer. A top-down approach was adopted to design, deliver and implement the solution with a common strategy and processes being used by all actors. There was enterprise governance of data and KPIs were delivered before go-live. This enabled effective management decision-making by all of the actors from day 1 and they built a brand new engine plant at the same time. By comparison with defence contracts, the speaker was reminded of the 'Class sketch' from David Frost's satirical show with John Cleese, Ronnie Barker and Ronnie Corbett! Whilst extreme, it underlines the issues of complex projects where the IS provider often only gets third or fourth-hand access to requirements.

In addition to fractured access to requirements, it takes an eternity from 'flash to bang' for defence projects compared to wider industry. Industry would claim new projects should have a flash to bang of 12–14 months, and the huge projects with the Middle East airline above was delivered in 12 months.

There is a legacy landscape for the management of KPIs and management information with defence. The MoD and Industry tend to exhibit lots of good transactional systems operating in stovepipes. There are then typically powerful BI solutions dropped on top and they manage stovepipe information. The BI focus is downward looking and liable to be remote from the organisation's main KPIs and raison d'źtre. This is clearly unnecessarily complex and leads to suboptimal performance. It was advocated that with corporate performance management and integrated business operations you need to build the contract KPIs and the processes into the final solution. This will demand closer and more open relationships between customer, SI and vendor than hitherto, and shared views on KPIs.

Formalise collaboration management

Intelligent business operation solutions balance the roles between customer and provider. The best solutions ensure SLAs are met, but drive joint responsibility for the enterprise. To make PBL a success both sides of a contract need to share and own the same processes, but not necessarily the same performance information. Success is usually exhibited by the delivery of joint processes within a common enterprise.

In the UK defence case, the MoD needs first to understand the relationships between supply chain (SC) components and business functions, and reiterate these for the benefit of all who are working in the collaborative space. Log IS is somewhat isolated in the enterprise, but the impact of logistic data changes is far ranging – for example, upon finance – and this needs to be better understood. The MoD has been criticised as being unable to react to new business requirements, and thus needs clarity and agility in partnering frameworks to be collaborative. Where such arrangements have been attempted, there are instances where fighting over performance monitoring and a lack of patience threatens collaboration. The MoD therefore is seen to seek co-operative relationships, but it is not yet in the collaborative arena. Defence should therefore consider underpinning contracts by international standards to deliver future support services.

Throughout the master class, collaboration was considered in the context of defence/industry relationships. However, on reflection, there is a case for defence to promote, if not demand, inter-industrial partner collaboration in the defence support chain. At a recent debate between commercial supply chain leaders[4], it was highlighted that the competitive edge between products was in the products themselves, not in the supply chains – the customer would decide on the relative merit between brands and quality of service. Joint industry supply chain operations would produce win-win benefits for all concerned through collaboration in sourcing, transport, warehousing and materials handling. This could also read across to Log IS.

Better decision-making

How will data enable better decision-making in the future? What process performance information do we need to make the right decisions, rather than simply focusing on point performance indicators? There are already effective, connected information management systems in operation within the MoD today that are capturing business critical management information; but they are not managing the enterprise, just a silo or unit or function. A single point of truth is important, but a common view of success or failure of an enterprise more so.

There was a common view that defence does not necessarily understand what information it wants and needs to run its business at the enterprise level. Even in relatively successful collaborative ventures such as defence accommodation provision, there are data interpretation challenges for both vendor and customer.

Joint enterprise information and relationship requirements

Partnerships are held together by data and people, the information available to them and their behaviours. As part of the topic of defence applying international standards to its contracts, many joint information and relationship requirements were raised throughout discussions. This short section aims to capture as many of those as possible. They may appear to be intuitive, but they are clearly of concern to both defence and vendors, because they were repeatedly aired:

- The volume of data industry wants from the MoD is rising, but wherever possible, real-time metrics should be used because they serve both delivery partners and the MoD to pre-empt potential issues
- Auditing data against KPIs is vital, but is not always routinely done; this leads to inappropriate or valueless KPIs and obsolete targets that do not reflect current or emerging requirements
- Industry is worried about the consistency of the MoD's information needs, ways and means; standards help industrial partners to manage information needs

In terms of relationship management, it was deemed essential that defence should create organisational structures to mirror industry – that is, defence needs to provide SMEs in numbers and at the right location to manage the enterprise. With this in mind, Stable single points of contacts (SPOC) are good for the customer and supplier. Looking to wider structural activity and reflecting a requirement aired in the intelligent customer discussion, joint training with industry and continuously available staff, (possibly embedded with industrial partners) was deemed to offer a good return on investment that will greatly improve collaboration.

It is possible the MoD does not have the resources to manage long-term collaborative contracts. High turnover of staff in MoD projects and SME posts leads to loss of understanding and confidence in the relationship. In turn, with no stated standards, industry's perception is that there are too many opinions and a clear path in the form of doctrine is not presented by the MoD. Another symptom of this lack of long-term stability within the SME and leadership cadre is that the MoD discusses solutions too often, instead of the deliverables required from a relationship. In order to make progress in this vital area, industry might need to provide process support for the MoD. However, process does not replace a clearly articulated defence vision of the end state.

Informal delegate discussions in the Charterhouse Old Library

Theme 3: Managing supply chain risk

The third and final theme addressed was how defence might manage supply chain risk with the advent of the Defence Support Network. As defence support capability is outsourced (some 70% by 2017), how can or should defence use Log IS to manage supply chain risk through global, multi-layered out-sourced support chains? Are there any novel solutions that have been adopted by industry to manage risk? There is a clear causal effect that supply chain decision-making could have when managing supply chain risk, and as has been touched on earlier, Log IS and a real understanding of the information needed to enable sound decision-making is fundamental to this.

There are many types of risks that can threaten a supply chain. Risk comprises those factors that are known, is often graded by impact and likelihood, and can be considered for a range of management actions – by avoidance, mitigation or simply being resilient and riding it out. Uncertainty, however, comprises those factors that are unknown, and dealing with uncertainty may call for resilience that is simply unaffordable. Experience often transfers factors from the uncertainty pile to the risk pile!

Looking at internally focused risks, some of these may be arranged as illustrated in Figure 2. A major internal risk is driven by supply chain misalignment. In hierarchical terms, business strategy drives supply chain strategy, which in turn drives the supply chain network, processes and resource requirements. As with any chain, there needs to be feedback to attenuate shock and disruption brought about by change. The supply chain can be seen as three separate but indivisible interwoven chains, with physical, informational and financial strands running from end to end. If, however, the segments (strategy through to resource requirements) or strands (physical, informational, financial) become misaligned, a lack of co-ordination, predictability, resilience and consistency of performance can result that can severely disrupt the supply chain.

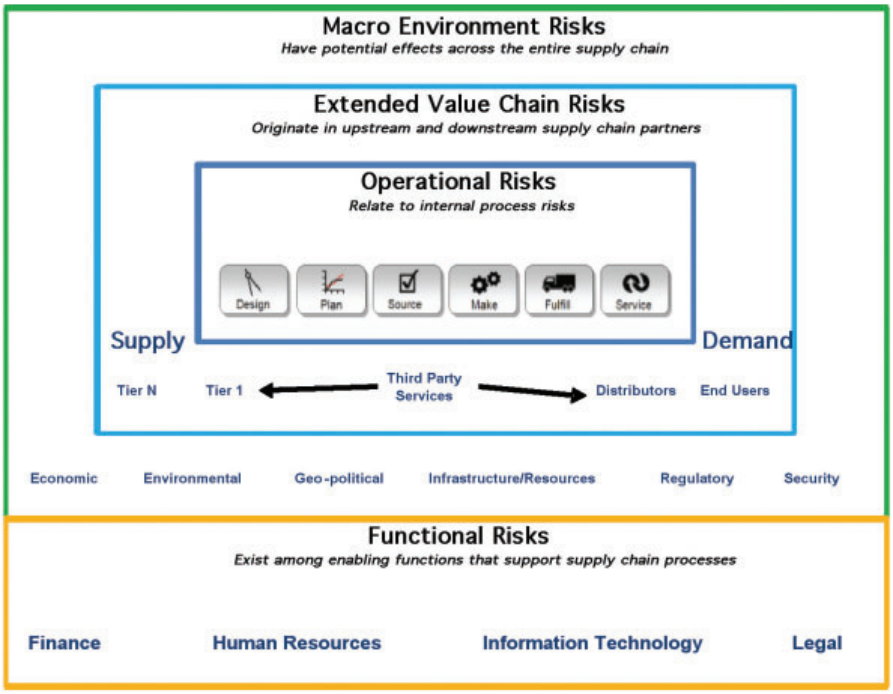

Figure 2: Understanding supply chain risk

Looking at the risks that can impact on a supply chain, they are so numerous that trying to understand them as a whole is probably impossible. One way to manage these risks might be to segment supply chains by commodity. Currently, defence treats every asset as equal for most processes, when the vast majority of inventory did not directly support the teeth arm, but is used in support activity. One historical example provided was where the now-defunct LITS team had created a high-activity centre that focused on those items that had moved in the last 12 months. Using this data it had been possible to create a Pareto curve to optimise the support for the things that moved the most.

In this way, each high-value, rapidly moving or mission-critical segment can be considered separately and overarching risks can then be considered with a more strategic view. With segmentation, when one part of the chain goes wrong, the impact can be minimised by exploiting other elements of the chain.

Segmentation had been promoted across the DE&S for some years, but the capability providers (IPTs) were not mandated to use it, and it had thus gained little traction despite the clear advantages it offered. There was a view this was due, in part, to a lack of professional awareness and financial training across the practitioner community. This led to a discussion on the merits and availability of management accounting expertise amongst the capability providers and, whilst the capability existed in small specialist teams within each service, the lack of routine engagement at desk level in DE&S was clearly a potential issue.

Risk management needs to be focused and centralised. What have in the past been manual, intermittent and disconnected processes need to be replaced with continuous, interactive, holistic and integrated processes. To do this, the supply chain owners need to align strategic goals with supply chain plans and operations, ensure full visibility of the physical, financial and information supply chains, and identify and allocate costs throughout the supply chain. Once this is done, the owners must ensure the financial viewpoint is embedded in the planning and execution processes. They can then quickly examine alternative scenarios and evaluate financial impact of decisions for any risk scenario, and deliver the 360j insight to allow the business to make informed decisions. Clearly, to achieve this, defence must first master the alignment of supply chain and financial data. It is notable that the top five commercial supply chains have implemented this sort of risk management strategy, and demonstrated real innovation and leadership in managing their data and inventories.

The human factor

There was a view from both defence and industrial delegates that information management in the armed forces needed to be professionalised, and setting up processes to mitigate risk was something military and commercial logisticians should work together to improve. There was, therefore, clear support for the establishment of professional information systems expertise in the MoD. A high expectancy is placed on migratory staff to solve huge logistics information systems issues. Unfortunately, all too often the MoD appears to appoint untrained hobbyists. Often those appointed do not have the requisite training or experience to act as intelligent customers, and are not equipped to deal with a contractor with the required level of understanding. It was suggested there was a case for professionalising a clear career path for military personnel in the logistics information systems sector. Coupled with this, the MoD needs to improve the commercial and contractual understanding and awareness within its logistic cadre. To enable this, there was a clear need for training in managing agile contracts and developing intelligent relationships with industry.

A US perspective

The US Defense Logistics Agency has attempted to minimise supply chain risk with a significant initiative to provide an integrated data environment or data gateway that enables connecting systems to share in the benefits of its modernised capabilities. The intent is that this network of systems will improve data visibility, access and timeliness. It should reduce data inconsistencies,

improve information interoperability and facilitate flexible integration of systems. Bold claims. However, the integration is based on three underlying principles: knowing what you have, knowing where your inventory is at any one time, and modernising systems where necessary.

Knowing what you have requires a consolidation of legacy stovepipe systems. This will produce a single consolidated view that can expose excess inventory (a major problem in the US armed forces). It will enable a mission-oriented view, as opposed to the historical service-oriented view resulting in lowered costs with less wastage through shelf life, storage and transportation inefficiencies. The process allows US Defense to move towards a just-in-time rather than just-in-case inventory, but most importantly provides a single version of the truth.

The second element of knowing where your inventory is may seem to be a non sequitur, but it provides a real challenge for US Defense. Working to the principle that you cannot use it if you cannot find it, it has introduced passive, active and in-transit tracking systems for items and consignments. However, integrating the various systems necessary for different environments has provided significant challenges. Given the single-service nature of the US inventories, which have not yet been fully consolidated, double counting of assets remains a problem until the first change requirement (system consolidation) has reached critical mass.

The third programme, modernising the Log IS capability, is similar to the UK's LOGNEC challenge, but may provide lessons worth sharing as it progresses. As with the UK, the USA aims to eliminate legacy single-service and specialist inventory systems once a consolidated system is in place. It has also learned to resist the temptation to customise the system to meet bespoke requirements, demanding that business processes change to fit the new system. It intends to use the system to leverage trading partners and monitor vendor compliance with contracted services. It is hoped this will provide additional confidence to allow greater reliance on third-party logistics.

Managing environmental supply chain risk

Should defence even bother investing in an ability to see down complex, extended, multi-layer supply chains, or should it put that onus on the contracted capability provider? One example from a leading car manufacturer suggests it should. A case study was presented and discussed on a supply chain event that forced BMW to develop new innovative technology to manage risk and uncertainty better. This was driven by the adverse effect the loss of production of a simple gearbox chip had caused to BMW when the only factory that was manufacturing that component had been closed down suddenly and unexpectedly following the Japanese Fukushima Daiichi disaster in 2011. BMW's reputation (not to mention costs due to disruption of its own production line) drove it to take extraordinary measures. This value of this reputation and production could be equated to the operational imperative of the defence supply chain on operations.

The study looked at how a global company that delivered approx 24 million spare parts daily could cater for such a low possibility–high impact risk as this. It was explained that in response BMW had mapped out its supply chain from Tier 1 to Tier n to get a better understanding of supply chain vulnerabilities. It had then developed an IS tool that linked a geo-visualisation system to an e-listening capability that monitored news channels, social media and other reporting sources around the world to be able to pick up quickly on any potential supply chain threats. It also scanned environmental warning systems for earthquakes, tsunami and other extreme weather events. This enables the company to react quickly in response to a disaster by immediately understanding which suppliers might be affected and by seeing where alternative suppliers' factories were located elsewhere. If the threat was deemed to be large enough for a vital component, or likely enough to happen for less critical spares, alternative suppliers could be instructed to increase production immediately to reduce the likelihood of disruption to the supply chain and, ultimately, the production line. Pre-emptive action to expedite delivery of components from the factories at risk, or using alternative distribution routes for stock in transit could also be effected to minimise risk. Further discussion revealed the technology, search algorithms and analytical tools used for these processes were relatively simple and available, and used globally by the likes of Google, Amazon and Yahoo!

Future risks

The expert community was canvassed for views on what the potential future risks for the defence supply chain and logistics information system were, revealing issues that might be considered by MoD logistic strategists. The different support approaches that were being contracted for by the MoD were seen as a growing risk. The increase in available contracting support solutions could confuse convergence. It was suggested that this risk could be mitigated if the MoD got its governance and authority arrangements right. Other potential risks included vendor lock-in and development costs.

There was a risk that the MoD might simply drown in data. It was explained that data should be seen as three distinct elements: data, information and insight. The problem is that a focus on today's operational issues meant that it was easy to ignore the third of these elements.

It was recommended that the MoD think in terms of optimising systems rather than individual elements because supply chains are not one-dimensional.

Delegates and moderators in a round-table discussion

Summary

There was an enormous amount of information produced during the event, drawing on over two millennia of experience amongst the delegates, who are listed in the Annex to this paper. This paper can only hope to capture the most significant issues raised in the plenary sessions, but the value of the event also includes the human, professional and academic exchanges that took place outside of the plenary chamber between the delegates, which cannot, unfortunately, be captured on paper.

There were many more issues than solutions raised across the three themes: developing intelligent customer capability; managing support chain partner performance across the Defence Support Network; managing extended supply chain risk. However, there were some common and enduring issues that ran through most of the discussions. The more prominent of these, and those that were recognised collectively by defence, industry and academic delegates, are incorporated into the paper, and have been subject to editorial re-brigading to prevent it becoming simply a verbatim record of discussion. Any misrepresentation, errors of omission or fact are unintentional, and the paper has been constructed in good faith. Inevitably, issues raised may be construed as criticism, but this is not the case. Many are driven by environmental, financial and operational pressures on defence and industry alike, and by raising them here, it is hoped that they can be considered in an objective way.

Of the enduring issues raised, the following are worth reiterating because, in the opinion of the author, they are the ones that can be readily identified, and something can actually be done about them, some in a collaborative way between defence and industry, some internally by defence, although it should be noted that many of the defence issues raised also exist in industry to some extent. Most of these issues are deep seated, and so addressing them will be a long-term, enduring task. However, if the first steps are not taken to recognise them formally and take action, their impact will only increase as the Defence Support Network and the new way of providing defence support capability evolves.

Human factors

Industry and some of the defence logistic leaders want the MoD to professionalise Log IS. The MoD is not seen to embrace Log IS at the highest levels (it is not a component of fighting power, and does not attract sufficient resource to meet acknowledged shortfalls), nor does it appear to understand the associated complications, because it keeps moving staff and teams. Even if defence outsources the expertise to design, deliver, maintain and operate Log IS, it will not be able to act as an intelligent customer unless it has the expertise to understand its own information requirements and recognise the good from the bad. Defence would expect the capability provider for armoured systems to understand the technical and operational aspects of those systems. It develops and hones that understanding through training, education and deep operational experience with the armoured systems. It should do the same with Log IS.

The lack of a professional cadre may contribute to poor governance in the future because the SMEs are unlikely to progress up the command chain and bring real understanding to higher leadership and decision makers.[5] Understanding vs authority is not limited to Log IS, but its effects are felt more acutely where those that have one often do not have the other. This is probably a function of defence's organisational structure. Couple this with the splintered approach to authority (too many people with authority over tiny parts of the plan) and it is no surprise the MoD has achieved only an estimated five years of technical benefits in 15 years of development. This is also due, in part, to the lack of professionalisation and a professional cadre identified above. Many of the leaders in specialist Log IS firms have a background of specialised Log IS experience in the armed forces, a legacy of the in-house Defence Log IS establishments that are now long gone. Building this sort of expertise in future may need the placement of serving officers in SI and vendor businesses. If this expertise is to be pushed up the command chain to the decider level, sufficient junior SMEs must be placed in industry to cover for career attrition and wastage. Developing this capability in the reserve pool may be a mitigating option for the interim.

Speed of transformation

It could be argued the MoD does not adequately manage adaptive change, nor fund it. In all three themes, the lack of agility in contracting for Log IS was highlighted. This inability to implement change rapidly led to providing yesterday's technology tomorrow, at the day after tomorrow's prices. Commercial IS solutions are typically implemented in 12 months, and defence should revolutionise its approach to procuring such capabilities to enjoy the benefits of innovation and current, proven capability.

Governance and authority

Most delegates supported a move towards a unified, defence-wide Log IS authority to bring coherence to the disjointed legacy systems. The creation of a defence information chief is a step in the right direction, but there must be a recognised and empowered authority to drive through business change in the logistic arena.

Until this new organisation has matured enough to be given, and exercise, appropriate authority (including financial control), Log IS should impose some disciplinary measures to prepare itself for proper incorporation into this structure. The first of these is that the democracy of user needs should not interfere with corporate needs. Users do not chose the MIS they want in order to deliver defence effect. Users' stovepipe usage does not qualify them to drive through the wider corporate change that converged MIS can support. There appear to be many IT departments within defence with their own budgets, agendas and processes making convergence of the enterprise MIS solutions very difficult. As an example, the MoD failed to get MJDI an interface into JPA, and there is little evidence of a corporate plan to bring these two major systems alongside financial MIS. Indeed, some parts of defence appear to act almost autonomously, with the potential to stifle innovation in the centre.

Informal discussions continue in the Charterhouse surrounds

Acknowledgements

Thanks must be given to all of the speakers, panellists and participants for being so candid and open in their discussion, the moderators, Drs David Moore, Andrew Humphries and Simon Templar for leading those discussions, and the rapporteurs, Major Ian Bowers and Squadron Leaders Robin Nash and Mike Reed for capturing it all. The intellectual content of this paper could not have been produced without significant input from all of them.

There was also a team of dedicated supporters who made the physical event possible, too many to mention, who gave a lot of personal time and effort to turn the idea of the occasion into reality. Special mention must go to Ana Walker, Forum Administrator and Development Co-ordinator, CILT, and Lara Ramsden Charterhouse, whose extraordinary efforts made the event memorable. The CILT Defence Forum is also indebted to IFS (www.ifsworld.com/en-gb/) and ToolsGroup UK (www.toolsgroup.com/en/) for their generous support that enabled the delegates to enjoy the event and concentrate on the intellectual content of the day.

About the author

Chris Markey FCILT is Director, Chris Markey Associates Ltd. Following a full career in the Royal Air Force over 35 years, he has been providing professional supply chain, logistics and leadership advice to commercial and academic enterprises since 2009. As Deputy Commander of the Joint Force Logistic Component in Kuwait and Iraq in 2003, he was part of the command team that successfully managed the reception, staging and onward movement of 42,000 personnel into Iraq in 2003, in half the time taken during the liberation of Kuwait in 1992, and supported the war-fighting phase of Operation TELIC I. He subsequently managed the transformation of the support organisation post-conflict to create a single logistics base, and reduce staffing from 7,800 to 3,000 personnel in support of stabilisation operations during Operation TELIC II. His last tour in the MoD was as a policy director responsible for the development and implementation of national and international policy for the UK Armed Forces Reserves. His remit covered operational use, health, welfare, employer support, communications and legislation. He is Chairman, Defence Forum and Thames Valley Group, CILT, and mentors young entrepreneurs in the Levant through the charitable foundation Mowgli.

References

1. Collinson Grant: An information system (IS) is an arrangement of people, data, processes and information technology that interact to collect, process, store and provide as output, the information needed to support an organisation.

Types of IS:

- Transaction processing systems
- Management information systems
- Decision support systems
- Expert systems
- Communications systems
- Collaboration systems
- Office automation systems

2. Facebook has 1.23 billion users a month, or 757 million a day. If it were a country, it would be the third largest. As we see from e-commerce and omni-channel supply chains, customers are generally more connected with 24/7 access where they want, across multiple touch points. Conversely, for businesses, customer intelligence equals competitive advantage: it costs five to seven times more to create a new customer than to retain a current one.
3. The move of 3,345 vehicles and major equipment, 50 fixed-wing aircraft and helicopters, plus 5,500 ISO container loads at a cost of recovery £300–350 million suggests two things: it will be a challenging ICT problem, and it will be subject to endless scrutiny.
4. SCALA's 11th Annual Logistics Debate, in association with the CILT: *Why isn't collaboration working?* A major theme that emerged was the need for collaboration to be part of a culture of an organisation supported and driven from a strategic and senior level. For Tony Wallis, Sales and Marketing Director, Toyota Material Handling Europe, collaboration is in the genes of Toyota with BMW engines used in Toyota cars as a norm. At United Biscuits, Rob Wright spoke of a wealth of experience in collaboration with competitors and partners. None of this would be possible without top-to-top support from CEOs and board members. Nigel Smith, Group Supply Chain Director, Tayto, included the development of a culture of collaboration as a significant ingredient in a recipe for effective joint working. He added the concept of vertical change, which involved collaboration across partners at all levels of operation to support the development of a collaborative culture.
5. When US Navy Secretary John Lehman was driving forward Ronald Reagan's programme to build a 600-ship navy, he realised that top-quality people were needed to manage acquisition programmes. The Navy Materiel Professional programme was initiated. Separate selection boards identified candidates for this role, and billets were identified up to four star-level and limited to materiel professionals.

Glossary of terms and acronyms

AWL
Augusta Westland Ltd

BAES
British Aerospace Systems

Bluelightworks
Bluelightworks™ is an innovative capability, providing unbiased, objective advice supporting transformational change initiatives to the emergency services; particularly those enabled by Information Technology.

CESG
Communications Electronics Security Group. CESG is the information security arm of GCHQ, and the National Technical Authority for Information Assurance within the UK. It is the definitive voice on the technical aspects of information security in Government.

CLS
Contracted/Contractor (provided) Logistic Support

COTS
Commercial OFF-THE-SHELF

DE&S
Defence Equipment & Support

IOS
Integrated Operational Support. IOS programmes allow customers to combine numerous individual short-term support contracts into a single, performance-based logistics solution that covers the maintenance, technical support and inventory management of their whole aircraft fleet. This reduces risk, reduces cost and improves efficiency and aircraft availability.

IPT
Integrated Project Team. Within DE&S, cells of individuals, whose skills span the design, development, manufacture and through-life aspects of a platform or weapon system.

JPA
Joint Personnel Administration

JSC Blueprint
Joint Supply Chain Blueprint. A guide for those involved in leading, planning, developing and delivering supply chain and supply solutions. This ranged from DE&S IPTs, Industry (as either a manufacturer or provider of CLS) through logistic planners, to deployed commanders and supply chain operators in a joint operating area or single service environment. It was laid out in Joint Service Publication 886 Volumes 1 and 2.

LITS
Logistic Information Technology Solution. An RAF LogIS designed to support acquisition, maintenance and correction of aircraft configuration data. It would support fleet management activities by the IPTs, analysing trends to provide evidence of continued airworthiness, relating to lifing, fault and reliability.

LogIS
Logistic Information Systems

LOGNEC
Logistics Network Enabled Capability. A partnership between the UK Ministry of Defence and industry is transforming the ability to manage logistic information by replacing ageing systems, converging processes and applications and rationalising the number of stakeholders involved in the overall process.

MIS
Management Information System(s)

MJDI
Management of the Joint Deployed Inventory. A deployable Log IS for demanding, receiving, supplying and maintaining details of materiel ranging from boots to ammunition and medical stores.

MoU
Memorandum of Understanding

NDA
Non-Disclosure Agreement

Niteworks
Partnership between the UK Ministry of Defence (MoD), including the Defence Science & Technology Laboratory (Dstl), and industry. It aspires to be the definitive partnership to provide decision support to enhance current and future capability, and provides a unique collaborative environment that enables the MOD and industry to work together to make informed decisions for the MOD.

PBL
Performance-Based Logistics. Also known as performance-based life-cycle product support or performance-based contracting, a strategy for cost-effective weapon system support. Rather than contracting for the acquisition of goods and services, the product support manager identifies product support integrator(s) (PSI) to deliver performance outcomes as defined by performance metric(s) for a system or product. The integrator often commits to this performance level at a lower cost, or increased performance at costs similar to those previously achieved under a non-PBL or transactional portfolio of product support arrangements for goods and services.

PPP
Public Private Partnership

R-R
Rolls-Royce

SI
Systems Integrator. A person or company that specialises in bringing together component subsystems into a whole and ensuring that those subsystems function together.

Notes

Delegate list

Note: Names have been removed in accordance with Chatham House rules.

Chief Executive, CILT

UP Supply Chain Development, DHL Supply Chain

London Chair IMS, The Institute for Management Studies

Officer, 151 Regt RLC

Scientist, Defence Science & Technology Laboratory

SO1 Log C4I LSCO, Army HQ

Sales Manager – Defence, Selex ES

Senior Consultant in Logistics, Systems Consultants Services Ltd

IT Bid Lead, Defence & Security, Babcock International Group

Head Service Delivery Accommodation, Ministry of Defence

Rapporteur, HM Forces (Army)

Head of Logistics, BAA Heathrow

Sales Excellence, Maersk Line

Chairman, ADS Group Limited

Commanding Officer, DCOS Inventory Management Operating Centre

Logistics Support, MOD NCHQ

Flying Officer, HM Forces (RAF)

IT Programme Manaager, Defence & Security, Babcock International Group

Flying Officer, HM Forces (RAF)

Head of Logistics, Babcock Naval Services

Officer, HM Forces (RAF)

Project Manager, Leidos

Director IT, Defence & Security, Babcock International Group

Master Principal Consultant, Oracle

Major General, HM Forces

Head of Government & Defence (UK & Europe), Damco UK

Supply Chain Director, Sauflon Pharmaceuticals Ltd

OC Support Party, HM Forces (RAF)

Events Manager, CILT

Head of Defence Logistics, Steria Ltd

Director, Aerospace & Defence Centre of Excellence, IFS World

General Manager – Land, Wincanton Ltd

Head ACDS Cap JLE, Ministry of Defence

Master, Charterhouse

Strategic Intelligence Director & Defence Adviser, Hewlett-Packard

Senior Technology Consultant, BearingPoint Limited

Assistant Chief of Defence Staff, Logistics Operations, Ministry of Defence

CEO, SCCI Ltd

IT Solutions Manager, Kuehne + Nagel Limited

Editor/Publisher, CILT

Material Control Manager, Babcock Naval Services

Senior Principal Consultant, Oracle Corp UK Limited

Lecturer in Business Economics & Strategy, Manchester Business School

EA/1SL, Ministry of Defence

Technical Programme Manager, Kuehne + Nagel Limited

Officer, HM Forces (RAF)

SO1 Support Chain Information Services, Defence Equipment & Support

DACOS Log Support, HM Forces (RN)

Officer, HM Forces (RAF)

Chief Engineer Architect, Boeing Defence UK Ltd

Director, Chris Markey Associates Ltd

Director of Logistics, Candy Professional Services Ltd

Officer, HM Forces (RAF)

Transformation Manager, Boeing Defence UK Ltd

Head, Centre for Defence Acquisition, Cranfield University

Officer Commanding, HM Forces (Army)

DICOM, MOD

Director, BearingPoint Limited

Group Sales Director, ToolsGroup UK

Flying Officer, HM Forces (RAF)

Senior Business Relations Manager, Boeing Defence UK Ltd

Supply Officer, HM Forces (RAF)

Senior Director – EMEA, Oracle

IT Bio Lead, Defence & Security, Babcock International Group

Director, Bisham Consulting

Senior Analyst, DSTL

Senior Strategy Analyst, DSTL

Specialist Sales, Oracle Corp UK Ltd

Flying Officer, HM Forces (RAF)

Director, PWC LLP

Operations Officer, Chronia Nigeria Limited

Pers Trg-Strat & Prog NEM Programme – TOS TL, Ministry of Defence

Lecturer, Cranfield University

Business Development Director, Unipart Group Ltd

Global Defence Advisor, Fujitsu Services

Movement Control Warrant Officer, HM Forces (Army)

Logistical Consultant, T2L Logistics

Commander, Bundeswehr Logistics Centre, German Federal Armed Forces

Head of Product Management, IFS World

Principal Consultant, UK Ministry of Defence

Forum Administrator and Development Co-ordinator, CILT

Partner, BearingPoint Limited

DACOS Logistics Strategy and Capability, HM Forces RN

Log Svcs WO1 Land Forces, HM Forces (Army)

Flying Officer, HM Forces (RAF)

Partnership Director, Serco Aerospace

Business Development Manager, Steria Ltd

Managing Director, ToolsGroup UK

Visiting Senior Fellow, Lincoln University

The Chartered Institute of Logistics and Transport

www.ciltuk.org.uk

The Chartered Institute of Logistics and Transport in the UK
Earlstrees Court, Earlstrees Road, Corby, Northamptonshire NN17 4AX