Kokoda Foundation

KOKODA PAPER NO. 19

Australian Defence Logistics

The Need to Enable and Equip Logistics Transformation

Dr Gary Waters and AVM John Blackburn AO (Retd)

June 2014

Kokoda Paper No. 19
June 2014

Australian Defence Logistics

The Need to Enable and Equip Logistics Transformation

Dr Gary Waters and AVM John Blackburn AO (Retd)

THE KOKODA FOUNDATION
www.kokodafoundation.org
RESEARCHING AUSTRALIA'S FUTURE SECURITY CHALLENGES

National Library of Australia Cataloguing-in-Publication entry

Author:	Waters, Gary, 1951- author.
Title:	Australian defence logistics : the need to enable and equip logistics transformation / Dr Gary Waters, AVM John Blackburn AO (Retd).
ISBN:	9780980730685 (paperback)
Series:	Kokoda papers ;no. 19,
Subjects:	Military art and science--Australia. National security--Australia. Logistics.
Other Authors/Contributors:	Blackburn, AVM John, author. Kokoda Foundation.
Dewey Number:	355.47994

ABOUT THE AUTHORS

DR GARY WATERS

Dr Gary Waters spent thirty-three years in the Royal Australian Air Force, retiring as an Air Commodore in 2002. He subsequently spent almost four years as a senior public servant in Defence and then worked with Jacobs Australia as Head of Strategy for just over seven years. He left Jacobs in March 2013 and now acts as an independent consultant.

He has written fourteen books on doctrine, strategy, cyber security, and military history. His latest two books are 'Optimising Australia's Response to the Cyber Challenge' (with Air Vice-Marshal John Blackburn) in 2011, and 'Getting it Right: Integrating the Intelligence, Surveillance and Reconnaissance Enterprise' in 2014. In early 2014, he also published his Kokoda Foundation Discussion Paper entitled 'Pressing Issues for the 2015 Defence White Paper'.

He is a Fellow of the Royal Melbourne Institute of Technology (graduating with majors in accounting and economics); a CPA; a graduate of the United Kingdom's Royal Air Force Staff College; a graduate of the University of New South Wales, with an MA (Hons) in history; a graduate of the Australian Institute of Company Directors; and a graduate of the Australian National University with a PhD in political science and international relations.

He has been a Fellow of the Australian Institute of Company Directors, a Vice President of the United Services Institute, and a Board member of Defence's Rapid Prototype, Development and Evaluation (RPDE) Program. He currently serves on the Board of the Kokoda Foundation.

AIR VICE-MARSHAL JOHN BLACKBURN AO (Retd)

John retired from the Royal Australian Air Force in 2008 as the Deputy Chief of the Air Force following a career as an F/A-18 fighter pilot, test pilot and strategic planner. His senior posts included Commander of the Integrated Area Defence System (IADS) located in Malaysia, commanding a multi-national headquarters established to effect the Five Power Defence Arrangements (FPDA), and Head of Strategic Policy in the Defence Headquarters. He is now a consultant in the fields of Defence and National Security.

He is the Deputy Chairman of the Kokoda Foundation Board and the Deputy Chairman of the Williams Foundation Board. He holds a Masters of Arts and a Master of Defence Studies. In February 2011 the Kokoda Foundation published his report "Optimising Australia's Response to the Cyber Challenge" which he co-authored with Dr Gary Waters. In February 2014 the NRMA published his report "Australia's Liquid Fuel Security Part 2."

CONTENTS

About the Kokoda Foundation

The Kokoda Foundation is a registered charity and not-for-profit organisation. Its research is independent and non-partisan. The Kokoda Foundation does not take institutional positions on policy issues nor do sponsors have editorial influence. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author.

Published in Australia by the Kokoda Foundation, June 2014.

Photos courtesy of the Australian Department of Defence

Series Editor: Catherine Scott

Publication Management: QOTE Canberra (02) 6162 1258

Published and distributed by:
The Kokoda Foundation
2/10 Kennedy Street
(PO Box 4060), Kingston ACT 2604

T: +61 2 6295 1555
F: +61 2 6169 3019
Email: info@kokodafoundation.org
Web: www.kokodafoundation.org

Additional copies are available from the Foundation at A$22.00 per copy
(including GST and postage in Australia).

PREFACE

This publication would not have been possible without the support and assistance of several areas across the Department of Defence and a number of industry representatives. The senior Defence officials and industry leaders who participated in the Defence Logistics project provided exceptional insight and assistance. A large number of interviews and meetings and three major workshops were conducted in the second half of 2013; the Kokoda Foundation would like to thank all of those involved in these activities.

The Project would not have been possible without the generous support of our sponsors – Accenture and RubiKon – who also provided sterling assistance in several briefings and discussions on key aspects of logistics and commercial supply chains.

This report aims to highlight to the wider Defence community the challenges faced by Defence Logisticians and the lack of priority that Defence leaders have placed on Logistics systems in the past. Its fundamental contention is that Defence will need to place greater emphasis on the Defence Logistics function if it is to meet the challenges of a more complex and challenging operating environment in the future. Given the complexity of the Logistics challenge, the report can only provide a high level overview of Defence Logistics. Readers who wish to discuss and debate aspects of this report are encouraged to do so by preparing a short commentary or longer article for the Kokoda Foundation's professional journal, Security Challenges.

Gary Waters
John Blackburn

EXECUTIVE SUMMARY

The Kokoda Foundation conducted a logistics study over the second half of 2013 to explore how Defence can better enable and equip the transformation of Defence Logistics in order to more effectively support Australian Defence Force Operations in the future.

This report explores Defence Logistics challenges by posing six questions:

- **What is Defence Logistics?**
- **What does Defence Logistics do?**
- **What is the current state of Defence Logistics?**
- **What are the future challenges for Defence Logistics?**
- **What can Defence learn from Industry / other organisations?**
- **What can be done to improve Defence Logistics?**

The answers to these questions were sourced from a range of Defence and Industry logistics and supply chain experts. In accordance with the practice of the Kokoda Foundation, all discussions and workshops were held under the "Chatham House" rule with no attribution.

Logistics support is a complex challenge for Defence and will become increasingly so in the forthcoming decade as Defence Logistics becomes even more integrated with commercial supply chains; many, if not most, of which are becoming global in nature. Despite the challenges, Logistics does not enjoy the same visibility or priority as do the military platforms and equipment that Logistics supports. This lack of visibility and priority for Logistics could give rise to increasing levels of risk for the Defence Enterprise.

The lack of priority has been compounded by a failure to assign appropriate responsibility and authority for this essential Joint function at the right level. Despite the appointment of the Chief of Joint Logistics (CJLOG) as the strategic J4, he does not have sufficient breadth of control to direct the entire Defence Logistics domain. Consequently, the Defence Logistics domain is viewed by many as being fragmented and lacking a holistic approach, to not only the domain itself, but also the broader environment in which it operates.

This comment in no way seeks to diminish the important role of the CJLOG nor the highly effective manner in which he and the Joint Logistics Command (JLC) execute their tasks. Rather, it highlights the unintended consequence of a failure to assign appropriate responsibility and authority at the joint level. The resulting tendency to view the various aspects of Defence Logistics through component elements introduces operational, enterprise and financial risk to Defence.

Whilst the answers to the questions posed by the report are informative, the fundamental challenge addressed in the report's recommendations is how can the existing Defence Logistics domain be enabled and equipped to deal with the transformation required to address the challenges and opportunities that arise from a future-oriented change agenda *whilst also dealing with the reality of ongoing business*. Whilst Industry can offer excellent examples of how to improve Defence Logistics and will, inevitably, operate significant components, the transformation of Defence Logistics must be led from within the Defence organisation.

The report therefore makes recommendations for changes in:

- **Organisational Design and Culture.** The apparent lack of "logistics champions" across the current senior leadership group, with the exception of CJLOG and his senior staff and a small cadre of senior officers in the Service Headquarters, is an issue. The importance of obtaining the right priority and support for the transformation of Defence Logistics as a whole cannot be overstated. It is important enough to warrant the Defence leadership firstly considering mechanisms such as recall days to inform and educate the wider leadership group of the issue. A second, but as critical an issue, is that of a Logistics Capability Manager. Until Defence is culturally able to accept the need for a "Joint Capability Manager" with the authority of the Single Service and Group Capability Managers, then Defence Logistics will continue to operate in the seams between the Capability Managers' areas of responsibility and accountability, without the required authority to transform and operate the transformed Logistics enterprise. If a Joint Capability Manager was appointed, then CJLOG could operate under their authority and under their unique joint purview.

The importance of obtaining the right priority and support for the transformation of Defence Logistics as a whole cannot be overstated.

- **Strategy, Concepts and Concepts of Operation.** The lack of an updated Logistics strategy, concepts and an endorsed Concept of Operations (CONOPS) based on an agreed logistics business architecture are significant impediments to addressing the logistics challenges at an enterprise level. Whilst much can be learned from Defence's past logistics experience, and from industry, translating those lessons into an integrated management model that will support the required transformation of Defence Logistics is not a small task. To date, the resources do not appear to have been available in either the Vice Chief of the Defence Force (VCDF) Group or under CJLOG to build the conceptual and architectural foundations required. Failure to invest in the "front end" will inevitably hamper the effective transformation of Defence logistics and in turn compromise future ADF operations. Defence needs to invest in these areas as a matter of priority.

- **Change Leadership and Resourcing.** Noting the challenge of managing change in addition to the overwhelming load of day-to-day business, CJLOG and his Command do need additional support and resources to perform their critical tasks, particularly given the dense and complex organisational processes employed by Defence. Whilst some supplementation of key functions appears warranted, there may also be value in considering additional support of a different nature. Noting the value of the US Combatant Commands' experience of exchanging liaison officers between Commands in order to translate and communicate across organisational boundaries, there may be benefit in CJLOG being supported by a senior advisory/liaison team that is not wholly comprised of logisticians. For example, if an inter-disciplinary team with organisational links to the Capability Managers and DMO supported CJLOG, there could be benefits in having the team develop the Logistics Strategy and plans under CJLOG guidance, which they could then communicate and champion across Defence, prior to formal consideration by the layered committee system. An experienced operator (vice logistician), having taken the time

to analyse and comprehend the logistics challenge, may have a greater chance of success in communicating the logistics needs and priorities to their parent Service and the senior operators therein.

If this report serves to highlight to the wider Defence community the challenges faced by Defence Logisticians and if it gives pause to think about the lack of priority that Defence leaders have placed on Logistics in the past, then it will have achieved the goals of the authors and the Kokoda Foundation. Defence will need to place greater emphasis on the Defence Logistics function if it is to meet the challenges of a more complex and challenging operating environment in the future.

ACKNOWLEDGEMENTS

The Kokoda Foundation wishes to express its thanks to Accenture and RubiKon for their generous sponsorship of the project.

The Foundation is also appreciative of the ongoing support of the Department of Defence.

SPONSOR PROFILES

Accenture Profile

At Accenture, we recognise both the challenge to more effectively integrate and synchronise logistics and the Kokoda Foundation's role in stimulating debate on solutions to these issues.

Through our support of this report, we seek to gain insight into characteristics that help to improve the productivity and efficiency of services for the warfighter, particularly in a climate of rising costs and budget cuts.

We believe that defence leaders must embrace four structural shifts—advancing toward personalised services, insight-driven operations, a public entrepreneurship mindset and a cross-agency commitment to mission productivity. By making these shifts, defence agencies can support the warfighter mission of safe, secure nations in a digital world – delivering public service for the future.

Around the world, Accenture helps defence agencies to achieve high performance in a complex, changing environment. We help improve the efficiency and effectiveness of mission and mission-support activities through our organisational performance and business process improvement strategies, information technology and preconfigured ERP solutions.

Accenture is one of the world's leading organisations providing management consulting, technology and outsourcing services. Our clients include 94 of the Fortune Global 100 and more than three quarters of the Fortune Global 500. With approximately 289,000 people serving clients in more than 120 countries, the company generated net revenues of US$28.6 billion for the fiscal year ended Aug. 31, 2013.

To read more about our Defence Services, and download our latest research and reports, visit www.accenture.com.

Rubikon Profile

The RubiKon Group is a specialist supply chain and project management consultancy providing services across a broad range of industries from mining and aerospace to healthcare and finance.

100% Australian owned and operated, with a strong government and defence heritage, RubiKon exploits a portfolio of powerful software tools and proprietary models to deliver class-leading outcomes in the fields of supply chain and project management.

Our aim, put simply, is to provide you with the solutions you need to be better in business. Whether this means optimising and refining existing practices and technologies, or the complete overhaul of a malfunctioning system to implement lean, best practice processes.....RubiKon can make the difference.

- Cost Estimating
- Procurement & Spend Management
- Inventory Optimisation
- Integrated Logistic Support
- Green Supply Chain Profitability
- Warehousing
- ICT Implementation
- Asset Accounting & Security
- Supply Chain Design & Analysis
- Project & Program Management

We are committed advocates of the principle that a good business is based on good people, using the right processes whilst being supported by the proper tools. Whether the objective is lower inventory stocks with greater customer satisfaction, a smaller environmental footprint with better profitability or simply a bigger competitive advantage, the path to success is the same.

By quickly learning the synergies and compromises inherent to your organisation and applying the people/process/tools principle, the RubiKon team will help you to become better in business.

Brisbane | Sydney | Canberra | Melbourne | Cape Town
WWW.RUBIKON.COM.AU
INFO@RUBIKON.COM.AU

INTRODUCTION

Logistics support is a complex challenge for Defence and will become increasingly so in the forthcoming decade as Defence Logistics becomes even more integrated with commercial supply chains; many, if not most, of which are becoming global in nature. Despite the challenges, Logistics does not enjoy the same visibility or priority as do the military platforms and equipment that Logistics supports. This lack of visibility and priority for Logistics could give rise to increasing levels of risk for the Defence Enterprise. Given these concerns, the Kokoda Foundation conducted a Defence Logistics study during the second half of 2013.

Purpose

The purpose of this study was to:

- comprehend the nature of Defence Logistics for the Australian Defence Force (ADF);
- explore the challenges faced by Defence Logistics, particularly at the enterprise level;
- explore the value of a systems approach to deal with complex Logistics challenges;
- explore emergent thinking on risk management and dealing with uncertainty at a strategic or enterprise level;
- review how logistics information management systems and logistics support concepts are integrated within the Defence Information Environment; and
- review if the Defence Logistics capability is as effective as it can be in supporting preparedness of the Joint Force in-being and the future force under development.

Report Structure

This report explores Defence Logistics challenges by posing six questions:

- What is Defence Logistics?
- What does Defence Logistics do?
- What is the current state of Defence Logistics?
- What are the future challenges for Defence Logistics?
- What can Defence learn from Industry / other organisations?
- What can be done to improve Defence Logistics?

WHAT IS DEFENCE LOGISTICS?

Defence Logistics acquires the resources for military operations, positions those resources where they are needed, sustains them throughout the conduct of operations and redeploys and regenerates them. It can be defined broadly as 'the science of planning and carrying out the movement and maintenance of forces'.

Logistics in the Broad

Military commanders have the responsibility to Raise, Train, Sustain (RTS) and employ combat forces. Logistics plays a major role in each of these functions through its ability to create and sustain support of weapons systems and forces that can be tactically employed to attain strategic objectives. Effective Logistics delivery has enhanced the capacity of smaller forces such as the ADF to conduct operations in increasingly complex situations.

Defence Logistics acquires the resources for military operations, positions those resources where they are needed, sustains them throughout the conduct of operations and redeploys and regenerates them. It can be defined broadly as 'the science of planning and carrying out the movement and maintenance of forces'.

Logistics encompasses four generic processes as follows:

- **Requirements determination** – establishing what is needed, in what quantity and quality, when, and where.
- **Acquisition (or procurement)** – buying the supplies and services and other resources needed to meet the requirements that have been determined.
- **Distribution** – moving the resources acquired to their place of use, which includes the supply tasks of collecting, storing, protecting and issuing resources.
- **Conservation** – deriving the greatest value from all resources, specifically by caring for them through the maintenance tasks of servicing, inspecting, repairing, modifying and overhauling. It includes the engineering tasks of ensuring structural integrity, engineering performance, and reliability, at minimum cost.

Management of the functions required to acquire, store, transport, and maintain the materiel necessary to support combat forces must be integrated.

Management of the functions required to acquire, store, transport, and maintain the materiel necessary to support combat forces must be integrated. The task of the Defence logistician is to establish the appropriate balance among these functions to achieve the required level of operational support while consuming the least amount of resources. However, when faced with complex systems or tasks, it is common practice to break down the systems or tasks to digestible parts, often managed under separate and sometimes disparate command chains. In doing so, it becomes increasingly difficult to understand how changes and component levels impact the overall effectiveness of the entire Logistics function. For example, optimisation of the various elements of the supply chain in isolation may appear to each individual responsible for a part of the chain to be an effective method. However, this can blind individuals to the opportunities that could emerge from the optimisation of the supply chain as a whole.

WHAT DOES DEFENCE LOGISTICS DO?

Defence Logistics operates under the overarching Defence Strategic Guidance provided by Government in order to support the current and future Preparedness of the Defence Force.

Defence Strategic Guidance

Strategic guidance for Defence is provided through the Defence White Paper. Current guidance calls for:

- The continuing emphasis for the ADF on readiness, mobilisation and interoperability to deal with traditional challenges and the development of new capabilities to counter the threat of terrorism and deal with cyber security.
- The emphasis on flexibility and adaptability for the ADF in a time of strategic uncertainty.
- The capacity of the ADF to conduct operations in higher intensity conflict, most likely as a participant in combined or coalition operations.
- The capacity of the ADF to support civilian agencies to protect Australia's borders and economic interests.
- Continuing counter-terrorism and counter-insurgency operations, including preventing the spread of Weapons of Mass Destruction (WMD).
- Continuing focus on the security of weak or failing states.
- Australia's security priorities still extend into distant theatres and the ADF must be able to deploy, operate and be sustained in these distant theatres.

The Department of Defence must ensure that the Logistics support environment can contribute to these requirements and meet Government's expectations. However, the context for the logistics support environment is changing. Emerging trends include the:

- increasing complexity of modern warfare and the diversity and sophistication of adversaries;
- broadening scope of ADF operations; and
- impact of changes in commercial logistics practice.

Preparing the Defence Force

Defence Logistics has to consider applicability of the provided support across diverse potential Areas of Operation, in both permissive and contested environments, and in alliance, coalition or self-reliant contexts.

The combination of fiscal austerity and growing strategic uncertainty underscores the necessity of adopting a risk-based approach as the foundation for Defence's preparedness and mobilisation principles. Preparedness is defined in this Report as *the sustainable capacity of Defence to accomplish directed tasks and provide contributions to Government for emerging issues and events that affect Australia's*

National Interests. Breaking this into its most basic elements, Defence needs to deliver a prepared Joint Force-In-Being (JFIB) that is able to: undertake directed national tasks and/or operations; and provide effective capability options to Government to allow them to respond to changes in the environment.

Preparedness is a combination of readiness and sustainability; that is, the enduring ability to execute and sustain a response that Government may expect Defence to deliver. Although readiness and sustainability are separate issues, they are inseparable in terms of overall preparedness management and must be considered in concert as a part of an integrated business planning framework. [1]

Mobilisation is a related concept – it is the transition period between preparedness and the conduct of a specific operation. Deliberate planning for mobilisation is a part of Defence preparedness. The preparedness posture of the JFIB provides the 'expansion base' from which Defence is expected to mobilise, should that be necessary. In essence, mobilisation moves force elements from a preparedness state to an operational state, which should help identify logistics drivers and costs.

The aim is to optimise Defence's preparedness posture[2] within financial guidance. Simply, Defence cannot, and would not, wish to keep all capabilities at high readiness for the full range of potential operational responses. Preparedness planning and management helps Defence to hedge, being cognisant of risk and understanding cost.

Defence Logistics must have the following capabilities and attributes to meet the demands of preparedness:

- it must be able to support the ongoing Raise, Train, Sustain (RTS) activities of Defence; which are largely planned, predictable activities, but which are not necessarily geographically constrained (engagement and exercise activities can be held throughout the region or further afield);
- it must be responsive so that it can support mobilisation for, and the conduct of, the full range of shorter-notice contingency responses – as articulated in the CDF's Preparedness Directive (CPD) and refined through the Quarterly Strategic Review (QSR) process; and

---

1 Readiness is the ability of a force element to be committed to an activity within a specified timeframe. It assumes the availability of appropriate competencies and other Fundamental Inputs to Capability (FIC) elements that provide an acceptable level of risk. Sustainability is the ability of Defence to maintain one or more of its elements for a prescribed function for a specified sustainability period at a level of activity required to achieve a nominated objective.

2 When describing how to adopt the appropriate preparedness posture, Defence refers to two complementary components:
- **Baseline** – the level of preparedness required to ensure that Defence can be brought to the required state to conduct joint combat operations for the Defence of Australia, within a specified strategic warning time; and
- **Additional requirements of Government** – the additional level of preparedness required to ensure that Government direction or expectations can be met.

- it must be capable of supporting mobilisation for, and the conduct of, the most demanding (Baseline) requirement for combined joint operations for the Defence of Australia.

Thus, Defence Logistics needs to balance the support required by a range of demands:

- from the planned RTS activities, for which efficient arrangements with low overheads and margins might be designed;
- through highly responsive short-notice contingencies, for which support inevitably requires additional capacity to allow surge, and which therefore impacts on efficiency measures; and
- the low likelihood, but highest consequence requirements for Defence of Australia. This no-fail requirement demands the capability of Defence Logistics to surge to support a mobilised and potentially expanded force-in-being, and the focus has to be on security of support, and capacity for assured growth.

WHAT IS THE CURRENT STATE OF DEFENCE LOGISTICS?

In order to examine the current state of Defence Logistics, the study focused on:

- Leadership of the Defence Logistics environment.
- Current Defence Logistics challenges.
- Capability Managers demands on Defence Logistics.
- The integration of the Fundamental Inputs to Capability.
- Managing Enterprise Risk.
- The Defence Logistics Strategy 2010-2015.
- The Defence Logistics Transformation Program.

Leadership of the Defence Logistics Environment

The Defence Logistics domain is viewed by many as being fragmented and lacking a holistic approach, to not only the domain itself, but the broader environment in which it operates. This is the unintended consequence of a failure to assign appropriate responsibility and authority for an essential Joint function with the result that no one individual has the authority to take a systems view of the whole Defence Logistics domain.

Defence logistics integration, coordination and modernisation are key undertakings of Commander Joint Logistics (CJLOG) who has been appointed by the Chief of the Defence Force as the Defence Strategic J4. Vesting this accountability for shaping the logistics capability under a single appointment provides an avenue for significant benefits and efficiencies. However, these benefits can only be harvested through close working relationships with all Services and Defence Groups, as well as Industry. Although CJLOG exercises technical authority across the Logistics enterprise he has not been appointed as the Defence Logistics 'capability manager' with the inherent responsibility and authority that would accompany such a title as in the case of

existing capability managers. He is in fact the 'capability coordinator' for Defence Logistics and does not have responsibility for, or oversight/authority over, all parts of the Defence Logistics domain.

The reason why this has not occurred can likely be traced to the cultural and historical tensions between the role of the Single Service Capability Managers (the Service Chiefs) and that of the emerging Joint Commanders and Group leaders. In order to defuse such tensions, the artifice of calling the Vice Chief of the Defence Force (VCDF), and other joint appointments such as CJLOG, 'capability coordinators' has been adopted. In the case of Logistics, there is growing evidence that the appeasement of internal tensions has in fact created an organisational dysfunction that currently limits, and will continue to limit, the operational effectiveness of the capabilities that the single Service Managers are actually responsible for. The persistence of this artifice is a reflection of a lack of organisational flexibility within the Department of Defence.

The Defence Logistics domain is viewed by many as being fragmented and lacking a holistic approach, to not only the domain itself, but the broader environment in which it operates.

Consequently, the Defence Logistics domain is viewed by many as being fragmented and lacking a holistic approach, to not only the domain itself, but the broader environment in which it operates. This comment in no way seeks to diminish the important role of CJLOG, nor the highly effective manner in which he and the Joint Logistics Command (JLC) executes their tasks. Rather, it highlights the unintended consequence of a failure to assign appropriate responsibility and authority for an essential Joint function with the result that no one individual has the authority to take a systems view of the Defence Logistics domain. The resulting tendency to view the various aspects of Defence Logistics through component elements introduces operational, enterprise and financial risk to Defence as will be discussed in the remainder of this report.

Current Defence Logistics Challenges

A lack of priority afforded to Logistics over the past decade manifested itself in recent years as major problems in the Landing Platform Amphibious (LPA) and Submarine fleets, which in turn led to the more recent Rizzo and Coles reviews.[3] The Rizzo Report highlighted inadequate maintenance and sustainment practices resulting from poor whole-of-life asset management, organisational complexity and blurred accountabilities, inadequate risk management, poor compliance and assurance, a 'hollowed-out' engineering function across Defence, resource shortages in Defence Materiel Organisation (DMO) System Program Offices (SPOs), and a culture that placed the short-term operational mission above the need for technical integrity.

So what are the issues concerning Logisticians today? There are three issues that are of particular concern to many Logisticians: Defence Preparedness, the Logistics Information Management System (LIMS) and the lack of a coherent Logistics business architecture.

3 These are the two latest reviews into sustainment issues that involve logistics at the heart. See Paul Rizzo, 'Plan to Reform Support Ship Repair and Management Practices', July 2011; and John Coles, 'Study into the Business of Sustaining Australia's Strategic Collins Class Submarine Capability', November 2012.

Defence Preparedness. Preparedness reporting remains platform-focused and the availability of underpinning support capabilities can become obscured. Force readiness levels assume the availability of support from a wide range of FIC. However, such assumptions can be very optimistic; e.g., when considering limitations in supporting IT capabilities, Defence Estate and Industry.

- **IT Capabilities Limitations.** These limitations are not the result of negligence or incompetence, rather they are the result of how Defence views and prioritises capability. For example, the operating budgets of the Chief Information Officer Group (CIOG) have been static; the sustainment budget for the 33 key logistics applications has been flat for some years, with an annual allocation of $42m. The current IT systems are deteriorating and will need additional funds to enable continued use. Compounding the challenge of maintaining the existing systems is the Defence IT acquisition system. The system is bureaucratic, slowing projects that have short life-cycles with the result that business requirements and potential technical solutions take second priority to process. This makes evolutionary acquisition difficult because of the bureaucratic and administrative cost overheads and time lags.
- **Defence Estate.** Under-investment in Defence Estate as a result of funding prioritisation to equipment acquisition has resulted in significant deficiencies in facilities. If, for example, fuel storage facilities are deteriorating, it is difficult to maintain operational readiness and sustainability. Whilst this may appear to be a statement of the obvious, it is unfortunately a reflection of the less visible, yet essential, logistics capabilities that have suffered from under investment.
- **Industry Support.** Readiness levels translate well to training and other support requirements but sustainability analysis and reporting are less well-developed. Preparedness analysis does not incorporate issues related to industry support.

The LIMS. There are more than 33 logistics applications being managed by CIOG through a Service Level Agreement. The size of the LIMS domain has been subjected to considerable review in recent months, with the number of applications being reduced from more than 400 to 239 (of which 42 are considered core), with further reductions in train.[4] Currently, Defence's Military Integrated Logistics Information System (MILIS) is the single point of record for inventory, and is a priority focus for CJLOG and his Command. There are a number of challenges with MILIS and LIMS integration including:

- MILIS currently supports only the land and ground support elements for maintenance. Air Force maintenance and the maintenance of all Defence aviation elements are supported by a system called CAMM2. Naval maintenance is supported by the Asset Management and Planning System (AMPS). MILIS, CAMM2 and AMPS are not fully integrated and thus do not provide a single maintenance picture across Defence. It is worth noting, however, that these systems do not provide the same functionality and that while it is important to integrate CAMM2 and AMPS, there is already some limited integration between CAMM2 and MILIS.

4 Whilst this number sounds large, there are in the order of 4000 applications that the CIOG is attempting to rationalise across the whole-of-Defence IT system.

- CJLOG is focussed on the integration of maintenance applications and the development of real-time materiel maintenance capability and real-time inventory management systems linked to the core system at every point in the supply chain. However, upgrades have been delayed because the focus has been on ensuring that the core MILIS system is in a state where it is able to take on a large change in its functionality. Whilst some concerns have been expressed at the ability to sustain the existing MILIS configuration until the upgrades are delivered under Project JP 2077 Phase 2D, JLC does not consider this to be a high concern as contractual arrangements are in place with the vendor to address this risk.
- The intent under Project JP 2077 Phase 2D is to develop a more integrated maintenance system on a whole-of-Defence basis. The scope and design of that system is yet to be determined. JP 2077 Phase 2D has been delayed, possibly until 2018-2019. As a result of the delay, Defence will experience difficulty in providing integrated Logistics support to existing capabilities as well as new ones such as the new Amphibious Capability and the Joint Strike Fighter (JSF). This issue will be explored further, later in this report.
- Australia is likely to face increasing strategic uncertainty and increased budgetary pressures over the next decade. Any delay in developing a truly integrated and coherent Logistics system will translate into increased preparedness and operational risk and, in turn, increased Defence Enterprise risk. **It appears that this increased risk is likely.**

Logistics Business Architecture. An issue that arose during the Kokoda project workshops was the lack of an integrating Defence Logistics business architecture.

- The absence of such a business (not IT) architecture, makes the job of the CIOG in implementing an IT architecture to enable Defence Logistics somewhat of a challenge. It is like designing an electrical wiring circuit for a house without having the complete house plans. The issue is not one that is unique to the logistics domain. Parallels can be found in other Defence capability domains, particularly where there is no clearly identified capability manager to take ownership of a whole business domain.
- Given the lack of a business architecture, it is apparent that the rationalisation of the logistics applications is not really a CIOG / IT problem; rather, it is a business process problem. The 4,000 applications across Defence need to be reduced down to the fewest, most sensible number required, based on the need to reduce sustainment costs and improve business capability; thus, the strategic focus across the Department is now turning to applications rationalisation. This means it will be for JLC and CJLOG to drive the logistics community to reduce the large number of separate Logistics applications. However, without the authority and purview of a capability manager, CJLOG can only hope to influence and encourage such decisions across the Logistics enterprise as a whole.

Capability Managers Demands on Defence Logistics

Capability Managers are experiencing difficulties with Logistics support. Example issues are identified in the following sub paragraphs.

- **Levels of Logistics Support.** Logistics support operates at three levels – the transactional level, the organisational or operational level, and the strategic level.
  - **At the transactional level**, Logistics functions well; however, there are examples of over-servicing[5], "pipeline" problems (both forward pipelines, and especially delays in reverse pipelines) and local process work-arounds that solve immediate problems but tend not to be reported upwards, thus masking the nature and extent of problems that might be evidence of systemic issues.
  - **At the organisational level**, there can be areas of overlap of Logistics role responsibility, particularly when it comes to funding current activities and providing for forecast activities in the forward estimates. There is also the issue of centralisation versus decentralisation - while Air Force and Navy tend to use a decentralised logistics management model, Army manages in a highly centralised fashion. These differences cascade into the operating divisions of the Defence Materiel Organisation (DMO).
  - **At the strategic level**, problems arise where transactional issues can distract from strategic Logistics management. For example, there is a strong focus on transactional issues around land materiel maintenance and logistics information systems. Compounding this concern are the additional layers of soft governance; these are layers of overhead that are purported to be governance but are simply additional process steps. An over-emphasis on reporting rather than managing can exacerbate the problem. A strategic level vision and strategy, a concept and plan, and a statement of definitive outcomes would assist in improving Defence Logistics at the enterprise level.
- **Shared Services Issues.** There are also concerns over shared services, where the theory is about efficiency through consolidating resources, enhanced professional development for staff, and standardised service. While this can help improve service delivery, it can also, in times of funding cuts, lead to a reduction in services that impact the operations that the services are meant to support.

The Integration of the Fundamental Inputs to Capability

Any misalignment of FIC manifests as differences in the scheduled delivery of capability elements (e.g., where major equipments are delivered before the required infrastructure). The Landing Helicopter Dock (LHD) is an example of misalignment between the platform and the supporting infrastructure and IT, as these supporting resources are managed by enabling organisations and are independently funded (i.e., not through the Capability Manager). The impacts of misalignment can be degraded capability and availability, and in turn, increased support costs.

5 Over-servicing is defined here in terms of too much inventory being sent / demanded because of poor system-of-systems integration, customer demand behaviours, and where the demand is deemed to have been satisfied or where the item demanded is considered to have been consumed (particularly for expendable items). Over-servicing presents as an increased cost to the Capability Manager.

The main causes of misalignment include: the highly-matrixed Defence organisational structure; immature governance and agency arrangements; and the mismatch between a shared service culture and reality. The problem in such a highly-matrixed arrangement is a diffusion of accountability and responsibility.[6]

The power of the joint force is in its integrated form, not in the strength of the single Service components.

There are a variety of arrangements for support across agencies that suffer from differing levels of maturity and lack of consistency in internal governance and agency arrangements. For example, a DMO Materiel Sustainment Agreement (MSA) would have funds allocated by the Service / Capability Manager, while a DSRG Customer Supplier Arrangement (CSA) would be centrally funded with no effective prioritisation system that involves the customer. Furthermore, a DMO MSA generally only covers between two to three FIC elements, so there is a sense of disaggregated support for the Capability Managers and no system-of-systems view of logistics support.

While the issues are known at the working level, they tend to be filtered out as reporting moves up the chain of command. Endemic to the problem is that continual short-term fixes are applied rather than initiatives that flow from a long-term structured and orchestrated plan. Indeed, Defence does default to process and organisational form that produces a culture and behaviours that are inimical to addressing the systems level view.

This lack of integration at the FIC level also cascades down to a lack of fusion of the basic elements of logistics – engineering, maintenance and supply. The impact of this is that issues involving workforce, information systems, and logistics support concepts for example are not being brought together and considered holistically across all elements of logistics.

Managing Enterprise Risk

The Continued disaggregation of logistics manifests as enterprise risk in two ways: additional cost due to expensive work-arounds and a potential inability to support the future joint force. The power of the joint force is in its integrated form, not in the strength of the single Service components.

Defence Enterprise risk relates to the ability or inability of Defence to meet Government expectations in addressing the strategic risks faced by Australia. Facets of enterprise risk include Financial Risks, Capability Risks and Organisational Risks. Examples include if:

- the force-in-being is unable to deploy and be sustained on operations as required by the Government;

6 As an example of the matrixed Defence structure, in DMO alone there are 40 Navy Product Schedules (within the Navy / DMO Materiel Sustainment Agreements (MSAs)) with review and signature required that involve 22 SES Band 1 officers / military one-stars, 6 SES Band 2 officers / military two-stars and 1 SES Band 3. Furthermore, there are 38 MSA Products that Navy receives logistics support for but where Army, RAAF, or some other Group is the lead Capability Manager.

- the investment program cannot deliver the future force called for in strategic guidance;
- the workforce skills and number of personnel are insufficient to operate the force; and
- costs are not effectively managed.

The Defence Enterprise is more than the Groups and Services that comprise the organisation; industry elements are also embedded within the broader enterprise. So, in effect it is a hybrid Commonwealth/corporate organisation. Industry is key to providing communications, transportation, accommodation, garrison support and deep levels of sustainment, just to mention some of the functions.

Disparate pieces of information exist across this enterprise but might not come together until a crisis occurs. When an enterprise risk crystallises, it can cause significant operational, reputational and other damage to Defence. The Landing Platforms Amphibious (LPAs), which were unable to put to sea to support the Government's response to Cyclone Yasi, are an example of this, where the risks were not being managed at an enterprise level and the enterprise risk was not recognised until failure occurred. And that failure occurred in 'plain sight'.

There can be a tendency for Defence to become self-absorbed in its own complexity and so fail to see the external change that is occurring. This can mean that its organisational assumptions about external systems and structures can remain unchanged despite changes in that external environment. For example, assumptions in defence policy relate to strategic warning that informs both the preparedness levels of the force-in-being and planning for the future force. Strategic warning time, as a Cold War concept, has been accepted as ten years, which has not been realistic in terms of how the Force has been used in recent years.

Assumptions need to be continually tested. Mobilisation and preparedness assumptions need to be tested in terms of the reality of logistics support that can be provided within Defence and also by external providers. Defence's assumptions about availability of deep Original Equipment Manufacturer (OEM) support; and availability of stocks from wholesalers, distributors and operators tend to hold up in only some scenarios.

Logistics assumptions might, for instance, indicate that sufficient robustness in support can be achieved over four years (i.e., shortfalls can be remediated and alternative sources of supply identified), which would fit neatly within a ten-year warning time for a defence of Australia scenario, but not for a 'come as you are' deployment to a crisis that emerges at very short notice. Furthermore, the advent of global supply chains means a number of Defence's traditional assumptions need to be re-visited.

Improvements in supply chain management have led to much thinner supply chains within individual companies but also across whole sectors than previously, and while that works well in normal times, these supply chains can be disturbed through modest unforecast perturbations.[7] These disruptions can quickly propagate across interdependent areas. The Thai floods in 2013 are a case in point that demonstrated

7 An excellent discussion of supply chain risks is contained in the World Economic Forum Report: "Building Resilience in Supply Chains" published in January 2013.

the rapid and widespread disruption to global automotive manufacture from a local Thai disruption. Resilience is a peacetime construct that can quickly unravel in times of conflict or crisis.

Thus, business intelligence around the total supply chains of all suppliers is as important to Defence as business intelligence around its Groups and Services and its internal business model. New assumptions are needed that address the reality of global supply chains – that stocks might not be available when Australia needs them, such as Precision Guided Munitions (PGMs). How would Australia obtain more at a time when a number of other countries wants them?

Consequently, Defence's approach to enterprise risk should highlight any systemic under-investment in enablers, such as logistics, and also highlight the changing external environment around global supply chains and stockholding levels. Plans are needed across the expanded enterprise to manage such risks, to improve resilience, and to ensure that surge capacity is there when needed.

The challenge is for Defence to be able to cater for the discretionary activities that can be carried out within the capacity of the current force, such as humanitarian assistance and disaster relief; and to be able to mobilise, as necessary, to deal with a defence of Australia situation. However, there is a plethora of other potential crises that sit in between these two points in the spectrum that, unless at least thought through in broad scenario terms and tested against an informed understanding of global supply chains, would challenge Australia's ability to ramp up and respond in a self-reliant way.

The strategic logistics issue is that Defence has not absorbed the impact of globalisation, especially in terms of technological interdependence flowing from the changing nature of supply chains in companies and across whole sectors as discussed above. Even high-end systems with their own sophisticated integrated logistics and capability management systems like the Joint Strike Fighter (JSF) are not stand-alone capabilities. They have interfaces with the broader ADF and its logistics support.

Establishing interdependencies between such systems and platforms is a necessary first step in building a strategic logistics capability that takes a whole-of-enterprise view. Adding the deeper understanding of the dependencies that Defence Logistics has on relevant external supply chains would allow defence decision-makers to make informed investment decisions in logistics, instead of decisions that optimise only parts of the Logistics enterprise and thus have uncertain second-order consequences.

Continued disaggregation of logistics manifests as enterprise risk in two ways: additional cost due to expensive work-arounds; and a potential inability to support the future joint force. The question here is how can Defence support an integrated force to achieve operational efficiency? After all, the power of the joint force is in its integrated form, not in the strength of the single Service components.

The Defence Logistics Strategy 2010-2015

Given the issues identified in this study it is worthwhile reviewing the Australian Defence Logistics Strategy for 2010-2015, to see if the strategy and the associated implementation plan will remediate the challenges identified in this report.

The Logistics Strategy did highlight how logistics support was essential to operational success but that it also had to be provided in a cost-effective manner. Of note, one of the strategic themes was the Defence Strategic Logistics Reform Program that was to be driven through the Defence Logistics Services Project aimed at improving wholesale storage and distribution, modernising land materiel maintenance, and adopting automated identification technologies. This was translated into the Defence Logistics Transformation Program (DLTP), which clearly is something of a misnomer, as discussed in the following paragraphs.

The Logistics Strategy noted that it was important to understand logistics as an overall system, so it does seem odd that the DLTP was focussed only on three aspects of that overall system. The Strategy also noted the need to build resilience at the same time as driving down cost. Again, this seems to be an odd way of achieving genuine reform (i.e., improvement) in resilience.

There was a lot of good work that went into the Logistics Strategy; however, the re-badging of a genuine transformation program into a savings (or efficiencies program) has conspired to undermine the ability to truly transform Defence Logistics. Furthermore, there has also been an inordinate focus on inventory control, driven mainly by adverse audit findings from the Australian National Audit Office and qualification of Defence accounts in past years, which has detracted from addressing macro and more encompassing logistics reform.

There are four main Logistics deficiencies that are being addressed by Defence within the Strategy. The initiatives are:

- establishing greater links between Logistics and capability development;
- addressing the specific Logistics aspects of DMO's role and its sustainment responsibilities;
- establishing greater links between Logistics and infrastructure requirements; and
- establishing greater links between Logistics and the expectation of the preparedness management system.

It is worth noting, however, that these initiatives are all internally focused and frankly the Strategy is in need of updating to address the systemic deficiencies in the Logistics structure, organisation and process which currently constrain the effective management and development of the Defence Logistics capability. Furthermore, an updated Logistics Strategy needs to flow from an overarching Defence Strategy that aligns all Defence areas.

The Defence Logistics Transformation Program

The DLTP has thus become a reform initiative rather than a strategic initiative. Furthermore, any real system efficiencies/savings are unlikely to be fully realised until the integrating information systems layer (JP 2077 Phase 2D) is in place.

While the authors are concerned over the limitations on realising the full potential of efficiencies until Phase 2D is implemented, they do acknowledge that some efficiencies have been realised in the disposal of neglected, obsolete and overstocked inventory; rationalisation of business processes; reduction of fuels and dangerous goods holdings; and improved policy for holdings of slow-moving and life-of-type stock. Savings have also accrued from personnel reductions, re-negotiated contract prices, and improved leasing and on-cost arrangements for storage areas.

An example of the tendency to approach Defence Logistics as component elements is the DLTP. The DLTP was initially envisaged as a broad program extending across the full gamut of logistics support. However, the focus has been diverted from this more holistic goal to a much narrower focus on efficiencies in the three main areas of warehouse storage and distribution, land materiel maintenance, and automated identification technologies.

The DLTP has thus become a reform initiative rather than a strategic initiative.

The focus might improve warehousing distribution and land systems maintenance support but there will frankly not be any overall logistics transformation. The DLTP has thus become a reform initiative rather than a strategic initiative. Furthermore, any real system efficiencies/savings are unlikely to be fully realised until the integrating information systems layer (JP 2077 Phase 2D) is in place.

WHAT ARE THE FUTURE CHALLENGES FOR DEFENCE LOGISTICS?

Success in the future joint logistics environment will come from aligning the efforts of Defence agencies, the industrial base, non-government agencies, national support, and Australia's interagency and multinational partners.

Trends and Drivers

As the ADF deals with the security challenges of the future, it will need to optimise the Logistics 'footprint' in Areas of Operation (AO) and decrease the size of the Logistics 'tail'. The paramount goal for the military logistician is to provide responsive, agile Logistics to support military operations in an effective and efficient manner. A critical requirement is that Logistics must operate similarly in both wartime and peacetime environments, across the full spectrum of military operations.

Changes affecting Logistics will occur in environments, technologies, processes and the workforce leading toward the development of more dynamic responsive Logistics. Environments will change in the military, commercial, and logistics sectors. Technologies will change in information technology and systems, packaging and

battlefield delivery, and integrating Logistics operations. Processes will change in materiel requirements, maintenance, and financial management. The workforce will change in terms of its age structure, its role (as technology, outsourcing and other changes impact), and its required competencies.

These changes will attest to the fact that the dynamic relationships among Logistics elements will reshape the future structure of Logistics. These dynamic relationships will be formed through a combination of synergy and balancing activities among Logistics elements. Logisticians recognise that numerous trade-offs will occur between Logistics processes. Rapid transportation allows for frequent inventory replenishment, thereby lowering inventory levels and reducing the need for warehouses. Precise delivery of information will reduce the uncertainty associated with inventory.

There will be constraints on the extent to which improvements in Logistics can be realised as budget, industry policy, operational requirements, priorities, levels of interoperability, and environmental factors will all come into play.

While the challenges for the Australian Defence Organisation (ADO) can be deduced from these trends and drivers of change, a number of significant and specific challenges for future Logistics support are:

- **Globalisation.** Multi-national organisations are establishing supply chain arrangements that aim to increase profitability, which challenge national sovereignty and assured Logistics support to the war-fighter. This challenge also includes global sourcing of components and the risks of non-supply due to disruption or dispute. The impacts of globalisation must be made as relevant to the ADO as they are to suppliers.
- **Performance Based Logistics and Performance Based Contracting**. There are significantly fewer Original Equipment Manufacturers (OEMs) as a result of global industry rationalisation in the last decade and a half. In an effort to improve Logistics support, there has been a tendency to use the OEMs as prime contractors responsible for delivery of weapon system Logistics support; although recently, there have been concerns that structural cost issues might limit OEM sustainment in future. Management of system manufacturer Logistics support is carried out through Performance Based Logistics and Performance Based Contracting (PBC).[8]
- **Supply Chain Reform.** A supply chain is a network of facilities and distribution options that performs the functions of procurement of materials, transformation of these materials into intermediate and finished products, and the distribution of these finished products to customers. Supply chain management is undergoing continuous development in an effort to provide the required level of support at the least cost. ADO logistics areas are focussing on effecting improvements to their systems and processes to better support the war-fighter. To this end, the ADO is looking at adopting various supply chain reforms being introduced in the commercial sector. The adoption of these supply chain reforms can have profound effects on how the ADF operates and how it is logistically supported. In this respect,

8 PBC offers the ability to: transform the approach in contracting from process / outputs / activities to one that focuses on outcomes and performance; develop a culture of greater cooperation and goal convergence between Defence and Industry by aligning contract rewards to capability outcomes; and drive 'best practice' by encouraging cost-effective and sustainable support solutions.

the focus of Defence Logistics must be on managing core Logistics processes and using innovative ways to achieve best-commercial-practice Logistics outcomes. Simplifying maintenance and adopting right-sized inventories are two key initiatives in this regard, which can be supported by the PBC framework.

- **Weapon Systems Technology.** New technology will change both the nature of the Weapon Systems and their Logistics support. New technology will require changes to existing systems or require new systems in order for the ADF to remain operationally effective. Additionally, changes in weapon system design will alter where and how maintenance is performed. Similarly, the increasing use of unmanned systems will present new challenges in Logistics support.
- **Logistics Information Technology.** The further pursuit of a network centric approach to war-fighting, miniaturisation, availability of faster processors, greater memory capacity, and reductions in hardware costs are seeing a trend for increased use of information systems and decision support tools. Additionally, new Logistics information systems will have a profound impact on Logistics delivery and business practices. The challenge will be to exploit these technological improvements without becoming overly dependent on information systems, recognising their limitations and vulnerabilities.[9]
- **Demographics and Workforce.** The number of people available for skilled Defence jobs will decline and competition for these people will be intense. The type of work undertaken will also change, as will the demographic profile. A strategic approach to workforce management will help to ensure the Logistics workforce can meet its mission. Effective workforce planning, recruitment and development strategies are vital. A career structure, certification framework, and critical skills shortages all need to be addressed.
- **Governance Issues.** The cumulative impact of the foregoing challenges combined with the risk of uncoordinated implementation of reform and efficiency initiatives have the potential to undermine the ability of Defence Logistics to meet its directed outcomes. Creation of new governance structures provides an opportunity to ensure Defence Logistics governance is consistent with whole-of-enterprise governance and risk management for the future.

- **Future Logistics Delivery.** The increasing tempo of operations demands more dynamic and responsive Logistics support and adoption of lean Logistics initiatives as well as networked distribution-based Logistics. Future Logistics delivery to the war-fighter must also provide agility and modularity; utilise open standards, e-business and e-portals; and minimise risk through its networked distribution-based focus.

9 For the future, Logistics IT systems should encompass Radio Frequency Identification (RFID)/Unique Identification (UID) as appropriate, Total Asset Visibility (TAV), connected best-of-breed decision support systems, and be better-integrated with other Enterprise Resource Planning (ERP) capabilities.

Managing the Future Logistics Environment

The supply chain leadership challenges are becoming increasingly complex. The future environment will likely be characterised by constant change with increasing levels of uncertainty and ambiguity. The Logistics challenge is to drive down cost, while at the same time, build a degree of resilience to hedge against risk of interruption to supply.

The actions that deliver Logistics support are steps in a long, interrelated and highly complex chain of activity. Logistics, therefore, needs to be understood in terms of an overall system-of-systems. The delivery of Logistics is via organic Logistics elements within each of the Services, supported by a complex network of Defence service providers, industry and international agreements.

Adding to the complexity is the need to tailor supply chains to suit the specific needs of operations as well as ensuring the proper support for capability systems across their life-cycle and the need to integrate into global supply chains.

Success in the future joint Logistics environment will come from aligning the efforts of Defence agencies, the industrial base, non-government agencies, national support, and Australia's interagency and multinational partners to further develop and refine Logistics support. Defence Logistics will become more efficient and effective when all Logistics partners and stakeholders are aligned, interoperable, can leverage all support available, and are synchronised such that the support provided is optimised.

The challenge this emerging new era in Logistics poses makes it critical that the ADO charts the course of Defence Logistics in the coming years by encouraging innovation and by ensuring there are Logistics champions at the right level to lead the effort to implement continuous improvements to business practices, Logistics processes and the underpinning Logistics information systems within the Defence Logistics support environment. It is also critical to identify and manage ongoing constraints such as funding, manpower and skills, ensuring that any trade-offs are carried out in an informed and risk-managed manner.

WHAT CAN DEFENCE LEARN FROM OTHERS?

Transformation Models

As enterprises seek to transform themselves, and upgrade their business systems to improve their organisational impact, they tend to move through several levels. At the first level, they focus on systems consolidation (simplifying/consolidating systems around a common platform) which leads to IT-run savings and reduced risk. At the second level, they focus on process integration (streamlining and standardising processes on common standards and automating through enterprise technology) that leads to improved efficiency and effectiveness. At the third level, they focus on using Enterprise Resource Planning (ERP) to achieve organisational optimisation (this is not just about an overarching ERP but also requires shared services, performance management, continuous improvement, and so on), which leads to operational excellence. At the fourth level, they focus on innovative capabilities (building differentiated capabilities, enabled by new technology, business processes and operating models that lead to advanced performance).

Different organisations will have varying program goals, depending on their level of maturity. Whatever the program vision – savings and reduced risk, improved efficiency and effectiveness, operational excellence, or advanced performance – the same broad technology trends will pertain. These include:

- Relationships at scale: moving from transactions to interactions.
- Design for analytics: this is no longer about a lack of data but a lack of the right data.
- Data velocity: matching the speed of decision to the speed of action.
- Seamless collaboration: embedding collaboration into the business process.
- Software-defined networking.
- Active defence: adapting defence to the threat.

Adopting a Portfolio Management Approach

Effective risk management of large enterprise-level IT systems leads organisations to adopt a portfolio management approach, thus allowing a more effective governance mechanism to be put in place from the start. The US Defence Logistics Agency (DLA) adopted such an approach as its focus moved over time from managing efficiencies for common items in the 1970s / 80s to better linking supply and demand in the 2010s by leveraging ERP capability, strategic network optimisation and performance based logistics. This was all about integrating functions to achieve effectiveness and efficiency through a portfolio management approach.

Effective risk management of large enterprise-level IT systems leads organisations to adopt a portfolio management approach.

The DLA saw the need to speed up the process of providing logistics support and to reduce cost and as it started its business transformation/ERP initiative, the DLA moved its management focus at the portfolio level on to the initiative. The DLA recognised that a logistics ERP that centres on inventory control must be able to deliver: real-time response and thus reduce customer wait time; be financially compliant; be a modern system and thus less expensive to operate; ensure data integrity; and provide improved forecasting which means less inventory. Replacing an IT system is relatively easy – it is the change management issue and culture change issues that create most of the problems. There are also issues around training people on the new systems and the impacts on business processes.

Transforming Logistics Information Management Systems - Commercial Trends

Those far-sighted organisations that are recognising IT as a strategic asset with which they can renew vital aspects of their operations — optimising at least and innovating at best – are increasing in numbers. These organisations are investing in the digital tools, the capabilities, and the skills to more easily identify useful data, evaluate it, excerpt it, analyse it, derive insights from it, share it, manage it, comment on it, report on it, and, most importantly, act on it.

It is no longer possible to separate 'the technology' from 'the business'; the two are too tightly coupled. IT helps redesign the company's products and services or the

government agency's outcomes and outputs and supports their processes, drives their supply chains, becomes part of the products/services or outcomes/outputs themselves and creates new ones, allows access to new customers, and provides the frameworks to create new offerings.

This is about transformation in the coupling of business and IT. It is a question of integration, and there are some key challenges apart from the technology itself that are discussed below.

Transformation Challenges

Transformation is not just an IT issue. The key challenges that all organisations face in managing transformation include:

- **Governance** – how does the organisation move to a centralised system approach in delivering IT that allows the business to focus on the business (such as engineering capability or maintenance capability)? This also involves practical governance around constraints, such as support costs. Perhaps the most significant governance challenges are those related to security and privacy.
- **Information management -** distributed data requires good master data management, which is the foundation for better analytics and for managing data privacy – two crucial differentiators.
- **Architecture** - business needs should be the prime motivator for adopting new technologies. Decoupling system architecture from infrastructure architecture increases agility, allowing quicker responses to market changes. A focus on analytics will help the IT organisation to become a close partner with business units in making better decisions that lead to improved business outcomes. .
- **Design for analytics (business intelligence)** - organisations are no longer suffering from a lack of data; they're suffering from a lack of the right data. Business leaders need the right data in order to effectively define the strategic direction of the enterprise. The current generation of software was designed for functionality: the next generation must be designed for analytics as well.
- **Approach** – is it a big-bang approach or is it a staged step-by-step process to integrate? Is there a roadmap that leads to the desired end-state? The challenge is to articulate roadmaps that deliver continual value.
  - **Strategic IT alignment** - in the past, alignment referred to how the IT organisation served the business's needs. New trends and their accelerated pace shift the alignment emphasis to educating the business about what new technologies can do and how IT can help improve execution of the chosen strategy. In that way, the IT function can move from its focus on service-level agreements and costs to being a creator of value. The design should be around the capabilities of the future (technology component) and the vision should support the changing needs of the business (business component). [10]

10 This raises three sub-questions:
- Justification – are there business cases that support the steps to integration?
- Integration – is the focus on the technology or is it on how the business needs to integrate?
- Over-integrating – should everything be integrated? It is important to determine the outcomes sought from integration and not to over-specify what has to be integrated.

- **Information security** - despite an increasing focus on securing the digital business, IT departments struggle to keep pace with recent advances in security technology. Enterprises know that endpoint security is not enough, but the move to active defence - risk-based approaches to security management, analytics-driven event detection, and reflex-like incident response - isn't yet happening on a broad scale. Although these technologies are maturing rapidly and communities are forming to expose risks, the biggest barrier is slow adoption of solutions that already exist. IT's core challenge is to become current with best practices in security while getting smarter about the new active-defence possibilities.

WHAT CAN BE DONE TO IMPROVE DEFENCE LOGISTICS?

There is considerable effort and energy being expended by teams of dedicated people in Defence to improve the Logistics enterprise. The question that needs to be answered is whether the actions underway will be sufficient to address the current and future challenges and whether organisational issues are impeding these efforts.

This section of the report will discuss potential improvements to assist in addressing Logistics challenges. Specifically, it examines the utility of:

- Complex Systems Engineering.
- Logistics Capstone Concepts.
- Smart Sustainment Programs.
- Sustainment Analysis in Project Development.
- Logistics Change Management.
- Resilience and Global Supply Chains.
- Addressing the Logistics Information Management Challenges.
- Information Security.

Complex Systems Engineering

Defence Logistics is a complex problem and complex problems are usually poorly structured because of the myriad of interacting issues and need to be tackled strategically. A key component of such a strategic approach is recognising that issues do not exist in isolation. This also requires the inter-related nature of circumstances to be recognised *up front* rather than relying on a *post hoc* screening to identify unintended consequences and impacts.

Systems' thinking is particularly powerful for understanding dynamic complexity, which stems from the relationships between factors in a system. It allows vital questions and concerns to be raised; relevant information and abstract ideas to be interpreted and assessed; open mindedness in arriving at well-reasoned conclusions and solutions; and

effective collaboration and communication with others in solving complex problems. So many important logistics problems that plague Defence senior managers today are complex, involve multiple actors, and are at least partly the result of past actions that were taken to solve them.

One of the disciplines that can be used in dealing with complexity is Complex Systems Engineering (CSE), which changes the focus from "...here is the solution designed from the requirements, now go implement it..." to "...here are the selective pressures acting on the elements present, now resolve or reduce them..." Complex supply chains will not only be here to stay but will evolve further. There will be niche markets, niche companies, and thus a diverse range of suppliers with differing requirements and expectations and they will change rapidly; all of which adds to the complexity. Different support systems will have different life-cycles, which will add further to the overall complexity. The principles of CSE may have some applicability for Defence Logisticians attempting to address the growing complexity of Logistics support and supply chains.

Logistics Capstone Concepts

Capability Development Group (CDG) are building a better understanding of the implications of logistics on future capability in order to be the lead into the smart sustainment initiative.[11] When CDG develops a business case for a project, they are now required to consider all aspects of the capability, including the logistics support arrangements; however, there is a paucity of logisticians in CDG to perform these tasks. They are also required to consider whole-of-life costs by including Net Personnel and Operating Cost (NPOC) estimates. This is likely to lead to a need for a better effects-based framework at the strategic level that will have real impact on the Department's costs and capability considerations.

In the main, Logistics has tended to be considered from a project level rather than from a program or enterprise level. Thus, the logistics support is optimised for the platform rather than for the wider ADF. The JSF project is a good illustration. All spares are globally owned and shared by JSF partner countries, which has the potential to generate significant economies of scale through a global pool of spares and the cost of running a few global repair facilities. However, for the first time in decades, the ADF will not be able to use a common inventory system for all of its logistics transactions.

11 Smart sustainment was one of the principal streams of Defence's Strategic Reform Program. This reform stream recognised that the real cost of staying on or ahead of the technology curve with specialist military equipment would continue to rise, ADF operational demands would remain high, and the economic downturn would continue to intensify pressures on Government funding. All of this meant that there was a clear need to focus on the affordability as well as the effectiveness of defence equipment; and that Defence, DMO and Industry needed to improve productivity to maintain or enhance supply levels at reduced cost.

This arrangement might be optimal for JSF; indeed, the JSF might not have been affordable otherwise. [12]

CDG has embarked on several important initiatives to improve decision-making in the future, including for logistics related matters:

- This first is in terms of integration, using Project Integration Needs Statements (PINS) to inform committees. There are three formal points to input integration issues / risks into the approval process via PINS – they are used to inform committee approval at the Project Initiation Review Board (PIRB) after the Needs Phase; at Government First-Pass Approval during the Requirements Phase; and at Government Second-Pass Approval at the end of the Requirements Phase. The PINS assessments look at organisational and technical interfaces around a number of categories, one of which is 'Support and Facilities' that includes logistics. Thus, CDG is obliged to consider logistics aspects of all projects that are reviewed. However, greater attention could be paid to this category in future; in particular, in terms of integrating this work with the work currently being undertaken by JLC's Strategic Logistics Branch for Defence Capability Plan (DCP) projects.

The PINS assessments look at organisational and technical interfaces around a number of categories, one of which is 'Support and Facilities' that includes logistics.

- A second initiative is the inclusion of Defence Operations and Enablers Functions (DOEF) in Operational Concept Documents (OCDs) to drive early consideration of project interdependencies (including FIC). Input from logistics stakeholders, particularly CJLOG, will make this something of a roadmap for projects considering their logistics support concepts. Perhaps it will also inform some architectural decisions for logistics IT systems.
- A third initiative is the risk management work that will allow CDG to move from a lag to a lead approach, which will involve shifting 'culture' and preferred behaviours to link all decisions to documented risks or opportunities. This will also promote documented recognition of logistics interdependencies.
- A fourth initiative is to learn from the Rizzo Review around the replacement of aging platforms, based on a clearer understanding of cost-capability trade-offs, which has relevance in CDG considerations.

---

12 The JSF Logistics System raises issues such as :
- A performance based contract, presumably with significant provision for liquidated damages will not mitigate the operational risk should spares be unavailable through supply chain disruption, cyber attack or prioritisation to another partner.
- The model requires a larger 'footprint' for the JSF's Autonomic Logistics Information System (ALIS), including system-specific operators, competing demands for bandwidth and power, and the lack of flexibility or redundancy to support one weapon through the IT system of another.
- The end-to-end assurance of the supply chain will be difficult to achieve. There has to be a cross-over point for the inventory at which Defence becomes accountable. Currently, Defence's MILIS is the single point of record for inventory, and it is difficult to ascertain how MILIS and ALIS will be integrated, notwithstanding Defence's intention to extend the range of Service Oriented Architecture integration points into MILIS to support initiatives such as ALIS.
- Logistics situational awareness will be difficult to provide.

So, what could be of use to CDG in addressing the Logistics implications of the future force? The addition of Logistics "capstone concepts" for combat systems that can be tailored to guide projects more consistently, while maintaining an integrating enterprise/program view of Logistics, could be of benefit. For example, LAND 400 provides an opportunity to utilise a capstone concept approach as it will have to integrate multiple sub-systems, and therefore multiple Logistics arrangements.

Improving Logistics Support through Smarter Sustainment

Smart Sustainment is exposing the costs of maintaining older equipment and the relationships with introducing new platforms into service. There is a bathtub-curve effect where costs are usually high as capabilities and equipments enter service and then there is a period where maintenance costs stabilise. Toward the end of the life-cycle, obsolescence issues and aging problems arise, wear and tear and structural fatigue increase, and costs go up. Deferring the planned withdrawal date causes substantial problems in terms of maintenance planning and constraining costs.

Changes in the contracting model are proving to be a challenge. For example, moving from a highly input-based contract where Defence has a say over everything that happens in the contract on an almost day-to-day basis, to a performance based contract where the contractor delivers an outcome for a particular price, means Defence has to move its workforce from managing that day-to-day hands-on activity to an output-based contract which requires a very different skill-set.

It is important to improve guidance on acquisition strategies to increase the emphasis on the design of Logistics support so that Defence ensures that future projects are designing support for life-of-type efficiency as well as effectiveness, and thinking through the myriad of issues that will impact cost.

The DMO currently oversees over 100 sustainment agreements with the Capability Managers, and manages the work output of contractors covering the maintenance and support of almost every Defence platform and system. It is the number of those agreements, their scope and complexity that point to the scale of challenge in implementing reform. There is no question that productivity has to be added to performance so that the DMO contracts for efficiency as well as effectiveness, and that is one of the key benefits from Smart Sustainment.

The Smart Sustainment initiative is focussed on the right outcome – that of moving the current workforce from doing a lot of transactional work to a more strategic focus and to help DMO develop a strategy for moving from a focus on transactional work to a far more strategic business approach to sustainment and logistics support. This more strategic approach to sustainment means that the DMO should be able to provide Capability Managers with more informed cost/availability trade-offs for their consideration.

The Need for Ongoing Sustainment Analysis

As the Rizzo Report argued, achieving effective sustainment in future necessitates adequate whole-of-life asset management, organisational simplicity and clear accountabilities, adequate risk management, strong compliance and assurance, an effective engineering function, sufficient resources in the DMO SPOs, and a culture that places technical integrity above any short-term operational imperatives

in peacetime. In addition, the Capability Managers and the DMO must be well-coordinated and well-integrated if asset management across the Capability's whole-of-life is to be as effective as it can be.

The strategic actions recommended in the Rizzo Report will assist in the further development of maintenance concepts for the sustainment of future capabilities. The need for the sustainment of assets must be given the same rigorous attention as asset acquisition because sustainment costs can significantly exceed those of the original procurement and the challenges can be more complex. Many of the causal factors for poor sustainment do not result from an inadequacy in any one function, such as engineering, but in the effectiveness in integrating the grouping of related functions such as operations, operational planning and culture. Effective sustainment is a partnership between the Capability Managers and the DMO across the entire capability life-cycle.

Defence has a mature capability life-cycle in-place and whole-of-life asset management can be effected through the current process. However, Defence needs to inject mature sustainment aspects into all phases of the life-cycle, such as at pre-first pass, pre-second pass, before acquisition, and as a fundamental part of introduction into operational service. Furthermore, the way in which the asset is operated can have significant effect on sustainment, especially maintenance planning; hence, operators must consider the sustainment implications of their operational actions.

Industry is a key factor in delivering effective sustainment and reducing bureaucratic and administrative overheads; short-term and narrow approaches to Industry engagement cannot be allowed to compromise this potential. Hence, in principle, the fewer the contracts and the longer-term the relationship with Industry, without compromising competitive tension, the more effective sustainment can be.

The Capability Managers must have clear accountability for through-life capability, together with the corresponding resources. The MSA between the Capability Managers and DMO is critical in this regard in establishing an effective collaboration, but it must be an active 'contract' that clearly defines the obligations of both the Capability Managers and DMO and that is supported by business-like performance measures; measures that are meaningful for each party and the shared outcome.

Like all organisations, Defence is influenced by external factors that impact on the organisation's appetite for risk. Risk decisions made at the Capability Manager level need to be accompanied by a robust mechanism for risk management spread horizontally throughout the organisation and vice versa. This means that individual technical risk assessments associated with the deferral of maintenance or acceptance of technical defects cannot be made in isolation. It is essential that decisions are made through consideration of the full range of risks to the capability, platform, product and operators, aggregating the information to provide a complete view over time.

The assessment of risk must also consider the benefits to be gained and the current context. For example, technical risks associated with reduced maintenance may be acceptable at a time of imminent threat, but according priority to a routine operational mission or exercise, ahead of serious cumulative shortfalls in maintenance, is not.

Defence must have a robust engineering function in-place to ensure that engineering influence is effective, adequate personnel and skills levels are maintained, a strong and effective compliance and assurance function is maintained, and a cohesive and aligned workforce is in-place. All of these, and more, are necessary to ensure that the prevailing culture does not become subservient to short-term operational imperatives and recognises the need for ongoing sustainment analysis.

The Need for Logistics Change Management

A consistent materiel flow is paramount if operational effectiveness is to be achieved. Materiel flow from industrial production through to the point of consumption / installation takes place through a dynamic network of supply chains. Ownership, operation and use of individual physical elements of this network are governed by one principle: constantly seeking to maximise immediate and future operational effect by streamlining, synchronising and integrating the logically separate flows within the network. This principle applies to the support of all military activity, from recruit training, through to routine maintenance, through to immediate operations in Australia and overseas. This is all about assurance of delivery.

A commercial enterprise does not realise the value of its investment until it makes a sale in the market place. With this in mind, Defence does not realise the value of its investment until it delivers a defined and measurable effect in the battlespace (readiness and deterrence are effects; albeit the second is harder to measure).

Materiel is a tangible measurement of investment. It is an expense as long as it remains within the enterprise. It can only have potential value when a sale is made, or in the military case, the effect is delivered. There is a balance to be maintained between the investment in materiel and its potential value in contributing to useful effects. This balance is dynamic because the determinants of value are themselves dynamic: e.g., the utility of materiel may fluctuate over time, depending on the nature of operations planned; or in commerce, depending on the changes in demand in the market. Hence, forecast accuracy and demand variability are the greatest obstacles to achieving supply chain goals.

Any transformation requires the whole business to change step together. In the inventory management space, the primacy of the principle of ownership and therefore accountability tends to drive decision-makers into separate enclaves. They can cooperate, but change takes enormous energy and therefore often fails, and actions become sub-optimised. This is also exacerbated by lack of portfolio governance.

This helps to explain why many people believe there are shortcomings in the overall Defence Logistics enterprise. The current focus on the project or component level will impede any transformation effort as it cannot possibly address the ability of the Logistics enterprise to deliver the required outputs with the required resilience at an acceptable level of risk. The project focus prevents the organisation from evaluating that risk.

With a focus on the materiel flow and not the materiel itself, Defence can step outside and above the supply chain, and relate every action within the supply chain to a target at the point of delivery of effect. In this way, everyone becomes focused on the same goal – assurance of delivery. This also leads to greater resilience and improved risk management.

To realise this change in perspective Defence needs to raise its sights from simply managing physical things to also managing information. If Defence can get the flow of information right, the flow of materiel will be as good as it can be within the physical constraints and resources applying at the time. Also, good information flow will expose the constraints on genuine improvement, which really is an iterative process.

Whilst a paradigm shift from cost to value is not difficult to understand or to accept as valid, the difficulty lies in understanding and embracing the implications of change and why change management is crucial.

Resilience and Global Supply Chains

The global nature of supply chains combined with efficiency changes has led to increased systemic risk and reduced resilience in some cases. Defence needs to take a fresh look at Enterprise risk assessment and the changing nature of logistics support.

Significant changes have occurred in supply chains over the last two to three decades as initiatives such as just-in-time inventory management and lean manufacturing techniques, amongst others, have been pursued to reduce overhead costs. This ensuing leaning out of supply chains, while financially logical, has led to increased overall risk and reduced resilience. Indeed, new risks have been introduced – these are often described as systemic risks because they result from how a system changes as a whole, when parts of the system are changed in an uncoordinated manner. An example of such a systemic risk is fuel supplies as discussed in the NRMA Report – Australia's Liquid Fuel Security Pt 2.[13]

A Systemic Risk Case – Australia's Fuel Supply Resilience.

Australia's combined dependency on crude and fuel imports for transport and Defence purposes has grown from around 60% in 2000 to over 90% today. While our 'just in time' oil and liquid fuel supply chains work well under normal circumstances or during small scale or short duration interruptions, **the resilience of the supply chains and associated infrastructure under a wider range of plausible scenarios has not been assessed**. Australia holds no public owned fuel stocks, does not mandate any fuel storage requirements on oil and fuel refiners/importers, and fails to meet the stockholding levels mandated by membership of the International Energy Agency (IEA). **The Australian Government does not have a viable contingency plan in place to provide adequate supplies for Australia's essential, everyday services and for our military forces. Australian Defence capabilities are completely reliant on "best endeavour" contracts with foreign owned oil and fuel companies.**

13 Blackburn, J, Australia's Liquid Fuel Security Pt 2, published by the NRMA 24 Feb 14.

In addition, global supply chains[14] have emerged as a result of the worldwide integration and coordination of economic activities supported by global communications, a global financial system and global logistics services. In this context, stakeholders seeking to reduce costs are able to exploit both their own advantages and the comparative advantages offered by other countries, such as lower labour costs, access to technology and production capacity.

Companies are commercial enterprises that see their responsibility as being the reliability of supply and not the security of supply. In other words, they seek to provide their customers with a reliable supply of products and services within a normal range of market conditions. This protects their market share and their brand and is clearly sensible. However, it is not their responsibility to assure the security of supply in a wider range of circumstances, such as conflict or a crisis, for example in the Asia-Pacific region.

There is no simple solution to this increased risk in supply chains; it is a complex interlinked set of problems that will need to be addressed systemically rather than in a piecemeal fashion. The notion of simply identifying how much extra capability/capacity is required and determining the cost to pay for it is not the answer. Why? Because the problem is complex, and there is an over-reliance on market forces to address all the issues.

Threats to the supply chain are constantly growing in sophistication, number, and diversity. The ICT supply chain for example is susceptible to both intentional and unintentional threats and vulnerabilities. Intentional threats include counterfeit products and malicious software. Unintentional threats include inadequate or poor product security and integrity practices throughout the development life-cycle; unintended access to critical systems; poor procurement standards and practices; reliance on third-party providers for sub-components; and inadequate personnel screening.

Addressing the challenges associated with ICT supply chain risk management requires integrating practices from enterprise risk management, information security, software assurance, system and software engineering, project management, quality assurance, acquisition, and a number of other disciplines.

Organisations such as Defence should develop, implement, and test a contingency plan to include the supply chain to ensure integrity and reliability of the supply chain even during adverse events (e.g., natural disasters such as storms or economic disruptions such as labour strikes). Such plans may incorporate the use of multiple suppliers or multiple supply chains, and actively manage integrators through Service-Level Agreements (SLAs) and standard operating procedures with event-triggered escalation rules.

Defence has traditionally exercised considerable control and ownership of its supply chains; however, this internal ownership and control of logistics and support functions in Defence has progressively been reduced as supply chain systems have evolved. While the responsibility for various activities within the Defence supply chain may have been outsourced, Defence still remains accountable for the combined effect.

---

14 For an expanded discussion on this topic see Wing Commander Neil R. Collie, RAAF, 'Managing Global Supply Chains', Australian Defence Force Journal, Issue No. 183, 2010, pp.77-86.

There are some specific risks and concerns that arise in the context of global supply chains that must be considered and, if necessary, mitigated which include:

- the perceived limited Defence influence on contractor and other customer behaviour;
- allowable knowledge sharing;
- the security and assurance of supply;
- use of proprietary logistics information systems;
- use of an OEM's proprietary parts inventory codification system; and
- the deployability of supply systems.

By definition, a global fleet support arrangement involves other customers who have a stake in goods and services that are part of the arrangement. Of concern is the potential behaviour of other customers. Any such arrangement must include an examination of the strategy to retain control over strategic fleet management policy as it affects the Australian portion of the global fleet. Also scrutinised should be the strategy to ensure that Australian interests prevail, particularly in relation to pooled inventory share and apportionment. Arrangements to address the security and assurance of supply of spares and other services must also be considered, particularly in conditions of 'surge' or significant fluctuation in operating tempo and rates of effort that induce dramatic demand oscillation.

Also scrutinised should be the strategy to ensure that Australian interests prevail, particularly in relation to pooled inventory share and apportionment.

The use of a proprietary OEM LIMS and the way in which it interfaces with Defence's LIMS - and how much it might cost to achieve this - is a major issue. Proprietary LIMS raise concerns as to security, Defence-approved software issues, and licensing. The central concern is deployability into a hostile or austere operating environment, where there is typically limited bandwidth available for 'reach-back' by the deployed communications system.

Defence's intent for MILIS is to provide a platform for a single system of standardised logistics processes across the organisation in order to provide end-to-end visibility of the Defence supply chain and the removal of the requirement for multiple logistics systems. Hence, any proposal to use proprietary LIMS in a global fleet support arrangement should include scrutiny of its capability to interface with the existing Defence non-secure and secure communications and IT systems, in particular MILIS. This scrutiny must elicit any additional costs associated with the use of LIMS, including hardware, software, software licensing and training. For deployable systems, the analysis should aim to determine the estimated bandwidth requirement and the potential for this to increase as and when proprietary LIMS hardware or software is updated.

Addressing supply chains more generally, the commercial view is that companies will only stock what they can sell, so demand management is crucial for effective supply. The Supply Chain Resilience Assessment and Management (SCRAM) methodology framework was introduced to standardise the environment. This methodology considers both vulnerabilities and capabilities in developing a view of the resilience of a supply chain. This leads to an assessment of whether the supply chain is at risk,

is well balanced, or is too risk averse, which impedes profitability for private supply chains and operability of Defence supply chains. Whilst in some circumstances there may be a need to create a temporary highly-resilient supply chain that can deliver fully as required, such as in disaster relief or human evacuation response, the need to interface the private and public supply chains will require a measured response.

As noted earlier in this report, supply chain risks are examined in the World Economic Forum (WEF) Report: "Building Resilience in Supply Chains" published in January 2013. It addresses the requirement for a multi-stakeholder risk assessment framework and the need to build agile and adaptable strategies that will improve resilience and protect against a range of global disruptions. It also addresses the requirement for a multi-stakeholder risk assessment framework and the need to build agile and adaptable strategies that will improve resilience and protect against a range of global disruptions.

The WEF Report notes that systemic risks have global geographic scope, cross-industry relevance, uncertainty as to how and when they will occur, and high levels of economic and/or social impact requiring a multi-stakeholder response. It maintains that risk management must be an explicit but integral part of supply chain governance. To achieve this, several steps are recommended:[15]

- Institutionalising a multi-stakeholder supply chain risk assessment process.
- Mobilising international standards bodies to further develop, harmonise and encourage the adoption of resilience standards.
- Incentivising organisations to follow agile, adaptable strategies to improve common resilience.
- Expanding the use of data sharing platforms for risk identification and responses.

Given the concerns highlighted in the earlier part of this Kokoda Foundation report regarding the growing levels of Enterprise risk that can emerge as a result of a fragmented Logistics domain, the WEF report provides additional justification for Defence to take a fresh look at Enterprise risk assessment and the changing nature of Logistics support. For the Australian Defence Organisation, collaboration is a crucial aspect that must extend beyond the notion of simple partnerships and is vital so Defence can understand where real supply chain resilience vulnerabilities lie. Contractual mechanisms do not allow real collaboration through the Australian Defence Contracting (ASDEFCON) mechanism. Furthermore, the PBC model is all weighted in favour of Defence. True collaboration is crucial for effective materiel flow and supply chain resilience.

15 World Economic Forum Report: "Building Resilience in Supply Chains", January 2013, p. 7.

Addressing the Logistics Information Management Challenges

The concerns regarding the ability to sustain the existing MILIS configuration and ongoing delays to Project JP2077 Phase 2D represent a challenge to Defence Logistics delivery and thus a substantial strategic risk to Defence's preparedness posture.

As mentioned earlier, JLC is not as concerned as the authors over the risk from delays to JP2077 Phase 2D, as JLC believes their contractual arrangements are sufficient to address this risk. There is also the view from Defence that the Next Generation Desktop will allow for the early identification of any further technical work required to sustain the engineering and maintenance applications. Nevertheless, the authors still contend that delays to the Project remain a challenge and a strategic risk.

Defence is pursuing the concept of a Single Information Environment (SIE) as an end-state that describes the ability to deliver data to the ADF and Defence's civilian personnel wherever and whenever they need it. This end-state can't be achieved without streamlining data delivery processes and eliminating excess capacity; nor can it happen overnight. Replacing legacy systems and rationalising current systems will take time. Furthermore, the way those systems are operated may change before they're replaced.

Rationalisation of data centres is already underway, leading to faster and more efficient networks. The result will be a smaller physical network footprint that will move data much more quickly and efficiently and be easier to secure because it will be easier to oversee. Ultimately, everyone will benefit because as the SIE becomes easier to secure, it will become more flexible - something that takes on added importance as the department embraces mobile platforms.

Challenges around the SIE must be dealt with to achieve a secure and user-friendly ICT environment that supports Defence business and operations. Confidentiality, integrity and availability must be assured – which involves policy and practice, human factors, technology, storage, transmission and processing. The SIE must also offer ease of compliance, risk awareness and risk tolerance, user focus and collaborative design.

Service Oriented Architecture (SOA) represents an architectural style that aims to enhance the agility and cost-effectiveness of delivering IT capability within Defence while simultaneously reducing the overall risk and maximising the organisational investment in its IT capability. It accomplishes this by encapsulating technical capability as one or more business services that are used and re-used throughout the enterprise. Some key SOA goals include risk reduction, agility, and leveraging existing technology investments.

The SOA Backbone enables the interoperability of business services in a consistent and predictable manner based on the codified business processes. As such, it underpins and guides the architectural intent of the SIE. SOA facilitates re-use, sharing and alignment with Defence's business functions. It positions re-useable services as the primary means for integration and the interoperability of systems within the SIE

and with partners and allies. Over time, the realisation of a SOA will provide the basis through which business logic can be de-coupled from underlying systems to support flexibility and maintainability.

One of the challenges Defence faces is to support a logistics capability that provides the flexibility for change over time and addresses the issues outlined previously. There are essentially two choices – the big bang approach or a planned evolution over time. SOA integration allows abstraction of the technical layer from the business layer so simply unplugging one system and plugging in its replacement can effect changes at the technical level, thus decoupling of technology from business processes.

The integration layer must not only work across all Defence capabilities but also into commercial supply chains. In the case of the Joint Strike Fighter (JSF), the point of integration between Lockheed Martin's Autonomous Logistics Information System (ALIS) and Defence's MILIS is yet to be defined. The integrity of the system of record (MILIS) will need to be maintained for data quality and data auditing purposes.

In a sense, Defence "business" needs to transform itself and set a clear end-state with sensible and achievable stages and milestones, deciding which functions must be automated as a priority and which can wait, before genuine IT transformation can occur. What has been missing is a LIMS strategy looking out 20 years into the future. This should be redressed through the Defence Logistics Information Strategy (DLIS) and a DLIS Investment Plan that are expected to be released in 2014. This investment plan will be crucial as the sustainment budget for the 33 key logistics applications has been flat for some years, and sits as an annual allocation of $42m.

The current systems are deteriorating and will need additional funds for continued use. The funding baseline is an issue, not just the inadequacy of the baseline figure of $42m but also the poor state of the Minors program, which has fallen to $3m per annum. CJLOG will not agree to any new LIMS capability without NPOC, so the increased rigour around the approvals process for any new proposals will necessitate increased funding from the start to address in-service management and maintenance.

DLIS and its accompanying investment plan will set an integrated program of work for CIOG for future years, which has not been possible in the past. The investment plan will have to focus on dealing with legacy systems, and is likely to be considered annually by the Defence Capability and Investment Committee.

JP2077 Phase 2D will address engineering and maintenance, amongst other functions, and will present an opportunity to build some serious analytics and business intelligence capability into Defence's engineering and maintenance modules for the future. However, JP2077 Phase 2D has slipped within the DCP and is currently not expected to be delivered until the end of the decade. **Defence Capability Managers are concerned with how the current engineering and maintenance applications will be sustained until Phase 2D is implemented; however as mentioned earlier, there is a view that the Next Generation Desktop will allow for problems to be identified and rectified.**

The delay does represent a substantial risk to Defence's preparedness posture. For example, as a result of the delay, Defence will have difficulty in providing effective integrated logistics support to the Amphibious Capability that will be introduced into service over the next few years and to the JSF, which has an Initial Operational Capability (IOC) of 2018. As illustrated in Figure 1, the nation will face increasing

strategic uncertainty and the likelihood of increased budget pressures over the next decade. The absence of a comprehensive integrated logistics system information environment will limit the understanding of logistics demands and risks by senior decision makers. **The combination of these factors will translate into increased preparedness and operational risk and in turn increased Defence Enterprise risk.**

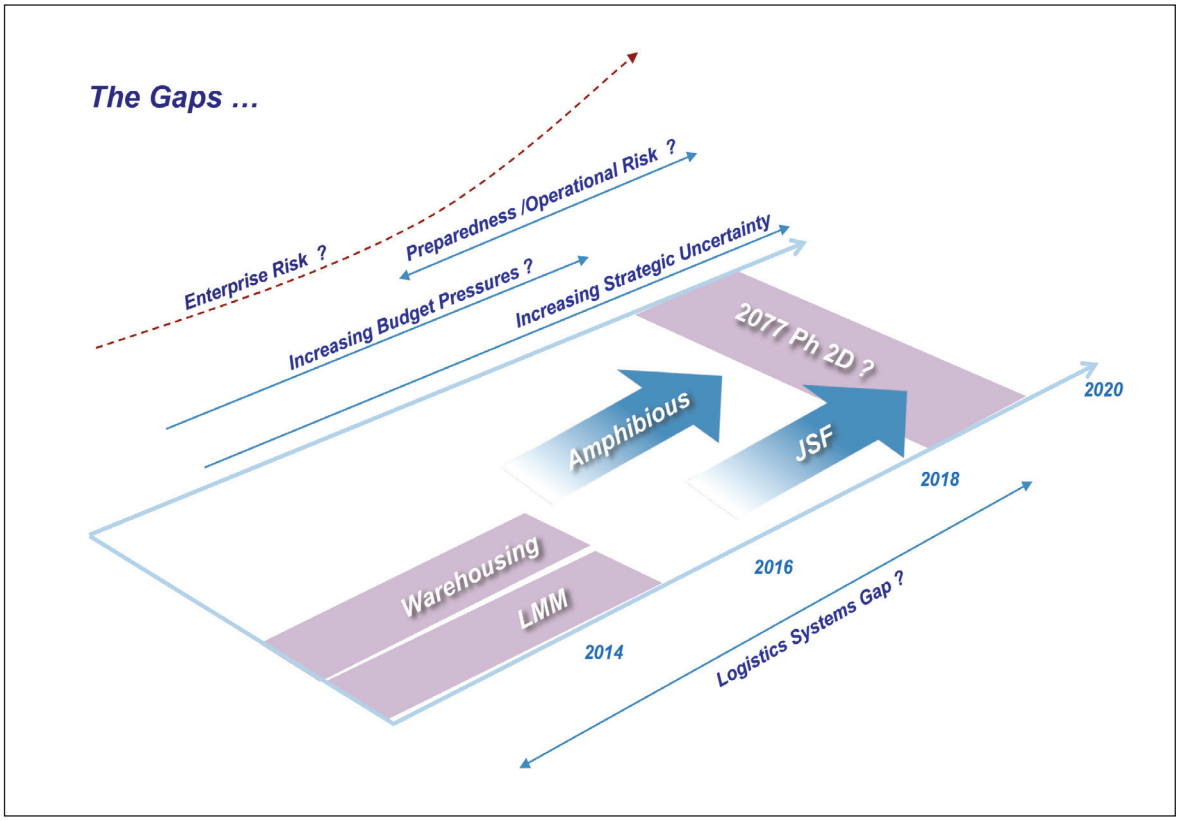

Figure 1: The implications of delays to JP 2077 Phase 2D

The Defence acquisition two-pass process introduces time lags with information technology; the acquisition process has been described as an industrial-age process for information-age requirements. This process with its low tolerance for risk impedes evolutionary acquisition of IT capabilities and thus degrades the performance of a Logistics information management system with attendant enterprise risk.

Ensuring Information Security

As military operations depend on logistics and as logistics depend on the underpinning ICT, a strong focus must be on ICT security – everything about ICT – not just that which connects to the Internet. The evolution of threats has seen greater sophistication in attacks and greater resourcing of those attacks, ranging from script kiddies (who operate for the fun of it) to Advanced Persistent Threats (APTs), which are state-sponsored attacks directed against corporate enterprises as well as government agencies.

Organisations are fighting to close the gap: they have made significant moves to respond to information security threats by addressing vulnerabilities with increased resources, training, governance and integration. However, the number and

sophistication of threats has also increased and is challenging information security functions to keep up. The gap between what information security functions are doing and what they should be doing has widened.

The basic principles of ICT security include confidentiality, integrity of information, availability of systems, and authentication of users. Auditing is also crucial as it verifies that the basic principles are working as designed.

LIMS are probably more complex than other information systems because of the number of connections and the de-perimeterisation of Defence's networks. Auditing of Defence LIMS is important but so too is auditing of LIMS all the way through the supply chain. It is important to identify the trophy LIMS that need to have heightened security focus applied to them.

IT security is important for LIMS for the reasons outlined above but also for these other particular reasons:

- Logistics supports military operations through the movement of troops and capability; hence the availability of the system/data is important.
- Logistics play a key role in inventory management and therefore financial management; so integrity of the data is important.
- Logistics systems contain information on what capabilities (and how many) are located where; so confidentiality of the system data is important, particularly in times of conflict.

Key mitigations for LIMS include the following good security practices:

- *Catch*: unwanted applications - only allow approved applications to run on systems.
- *Patch*: latest versions of software and security updates.
- *Match*: users access with requirements.
- *Minimise* user privileges.
- *Secure/harden* underlying infrastructure – secure the underlying operating systems, databases and network connections – including with suppliers.
- *Vulnerability assessment* – know where the weaknesses are and prioritise their remediation.
- *Educate* all users of the need for security, including suppliers.

The slow delivery of IT leads to a growth in shadow IT, where business owners obtain their own IT, which leads to further security challenges and duplicated capability with attendant support, maintenance and licensing costs. To get away from shadow IT, CIOG does need to create a digital delivery cycle - a quick cycle time for new applications and new technologies. Clearly, this does not apply at an ERP level. It is important not to stifle creativity and innovation so this delivery cycle must be very quick, even if it doesn't quite match the speed of delivery of shadow IT. The challenge is to create an IT environment that people want to use and that discourages them from looking for other applications.

Security analytics and metrics are as important to the business as any other key performance indicator. Organisations are demanding that key security analytics and metrics be included in the operational risk portfolio. This puts pressure on security

teams to provide analysis and insights that give management the risk intelligence they need to drive better performance.

Security analytics, when properly designed and implemented, can deliver much-needed insights in mapping the size, scale and scope of risks. Analytics can provide a basis for root cause analysis and remediation strategies across policies, processes and, ultimately, investments in technologies.

CONCLUSIONS

Logistics support is a complex challenge for Defence and will become increasingly so in the forthcoming decade as Defence Logistics becomes even more integrated with commercial supply chains; many, if not most, of which are becoming global in nature. Despite the challenges, Logistics does not enjoy the same visibility or priority as do the military platforms and equipment that Logistics supports. This lack of visibility and priority for Logistics could give rise to increasing levels of risk for the Defence Enterprise.

Logistics support is a complex challenge for Defence and will become increasingly so in the forthcoming decade.

The lack of priority has been compounded by a failure to assign appropriate responsibility and authority for this essential Joint function with the result that no one individual has the authority to take a systems view of the Defence Logistics domain. Consequently, the Defence Logistics domain is viewed by many as being fragmented and lacking a holistic approach, to not only the domain itself but also the broader environment in which it operates. As previously noted, this comment in no way seeks to diminish the important role of the Chief of Joint Logistics (CJLOG) nor the highly effective manner in which he and the Joint Logistics Command (JLC) execute their tasks. Rather, it highlights the unintended consequence of a failure to assign appropriate responsibility and authority at the joint level. The resulting tendency to view the various aspects of Defence Logistics through component elements introduces operational, enterprise and financial risk to Defence.

Whilst the answers to the questions posed by the report are informative, the fundamental question is how can the existing Defence Logistics domain be enabled and equipped to deal with the transformation required to address the challenges and opportunities that arise from a future-oriented change agenda *whilst also dealing with the reality of ongoing business.*

Whilst Industry can offer excellent examples of how to improve Defence Logistics and will, inevitably, operate significant components, the transformation of Defence Logistics must be led from *within* the Defence organisation. The report's recommendations therefore deal with this fundamental issue of how can Defence itself lead the transformation of Defence Logistics more effectively than it has to date?

If this report serves to highlight to the wider Defence community the challenges faced by Defence Logisticians and if it gives pause to think about the lack of priority that Defence leaders have placed on Logistics in the past, then it will have achieved the goals of the authors and the Kokoda Foundation.

Defence will need to place greater emphasis on the Defence Logistics function if it is to meet the challenges of a more complex and challenging operating environment in the future.

RECOMMENDATIONS

In order to *enable and equip* Defence Logistics to cope with the transformation required to meet future Defence operational requirements, this report makes recommendations for changes in:

- Organisational Design and Culture;
- Strategy, Concepts and Concepts of Operation; and
- Change Leadership and Resourcing.

Organisational Design and Culture

The need to afford the right priority and support for the transformation of Defence Logistics as a whole is a critical Defence leadership issue; Defence needs to appoint a Joint Capability Manager under whom the CJLOG can operate.

Regardless of what actions CJLOG and his staff take, or attempt to take, the absence of a Defence-wide understanding of the challenges existing in the current Logistics domain and those projected for the future will prevent the required changes taking place. When faced with similar problems with Defence culture and organisational effectiveness more than a decade ago, the Defence leadership of the time initiated a program of leadership change whereby all of the senior Defence civilian and military officers met in a series of recall days to explore, comprehend and address the systemic issues in Defence – the issues and challenges, the potential solutions, and the impediments to change.

The apparent lack of "Logistics champions" across the current senior leadership group, with the exception of CJLOG and his senior staff and a small cadre of senior officers in the Service Headquarters, is an issue. The importance of getting the right priority and support for the transformation of Defence Logistics as a whole is such that the Defence leadership should firstly consider mechanisms such as recall days to inform and educate the wider leadership group of the issue.

A second but as critical an issue is that of a Logistics Capability Manager. The Defence Logistics enterprise is probably one of the largest in the country when both the domestic and international components are considered. If the Logistics enterprise were a business, it would have a Board and a CEO with appropriate delegated authority and funding to run the business. Clearly, the Defence Logistics enterprise is attempting to operate a large scale "business" without the required governance and management system in place. Until Defence is culturally able to accept the need for a "Joint Capability Manager" with the authority of the Single Service and Group Capability Managers, then Defence Logistics will continue to operate in the seams between Capability Managers' areas of responsibility and accountability, without the required authority to transform and operate the transformed Logistics enterprise. If a Joint Capability Manager was appointed, then CJLOG could operate under their authority and under their unique joint purview.

Strategy, Concepts and Concepts of Operation

Defence needs to update the Logistics Strategy, Concepts and Concept of Operations based on an agreed logistics business architecture.

As noted in the report, the lack of an updated strategy, Logistics concepts and an endorsed Concept of Operations (CONOPS) based on an agreed logistics business architecture are significant impediments to addressing the Logistics challenges at an enterprise level. Whilst much can be learned from Defence's past Logistics experience and from industry, translating those lessons into an integrated management model that will support the required transformation of Defence Logistics is not a small task. To date, the resources do not appear to have been available in either the VCDF Group or under CJLOG to build the conceptual and architectural foundations required. Failure to invest in the "front end" will inevitably hamper the effective transformation of Defence Logistics and in turn compromise future ADF operations. Defence needs to invest in these areas as a matter of priority.

Change Leadership and Resourcing

Defence needs to provide CJLOG and his Command additional support and resources to perform their critical tasks, particularly given the dense and complex organisational processes employed by Defence.

Noting the challenge of managing change in addition to the overwhelming load of day-to-day business, CJLOG and his Command do need additional support and resources to perform their critical tasks, particularly given the dense and complex organisational processes employed by Defence.

Whilst some supplementation of key functions appears warranted, there may also be value in considering additional support of a different nature. To date, logisticians have performed the analysis of, and argument for, the transformation of the Logistics enterprise. Whilst this is logical, it does hamper the ability of CJLOG to champion the cause across the Australian Defence Organisation as a whole and in the midst of competing priorities.

Noting the value of the US Combatant Commands' experience of exchanging liaison officers between Commands in order to translate and communicate across organisational boundaries, there may be benefit in CJLOG being supported by a senior advisory/liaison team that is not wholly comprised of logisticians. For example, if an inter-disciplinary team with organisational links to the Capability Managers and DMO supported CJLOG, there could be benefits in having the team develop the Logistics Strategy and plans under CJLOG guidance, which they could then communicate and champion across Defence, prior to formal consideration by the layered committee system. An experienced operator (vice logistician), having taken the time to analyse and comprehend the Logistics challenge, may have a greater chance of success in communicating the Logistics needs and priorities to their parent Service and the senior operators therein.

GLOSSARY

Area of Operations	**(AO)**
Australian Defence Force	**(ADF)**
Australian Defence Organisation	**(ADO)**
Autonomous Logistics Information System	**(ALIS – Lockheed Martin)**
Capability Development Group	**(CDG)**
Chief Information Officer Group	**(CIOG)**
CDF's Preparedness Directive	**(CPD)**
Chief of the Defence Force	**(CDF)**
Chief of Joint Logistics	**(CJLOG)**
Concept of Operations	**(CONOPS)**
Defence Capability Plan	**(DCP)**
Defence Logistics Transformation Program	**(DLTP)**
Defense Logistics Agency	**(DLA – United States)**
Defence Materiel Organisation	**(DMO)**
Enterprise Resource Program	**(ERP)**
Fundamental Inputs to Capability	**(FIC)**
Joint Force-In-Being	**(JFIB)**
Joint Logistics Command	**(JLC)**
Joint Strike Fighter	**(JSF)**
Landing Helicopter Dock	**(LHD)**
Landing Platform Amphibious	**(LPA)**
Logistics Information Management Systems	**(LIMS)**
Materiel Sustainment Agreement	**(MSA)**
Military Integrated Logistics Information System	**(MILIS)**
Net Personnel and Operating Cost	**(NPOC)**
Original Equipment Manufacturer	**(OEM)**
Quarterly Strategic Review	**(QSR)**
Raise, Train, Sustain	**(RTS)**
Supply Chain Resilience Assessment and Management	**(SCRAM)**
Single Information Environment	**(SIE)**
Service Oriented Architecture	**(SOA)**
System Program Office	**(SPO)**
Vice Chief of the Defence Force	**(VCDF)**
World Economic Forum	**(WEF)**
Weapons of Mass Destruction	**(WMD)**

www.kokodafoundation.org