WHITE PAPER
Information Superiority for Capability Management

Dr Andrew Dixon & Richard Bryson | Autumn 2021

ABSTRACT

The phrase "Information Superiority" has been in common use within Defence for around twenty years. It is defined by the US Department of Defense as:

"The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same". [1]

The principles behind this definition - the collection, processing and dissemination of information - are valid in every aspect of Defence - a fact reflected in the vision of the British Defence Information Strategy (DIS) [2] which is to: *"... deliver information capabilities to defence that act as a force multiplier, and to do so at real pace".* The DIS further articulates the primary outcome of the force multiplier in the following terms:

"From the warfighter to the corporate HQ, users are at the heart of a single information environment in which they can access, via a single identity, and appropriately share the information they need to meet their business objectives or achieve information superiority over an enemy".

The emphasis within these examples reflects an observation that Information Superiority is too often focussed on the Operate function within Capability Management [3], and insufficient emphasis is placed on the application of Information Superiority to the Direct, Develop, Deliver, Generate and Assure Coherence functions.

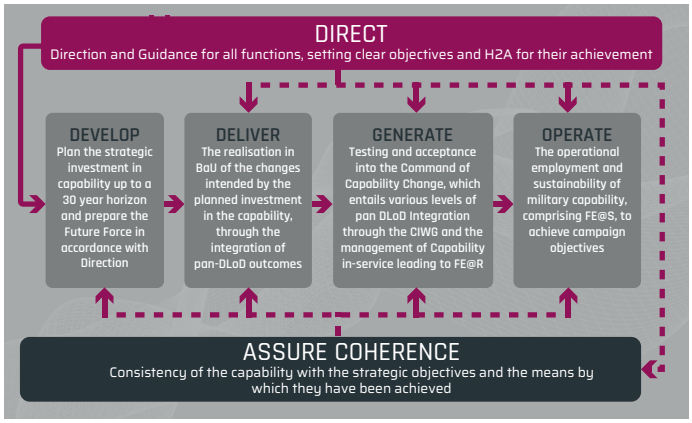

Figure 1 - Capability Management Functions [4]

Such an emphasis belies the significant effect on Defence Outputs and Outcomes which is enabled through information superiority during the acquisition phase and in particular during the activities outlined by the Capability Management Practitioners' Guide [5]. This paper outlines the case for a rebalancing, through the development and deployment of new technology, to deliver more effective information superiority solutions to be applied during the "Acquire" and "Develop" functions of the Defence Operating Model [3].

+44 (0) 1747 820 900

mail@svgc.co.uk svgc.co.uk

INFORMATION SUPERIORITY IN BUSINESS OPERATIONS

COLLECT

In military operations, a range of data and information sources are used to inform operational decision making. Sensors generate a vast amount of data for processing where issues such as volume, variety, velocity, veracity, validity and volatility are addressed by the processing disciplines of 'Big Data' [6].

In organisations, this information generally travels along defined routes using databases, conducting business analysis and rising through the management chain. However, business information is increasingly being made available from external sources, harvested from the internet, such as suppliers and social media, where more 'Big Data' issues are emerging and therefore challenging the traditional models of organisational data and information management.

Data and information from any source needs to meet various conditions to be useful to inform decision making. Timeliness (not to be confused with "velocity"), Veracity and Volume are key factors to consider. In the paper aptly entitled "Data Doesn't Matter, Time Matters" [7], the author explores the business value of information and differentiates between a data-driven company and a time-driven company. He defines a data-driven company as *"an organization that provides information to every employee and every business process in order to improve decisions and overall performance"* [7] and explains that context is critical to the information because it determines the conditions under which the information is actually useful. The Data itself is not as important as the ability of the organisation to exploit it within a specific context. Consequently, a time-driven company is *"able to change and adapt quickly in an internal way, but it also reacts quickly to changes in the environment"* [7].

What then of the 'exploiting' phrase within the definition of information superiority? Defence Intelligence (DI) is focussed on a variety of overt and covert sources to provide *"timely intelligence products, assessments and advice to guide decisions on policy and the commitment and employment of the Armed Forces; to inform defence research and equipment programmes; and to support military operations"* [8]. Within DI, there is a need to understand how aggressor nations are exploiting data and information and how this is being used to inform both their operations and their acquisition decisions.

We need to operate with at least as much agility and flexibility in our information infrastructure during the acquisition phases of defence operations as our enemies do, and equally, our coalition partners, if we are not to be left behind in seeking to defeat common threats.

To achieve an understanding of alternative approaches to the exploitation of data and information in the business of defence, experimentation in defence acquisition is proposed. Such experimentation will explore new and novel ways of gaining insight and foresight which other nations are either known to use, or could use. Such experimentation will seek to understand how to use this data and information to make

well informed, timely decisions which are able to cope with the volume and veracity issues becoming increasingly common in our inter-connected world, and to compare and contrast UK "acquisition capability" with that of other nations - including aggressor nations.

The emphasis for information superiority for conducting business operations will be to create conditions and environments which adapt rapidly to new information sources, and new ways of processing and disseminating data and information. Importantly, to achieve information superiority in acquisition will require the whole Defence Enterprise to be involved including the MOD, large and small business – suggesting the use of experimentation or solutions centres in which data and information for decision making in acquisition may take place.

PROCESS

The Defence Information, Knowledge, Digital and Data Policy Commitments [9] describes a future state involving common information sharing with Other Government Departments (OGDs) and recognised its role to *"be a standard bearer for good government, actively contributing to pan-government initiatives which improve how departments function and collaborating with our colleagues in other departments to add value"* [9]. In 2017, the DIS acknowledges the importance of Data and the use of Information to achieve effective decision making. It describes the need *"to exploit the full potential of the data it holds through active data management, better digital processes, and more timely and cost-effective analysis to derive maximum value to support evidence based decision making"* [2].

Capability Management lies at the heart of UK Defence Management and is captured within the Acquisition Support Guidance [5], the Generic Capability Management model [10] and the Capability Management Practitioners Guide [4]. This seeks to exploit the full potential of data to enable sustained and coherent military capability through time.

From these descriptions, Capability Management, (summarised in Figure 2), considers the long-term context in which the capability area resides; the uncertainty associated with that context; the long-term demand and associated trends; the supply of capability as planned and as expected to be implemented; determining the differences (positive and negative gaps) between demand and supply; to drive out options delivering identified benefits and within certain controls and subsequently a course of action in an appropriate form. This provides the necessary material for business cases to present evidence based recommendations to deliver long-term capability solutions in response to the demonstrated demand set in the relevant context.

As anticipated within the MODIS [9] and DIS [2], Capability Management requires close industry involvement to properly understand the 'Capability Context' and to understand the capacity and ability of industrial supply, along with evaluation of the art of the possible prior to locking down a course of action. MOD organisations go a long way to engage industry but have not traditionally focussed Network Enabled Capability on the

acquisition environment. It is time for that to change, and for the rebalancing to occur – recognising the significant difference which effective use of data and information can make early in the defence operating cycle.

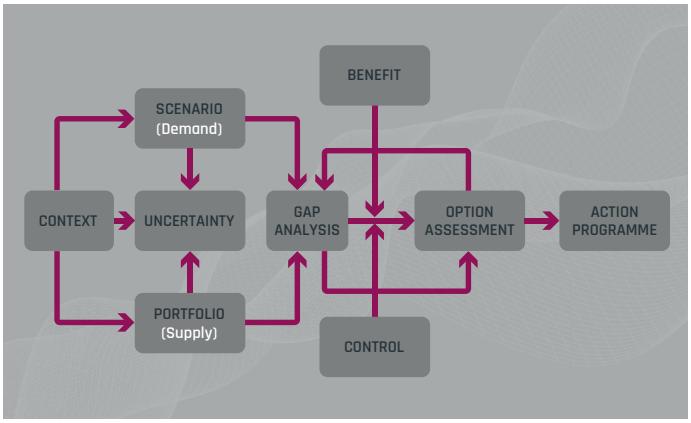

Figure 2 - SVGC Summary of Through Time Capability Management

Building on the collect function proposal to have Defence Acquisition experimentation, there is a need to understand how to process data and information to make informed evidence-based decisions within acquisition in a world which has real-time data feeds, the internet-of- things, data lakes, big data, artificial intelligence, machine learning, predictive and prescriptive analytics.

DISSEMINATE

Dissemination of information is the act of sharing and communicating findings. Such an act may be achieved in a passive way - for example, through the publication in a 'browser' type environment in which others have to search to find the information; or in an active way, ensuring the right people (or processes) are alerted to and receive the right information at the right time. The right people (or processes) are those which require it in order to enhance a business output or outcome. The right information means that it is beneficial information, but also that it is in a form which can be exploited. Exploitation of the information is only possible if the information is timely and that its context is understood. Information superiority for acquisition requires active, timely dissemination across the Defence Enterprise.

Many ways of achieving information dissemination have been explored over the years within the Defence Enterprise. Historically, this has been achieved through the implementation of an "e-commerce" agenda. The Defence Electronic Commerce Service (DECS) provides a range of hosted services that seek to standardise the way trading partners interface with the MOD in a secure environment. Established in 2000, DECS became an element within the Defence Core Network Services (DCNS) and included the provision of Information Management, Project and Portfolio services [11].

TOWARDS INFORMATION SUPERIORITY FOR CAPABILITY MANAGEMENT

In the paper "Achieving Information Superiority" [12], the authors identified five imperatives which are necessary to achieve information superiority and here we reinforce them as the key tenets, and apply them to Capability Management for Defence and

Security acquisition.

- **Treating information as a strategic asset;**
- **Having centralised governance;**
- **Building an information culture;**
- **Taking the right cyber security posture;**
- **Designing and delivering an integrated ICT infrastructure.**

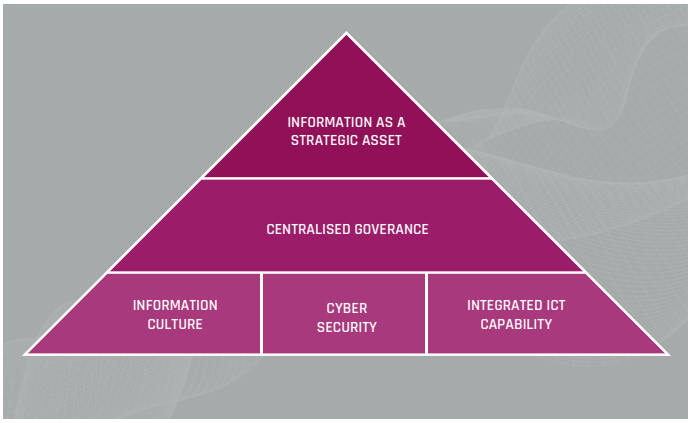

Figure 3 - Information Superiority Strategic Imperatives [12]

TREATING INFORMATION AS A STRATEGIC ASSET

Information is a *"strategic asset which needs to be assured, shared and protected"* [2]. Managing Capability requires the understanding of context [4]. Publications such as the DSTL Global Strategic Trends [13] provide a useful contribution and through the internet provide an example of passive information dissemination[1]. However, all parts of the MOD, and many parts of defence Industry need access to common information – for example - on Political, Economic, Social, Technological, Environmental and Legal (PESTLE) matters. Industry could also benefit from information on operational challenges and lessons learned in order to focus private venture (PV) investment. Equally, the MOD needs information on the industrial art- of-the-possible in order to achieve a successful procurement.

Organisations such as Niteworks[2] used to provide significant support to this principle, recognising the need to share and protect information, and fundamentally treating the information as a joint asset of value to the defence enterprise as a whole - a core principle which it is hoped will be re-established with the emerging Futures Group.

It must also be recognised that the use of data and information is changing. MOD has transitioned to Office 365 - an 'evergreen' software environment which is designed with the principles of collaboration at its core. Our white paper on "Capability Management 2.0" [14] proposes the use of a collaborative approach to application development for better information analysis for decision making.

HAVING CENTRALISED GOVERNANCE

The DIS [2] and other related policies and practices must be driven by a strategic leader who provides the top-level ownership of the

[1] An official-sensitive version is also available within the MOD via the government secure intranet.

[2] www.niteworks.net . Niteworks was established by the Ministry of Defence (MOD) to provide a commercially neutral partnership between MOD, industry and academia. The author is a former consultant to, and Director of, Niteworks.

+44 (0) 1747 820 900

mail@svgc.co.uk svgc.co.uk

information DLoD[3]. This role must have the authority to manage the strategic asset, to enable effective capability decisions to be made. This is especially true considering the intention to become the "Masters-of- our-own-Destiny" expounded in DIS.

This is best achieved through a centralised approach with appropriate authority, organisational structures, policies, standards, procedures, and controls. Critically, wider members of the defence enterprise should be involved as part of the governance mechanism - ensuring large and small businesses have protected and assured access to information assets.

Such a governance approach needs to be constantly challenged to ensure it does not become a blocker to achieving information superiority. One approach is through experimentation - the use of a "sandbox". Following recommendations by the Government Office for Science, the UK Finance and Conduct Authority was asked by Her Majesty's Treasury (HMT) to investigate the feasibility of developing a regulatory sandbox for financial services [15]. This provides a *'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question"*. Such a model could be explored either as an experimentation environment in its own right, or as part of the scope for Niteworks replacement or other framework environments.

Team Defence Information (TDI) has gone a long way to promote the importance of information, but even this has its routes in logistics information rather than up-front acquisition information. This paper is encouraging TDI and Information DLOD owners to re-balance towards acquisition information.

BUILDING AN INFORMATION CULTURE

Militaries aspiring to achieve information superiority have started to shift their cultural paradigm from "need to know" to "need to share wherever appropriate and beneficial to do so". Such a behavioural shift is also required within the acquisition community by both MOD and Industry.

All personnel involved in the enterprise need to understand the importance of information and their role in delivering broader information awareness. This requires a fundamental shift in behaviour and one in which collaboration practices are to be encouraged to support and enable the sharing of information.

A programme is required which recognises the benefit and mechanisms for data and information sharing involving both MOD and Industry, and which conducts experimentation into ways of achieving this, along with a re-think on the types of data and information which are required and the way in which these are consumed.

[3] Defence Line of Development

TAKING THE RIGHT CYBER SECURITY POSTURE

Cyber security is vital as the sharing of data and information increases. However, it must not be allowed to become a barrier to sharing, and therefore proactive cyber behaviour, tools and methods are essential.

Advances in technology are changing the way in which information security threats can occur at a rapid pace. Information capabilities need to be able to respond. An architectural approach is required which is focussed on designing in cyber protection to defence information solutions providing data assurance which includes confidence in the origins and validity of data and information used for Capability Management decisions.

DESIGNING AND DELIVERING AN INTEGRATED ICT INFRASTRUCTURE

This paper has discussed the importance of flexibility in information infrastructure. The information and communications technology (ICT) system must provide the ability to collect, process and disseminate information by securely linking Industry and the MOD. ICT systems must be interoperable across joint forces, coalition forces, and government agencies. Given the importance of digital applications, the technology should also respond to the current and anticipated future context of cloud solutions, big data challenges, quantum computing and the internet- of-things.

An important element of the infrastructure will be the existing and forecast skills across the Defence community that are able to exploit the infrastructure. Joint workshops are proposed with MOD and Industry participants – facilitated through bodies such as TechUK and/or Team Defence Information and focussed around Capability Management as a theme to share experiences of data and information, understanding and act on enablers and blockers which seek to drive the achievement of the vision of the DIS [2]. Such workshops should be conducted as part of the wider and on-going experimentation programme for Defence Acquisition.

CONCLUSION

The UK Ministry of Defence and the wider Enterprise need to become a “time-driven” organisation which can share vast amounts of data and information for mutual benefit. The Defence Enterprise needs to embrace the principles of the Defence Information Strategy with a collective focus on secure and flexible information infrastructure which supports the principles of information superiority within the Direct, Acquire Generate and Develop functions of the Defence Operating Model.

To do so, experimentation is required which is focused on “achieving information superiority for capability management” - to explore ways of conducting capability management using contemporary approaches to sharing data and information assets, to understand the risks and benefits of doing so, evolving the processes and practices of capability management to maintain the optimum approach as the data and information context changes. Such experimentation should include the ways and means for sharing, the implementation of governance mechanisms and consider the change

+44 (0) 1747 820 900

mail@svgc.co.uk **svgc.co.uk**

requirements to build an information sharing culture across the Defence Enterprise. Further, the experimentation should explore the emerging cyber threat and the most appropriate ICT infrastructure architecture which enables Information Superiority in Capability Management to be achieved, and in doing so, support and enable the optimum military effect to be achieved through time.

REFERENCES

[1] Department of Defense, "Joint Publication 3-13. Information Operations," 27 November 2012. [Online]. Available: http://dtic.mil/doctrine/new_pubs/jp3_13.pdf. [Accessed 03 September 2017].

[2] "Defence Information Strategy.," February 2017. [Online]. Available: https://www.gov.uk/government/publications/defence- information-strategy/latest-amendment. [Accessed August 2017].

[3] Ministry of Defence, "The New Operating Model. How Defence Works. Version 3.0," TSO, London, 2012.

[4] Ministry of Defence, "Capability Management Practitioners Guide (CMPG)," 2013.

[5] Ministry of Defence, "Aquisition Support Guidance - Version 2.0.16," [Online]. Available: http://www.aof.mod.uk/aofcontent/cm/cm.htm. [Accessed 1 August 2017].

[6] I. Enterprise, "Big Data Innovation Summit," September 2013.

[7] M. Rafalo, "Data Doesn't Matter. Time Matters.," Cutter Consortium. Vol 30, No 2. Feb 2017, 2017.

[8] "Defence Intelligence (now withdrawn)," 12 December 2012. [Online]. Available: https://www.gov.uk/guidance/defence- intelligence. [Accessed 03 September 2017].

[9] Ministry of Defence, "Defence information, knowledge, digital and data policy commitments," Crown Copyright, July 2019.

[10] Ministry of Defence, "Generic Capability Management (GCM) Model," 2013.

[11] "DECS Collaboration," 2012. [Online]. Available: https://www.capgemini.com/gb-en/wp- content/uploads/sites/3/2017/07/DECS_Collaboration_Progra mme DCP Collaboration_at_the_heart_of_the_MOD.pdf. [Accessed August 2017].

[12] Abdulkader Lamaa, Mark Jansen, Hugo Trépant, Andrew Suddards, "Achieving Information Superiority - Five Imperatives for Military Transformatin," Strategy&, 2014.

[13] Ministry of Defence, "Strategic Trends Programme, Global Strategic Trends - out to 2045. Fifth edition," Ministry of Defence, 2014.

[14] SVGC Limited, "Capability Management 2.0," no. 1, p. 6, 2017.

[15] Financial Conduct Authority (FCA), "Regulatory Sandbox," 2015. [Online]. Available: https://www.fca.org.uk/publication/research/regulatory- sandbox.pdf. [Accessed 3 September 2017].

[16] Ministry of Defence, "Defence Industrial Strategy, CM 6697, Para A1.23," 2005.

[17] J. Pontin, "ETC: Bill Joy's Six Webs," MIT Technology Review, 29 September 2005.

[18] "Glossary of Defense Acquisition Terms," [Online]. Available: https://dap.dau.mil/glossary/Pages/2034.aspx. [Accessed 28

SVGC - AN INTRODUCTION

Established in 1997, SVGC offers a broad spectrum of support to help resolve its clients' most challenging issues. Originally founded to provide support to the Ministry of Defence and associated industry, our services are increasingly in demand from other government departments, commercial organisations and the nuclear sector.

At the heart of our approach is an unparalleled understanding of, and focus on, our customers' needs. Our blended team of business, military and security experts provide high-quality, rapid and cost-effective solutions whatever your issue may be.

SVGC operate a collaborative business relationship cluster with fourteen partners, providing access to over one hundred capable professionals and have been at the forefront of Through Time Capability Management since its inception in 2004, contributing to every evolution since.

Our specialists (permanent team or members of our partnership) are able to operate from SVGC premises using secure, government-approved IT networks, or can be fully embedded within your organisation. Through this extended network we ensure that our services continually evolve to reflect the latest industry practices and thinking.

As an approved supplier to UK MOD and wider Government, SVGC is ISO 9001, ISO 27001 and ISO44001 certified and have a range of permanent team qualifications including PRINCE2 and APMP.

- Making effective decisions which will withstand public scrutiny
- Strategic and long-term evidence-based planning
- Delivering effective change – overcoming mindset and skillset challenges
- Executing effective acquisition in an auditable way
- Maturity, process improvement and benchmarking of business process
- Supporting the establishment of collaborative business relationships
- Ensuring through-life traceability from requirements to disposal
- Applying Enterprise Architecture and Systems Engineering to enable robust solutions
- Our business has supported and engaged with the Cyber Essentials accreditation since launch and has achieved Cyber Essentials Plus status and are members of the Armed Forces covenant.

Figure 5 - SVGC accreditations

+44 (0) 1747 820 900

mail@svgc.co.uk svgc.co.uk

We are leading the implementation of Digital Decision- Making Environments through research and development to deliver on the principles of the Defence Information Strategy. This will deliver better, evidence based, hindsight, insight and foresight to our clients through secure, safe, open and collaborative engagements.

- Generating value and benefit out of unstructured data
- Managing and analysing large and complex data sets to improve decision making
- De-duplication of files and identification of sensitive content
- Delivering integrated business processes and enabling software solutions
- Digital transformation of business processes in government
- Data-enabled evidence using analytics for decision management
- Applying Solution Architectures and effective Agile Engineering

Please contact us to discuss how our expertise in people, processes and tools like databases, cost models or training software could help solve your business problems.

+44 (0) 1747 820 900

mail@svgc.co.uk **svgc.co.uk**