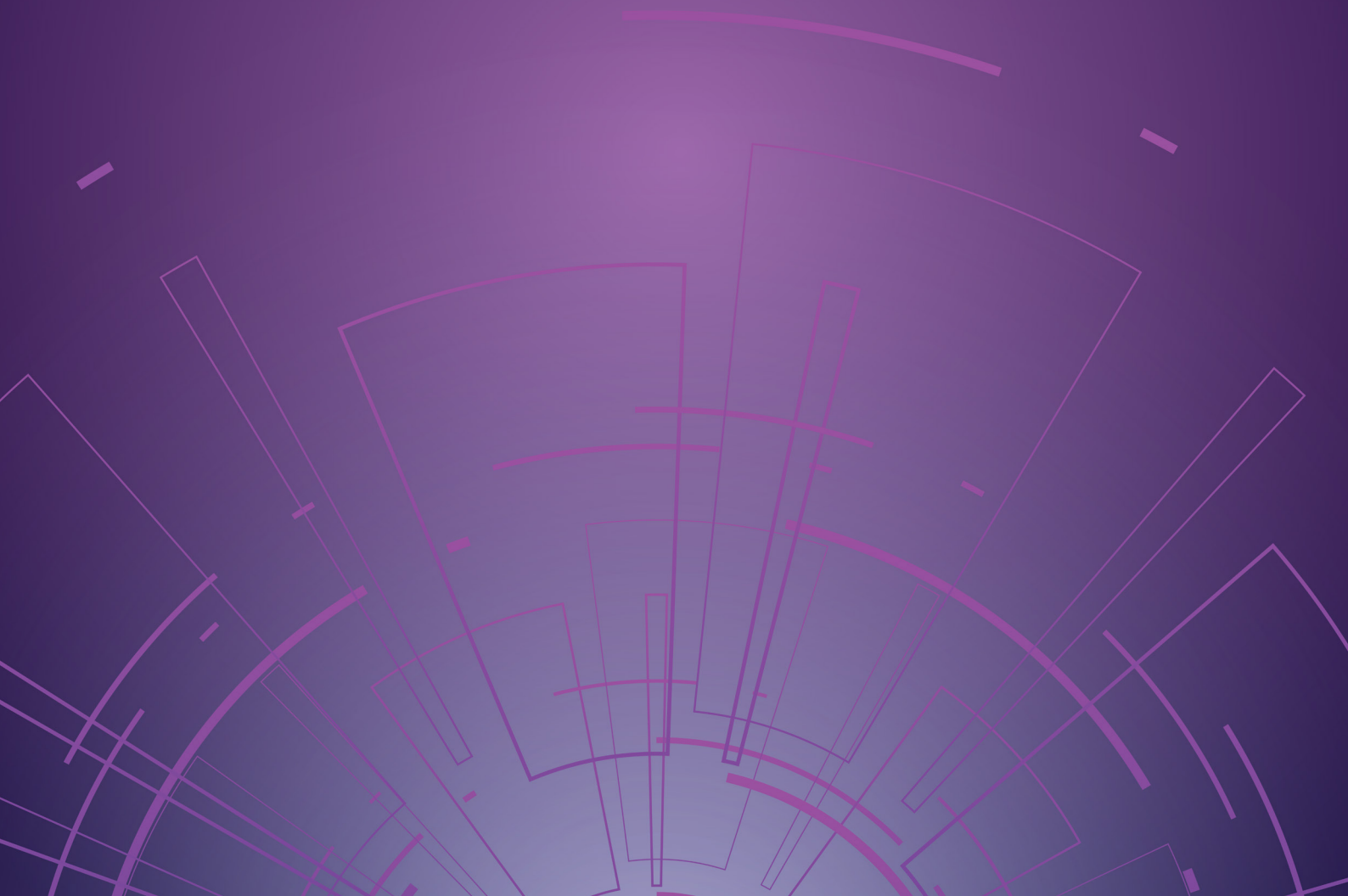
RAND EUROPE

QINETIQ

Command and Control in the Future

Concept Paper 4: C2 Enablers

Rebecca Lucas, Stella Harrison, Conlan Ellis, James Black,
Ben Fawkes, Martin Robson, Alan Brown, Edward Keedwell



For more information on this publication, visit www.rand.org/t/RRA2476-4

GLOBAL
STRATEGIC
PARTNERSHIP

The Global Strategic Partnership (GSP), a consortium of research, academic and industry organisations that is led by RAND Europe, provides ongoing analytical support to the UK Ministry of Defence.

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

RAND® is a registered trademark.

Cover image: Adobe Stock

Preface

This is the fourth and final in a series of four Concept Papers (CPs) examining how Command and Control (C2) will manifest in the future. The other papers in this series are as follows:

- **CP1:** James Black, Rebecca Lucas, John Kennedy, Megan Hughes, & Harper Fine. 2024. *Command and Control in the Future: Concept Paper 1 – Grappling with Complexity.* Santa Monica, Calif.: RAND Corporation. RR-A2476-1 (henceforth Black et al. (2024));
- **CP2:** Rebecca Lucas, Conlan Ellis, James Black, Peter Carlyon, Paul Kendall, John Kendall, Stephen Coulson, & Louis Jeffries. 2024. *Command and Control in the Future: Concept Paper 2 – The Defence C2 Enterprise*. Santa Monica, Calif.: RAND Corporation. RR-A2476-2 (henceforth Lucas et al. (2024)); and
- **CP3:** Conlan Ellis, Rebecca Lucas, Ben Fawkes, Martin Robson, Alan Brown, Edward Keedwell, & James Black. 2024. *Command and Control in the Future: Concept Paper 3 – Conceptualising Command and Control as a Capability*. Santa Monica, Calif.: RAND Corporation. RR-A2476-3 (henceforth Ellis et al. (2024)).

This report is part of a series commissioned by the Development, Concepts and Doctrine Centre (DCDC). As of 1 July 2024, DCDC has been renamed as 'Defence Futures', part of the Integration Design Authority. The overarching study is being delivered by DCDC, Strategic Analysis Support Contract (SASC) with the Global Strategic Partnership (GSP), a consortium of UK and international research organisations providing strategic analysis and academic support to the DCDC within the UK Ministry of Defence (MOD). This paper is intended to capture the findings of a second phase of the study and has been drafted on the assumption that it will be read by an audience with some familiarity with C2 and the preceding papers in the series. Equally, it is intended to feed into the other three papers in the series and therefore stops short of providing fulsome coverage of all aspects of thinking about C2 in the future, including the development of concrete recommendations.

The GSP is led by RAND Europe, part of the RAND Corporation, an independent, not-for-profit research institute that aims to improve policy and decision making through objective research and analysis. RAND's clients include Allied governments, militaries, inter- and non-governmental organisations, and others with a need for rigorous, independent, interdisciplinary analysis.

For more information about RAND, the SASC, or this study, please contact:

James Black

Assistant Director – Defence & Security Research Group,

RAND Europe

t. +44 (0)1223 353 329 / e. jblack@randeurope.org

Summary

This Concept Paper (CP) is the final paper in a series of four on Command and Control (C2) in the future.

The first three papers set out the operating environment within which the C2 enterprise exists and how its systems will need to evolve in the future

The previous three CPs looked at high-level enablers and challenges for the Defence C2 enterprise and the associated systems needed to adapt to a fast-changing threat environment and technology landscape:

- CP1 explored how the complexity of the future operating environment (FOE) out to 2040 is likely to shape the demands placed on C2. It provided a baseline of understanding to inform subsequent papers, which explored various and specific aspects of C2 capability requirements in more detail.[1]
- CP2 focused on the resulting opportunities, challenges and dilemmas that the FOE will likely pose for design of the future C2 enterprise, given the attributes and traits it will need to develop.[2]
- CP3 argued for the need to conceptualise C2 as an integrated capability to be proactively cultivated and stress-tested across Defence, rather than a set of individual systems or siloed activities.[3]

This final paper considers the enablers required for C2 systems out to 2040

Building on the findings of previous papers, CP4 takes a closer look at enablers for C2 systems in the future, in terms of technological, personnel-related, and organisational characteristics.[4] It also looks at how Defence can ensure that C2 capability continues to evolve and adapt to the demands of the FOE. It ends by drawing out a series of key implications for the UK Ministry of Defence from the findings of all four CPs.

Technology-focused enablers

In consultation with DCDC, the research team identified a series of technology areas of particular interest. This CP does not set out to make a comprehensive list of emerging technologies that may be relevant to C2, nor to prescribe which technical solutions or architecture Defence should adopt. Rather, it aims to discuss a small selection of areas to illustrate how the disruptive effects of technology more broadly might impact on C2 systems in the future, and what new capabilities and properties this innovation might enable.

[1] Black et al. (2024).
[2] Lucas et al. (2024).
[3] Ellis et al. (2024).
[4] See Chapter 1 for a definition of C2 systems as applied throughout this paper. Please see Ellis et al. (2024) for a more detailed discussion of C2 as a socio-technical system.

Table 0.1 Technology areas, capabilities and properties for consideration

Examples of relevant technology areas	Technology capabilities and properties
• Artificial intelligence (AI), machine learning (ML), and human–machine teaming (HMT) • Encryption • Sensing, observation, and analysis • Computational approaches • Information and knowledge management • Synthetic environments	• Aids for decision making and sense making in complex situations • Support for more effective conduct of multi-domain operations (MDO) and collaboration with partners across government (PAGs), international allies and partners, industry, academia, and others • Automation and autonomy within C2 • Information processing and communications • Enablers of adaptability, agility and resilience

Source: SASC research in consultation with DCDC.

People- and organisation-focused enablers

Change is about more than technology. C2 capability is a complex socio-technical system comprising variously and dynamically configured social and technical components. With this in mind, Chapter 3 considers some of the organisational and human enablers for C2 systems in the future. Drawing on the findings of CP2 and CP3, which considered these issues in more detail, this fourth and final paper summarises their findings along several topical lines identified in consultation with DCDC, namely:

- Nurturing a new Defence mindset and culture that supports operating effectively in the face of complexity, uncertainty and change;
- Overhauling approaches to education and training;
- Promoting new ways of working;
- Bolstering resilience and adaptability across all levels of the enterprise; and
- Designing different headquarters functions that are fit for a variety of purposes and contexts.

Deprecated enablers

Crucially, Defence must not just focus on what is new when exploring the future of C2; it must also think about how best to manage or phase out legacy systems and ways of doing command and control. To this end, Chapter 4 considers how Defence can ensure that its C2 systems continue to evolve and keep pace with a fast-changing operating environment. This includes identifying areas of existing capability that face obsolescence, and considering how Defence can speedily but gracefully handle the transition from legacy ways of working to next-generation capabilities and technologies.

The paper concludes with key implications drawn from the complete series

Insights and implications for the UK MOD to consider as it develops a new Joint Concept Note (JCN) and vision for C2 in the future include:

- **To cope with the challenges of the FOE, the C2 enterprise of the future will not be a single entity, but rather a more fluid assemblage of varying combinations of individuals and organisations.**
- **Collaboration with diverse partners is going to be a key enabler of C2 systems in the future.** Defence will often need to work with partners that it can neither command nor control, in the traditional military and hierarchical sense. Instead, Defence will need to be more comfortable and capable when it comes to building and sustaining non-hierarchical relationships to enable partnership, cooperation and coordination with a more diverse set of actors.
- **The Defence C2 enterprise will therefore need to consist of multiple, parallel C2 systems that can adapt effectively,** possibly moving flexibly and efficiently between different C2 approaches to handle diverse challenges and circumstances. This will necessitate the enterprise being able to add and integrate new partners quickly, while selectively sharing information to protect confidentiality. It will also need to include modes to enable security, survivability and resilience in denied and degraded environments, such as reversionary modes or more hardened methods of communication. It is likely that multiple C2 states will exist and even operate in parallel, with C2 in more benign settings (e.g. in more permissive environments) configured rather differently from C2 in degraded and denied environments.
- **Defence is going to need profound change both to ways of organising as well as more intangible aspects of institutional culture** to make this more flexible and adaptable C2 enterprise work in practice. This is unlikely to be a one-time shift, but rather a long-term effort to transition to a culture of continuous learning and development to adapt to changing circumstances. At a minimum, Defence culture will need to support increased tolerance for risk, experimentation and challenge (where appropriate), as well as a mindset of increased comfort and familiarity with complexity, uncertainty and systems thinking.
- **The necessary organisational changes will not be possible without a united effort from Defence, including clear endorsement and investment from leadership.** In order to bring the whole Defence enterprise along in this change, leadership will need to clearly communicate the desired changes across Defence and be open to feedback and challenge from all levels of the organisation, as well as observers and stakeholders outside of Defence.
- **Training, education and rigorous and challenging exercises will be key enablers for a range of capabilities,** including fostering cooperation and collaboration, both across Defence and with PAGs, international allies and partners, industry and others; practising operating under considerable pressure, risk, change and uncertainty; testing and integrating new technologies and ways of working; and challenging and adapting existing ways of working.

- **To guide this process of learning and iteration, and support resource prioritisation, Defence will need metrics and a shared understanding of what 'good' looks like** in different contexts so it can make the difficult decisions and trade-offs that will be inherent in C2 systems.
- **Defence will need to put in greater effort to recruit, develop and maintain a variety of skills crucial to C2 systems in the future**, including a range of technical skills and knowledge; working with advanced technologies, including AI and ML; comfort with decision making under uncertainty; 'soft' interpersonal, management and communication skills; and a willingness and ability to challenge existing models or decisions appropriately and constructively.
- **Given intense competition for such skills from across Defence, PAGs and the private sector, Defence must consider how best to motivate, develop and retain this talent.** This will in part require consideration of how to get the most from a Whole Force approach – and from use of AI, ML and HMT, including autonomy and automation, as means to bolster workforce productivity and offset a potential lack of resource (e.g. manpower).
- **Defence will need to understand C2 as a socio-technical capability that needs to be continuously cultivated in a holistic and proactive manner** to join up efforts from across Defence and achieve shared goals. This requires an empowered Senior Responsible Owner, with sufficient resource, as well as incentives to drive accountability and coherence for those tasked with delivering associated change and development activities at lower levels.
- **Defence cannot simply 'purchase' new C2 technologies off-the-shelf and should be wary of promises of any technological 'silver bullet'. Rather, it will need to invest in and iterate new capabilities and systems over time while responsibly managing the transition away from legacy ways of working.** Achieving these objectives will require collaboration and cooperation across the whole of the Defence enterprise, including industry and academia, to help participants understand Defence's needs and cooperate in seeking to meet them.

The GSP hopes that identifying these implications will contribute to Defence's ongoing thinking on the future of C2 capability more broadly, as well as DCDC's specific work regarding the update and replacement of the current JCN 2/17 on Future C2.

Table of contents

Figures, tables, and boxes

Figures

Tables

Boxes

Abbreviations

AI	Artificial Intelligence
AIM	Analog Iterative Machine
AR	Augmented Reality
BAT	Bi-directional Adapter for Tracking
BCS3	Battle Command Sustainment Support System
C2	Command and Control
C5I	Command, control, communication, computers, cyber and intelligence
CIM	Coherent Ising Machine
COA	Course of Action
CP	Concept Paper
CPU	Central Processing Unit
DARPA	Defense Advanced Research Projects Agency
DCDC	Development, Concepts and Doctrine Centre
DLODs	Defence Lines of Development
DOD	Department of Defense (US or Australia)
Dstl	Defence Science and Technology Laboratory
E2C	Edge to Cloud
EMS	Electromagnetic spectrum
EW	Electronic Warfare
FAWS	Fully Autonomous Weapons Systems
FOE	Future Operating Environment
GMTI	Ground Moving Target Indicator
GPU	Graphics Processing Unit
GSP	Global Strategic Partnership
HMT	Human–Machine Teaming

HQ	Headquarters
IHL	International Humanitarian Law
IML	Interactive Machine Learning
IOpC	Integrated Operating Concept
IR	Integrated Review
ISTAR	Intelligence, surveillance, target acquisition, and reconnaissance
JADC2	Joint All-Domain Command and Control
JCN	Joint Concept Note
KM	Knowledge Management
LAWS	Lethal Autonomous Weapons Systems
LOAC	Law of Armed Conflict
M&S	Modelling & Simulation
MDO	Multi-Domain Operations
ML	Machine Learning
MOD	Ministry of Defence
MR	Mixed Reality
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
OAI	Office for Artificial Intelligence
PAG	Partners Across Government
PQC	Post-Quantum Cryptography
QKD	Quantum Key Distribution
RAS	Robotic and Autonomous Systems
RQ	Research Question
S&T	Science and technology
SAR	Synthetic Aperture Radar
SASC	Strategic Analysis Support Contract
SE	Synthetic Environment
SQEP	Suitably qualified and experienced personnel
STEM	Science, technology, engineering and mathematics

TTPs	Tactics, techniques and procedures
UK	United Kingdom
US	United States
VR	Virtual Reality
XR	Extended Reality (includes AR, MR, VR)

Acknowledgements

The authors are grateful to the Ministry of Defence (MOD) for their sponsorship of this study and their support and input throughout the research, including feedback on a draft of this concept paper. In particular, thanks are owed to Lt Col. Robert Kace, Lt Col. Ed Vickers and Cdr Leif Hansson of the Development, Concepts and Doctrine Centre (DCDC) – the latter posted from the Swedish Armed Forces, given DCDC's dual role as the Swedish Concepts and Doctrine Centre – as well as Mr Peter Houghton and Mr Jack McEvoy of the UK's Defence Science and Technology Laboratory (Dstl). Despite these valued contributions, any errors or omissions remain the sole responsibility of the authors.

1. Introduction

This chapter introduces the backdrop against which this paper was commissioned, as well as the definition of Command and Control (C2) used throughout the wider study for DCDC. It then situates this final paper of the series within the context of the preceding papers, before laying out research questions and the methodology employed to explore them.

1.1. Background and purpose

Effective and resilient C2 is essential to the basic functions of Defence and to the planning and execution of military operations, up to and including warfighting. While the nature of war remains constant, the character of warfare continues to evolve.[5] So too do the types of mission that the military are expected to undertake, the political, legal and ethical considerations that are placed on decision making, and the threats, technologies and human factors that influence approaches to C2.

According to the UK MOD, C2 is the 'pre-eminent Joint Function' and 'critical to enabling joint action'.[6] Ensuring that C2 systems and organisations remain fit for purpose in the face of changing operational demands is thus essential to maintaining the advantage of the UK and its North Atlantic Treaty Organization (NATO) allies over any competitor. To this end, DCDC is conducting ongoing analysis through an initiative known as Project Mimisbrunnr that aims to inform future thinking about C2, including a planned update to *JCN 2/17: Future of Command and Control*.[7] For continuity, and in consultation with DCDC, the research team used the understanding of C2 as shown in Box 1.1.

Box 1.1 Understanding of C2 as provided by DCDC

'A dynamic and adaptive socio-technical system configured to design and execute joint action' whose purpose is thereby '[to] provide focus for individuals and organisations so that they may integrate and maximise their resources and activities to achieve desired outcomes'.

Source: DCDC based on UK MOD (2017).

[5] Von Clausewitz (2006).
[6] Commander Joint Forces Command (now UK Strategic Command), quote. in JCN 2/17. UK Ministry of Defence (2017).
[7] Other Joint Concept Notes (JCNs) tackle the related topics of human–machine teaming (JCN 1/18), information advantage (JCN 2/18) and multi-domain integration (JCN 1/20). See: UK Ministry of Defence (2018a), (2018b) and (2020b).

To support this effort, DCDC asked the Strategic Analysis Support Contract (SASC) to produce four exploratory papers in 2023 and 2024 to:

- Inform Defence thinking and experimentation about C2 in the future;
- Explore Defence integration with partners across government (PAGs) and international allies and partners to deliver decision advantage from 2030 onwards (i.e. in the timeframe of the Capstone Concepts currently under development); and
- Research innovative approaches and revolutionary future understandings of the Integrated Operating Framework.[8]

As agreed with DCDC, to answer these questions, the team produced four exploratory concept papers (CPs) over the course of 2023 and 2024. The three previous papers concerned the following:

- CP1, *Grappling with Complexity*, aimed to provide an indication of how the complexity of the future operating environment (FOE) (specifically out to 2040) is likely to shape the capability requirements for C2. It provided a baseline of understanding to inform subsequent papers, which explore specific aspects in more detail.[9]
- CP2, *The Defence C2 Enterprise*, focused on the resulting opportunities, challenges and dilemmas for the design of the future C2 enterprise, and involved significant input from across the SASC.[10]
- CP3, *Conceptualising C2 as a Capability*, focused on the need to conceptualise C2 as a capability that must be proactively cultivated and maintained across Defence, rather than as a set of individual capabilities or activities.[11]

1.2. Paper 4: Enablers for C2 in the future

Considering the demands of the FOE and the desired characteristics of the C2 enterprise, this fourth and final paper in the series focuses on those underpinning capabilities that will be required to enable C2 socio-technical systems in the future.[12] It considers the types of technologies that may underpin C2 systems in the future, as well as the personnel qualifications and organisational characteristics that should be cultivated. However, it stops short of prescribing exactly what the eventual technical solutions, architecture, structures, or processes should look like (as that is out of scope of this CP). The paper also discusses how these various enablers may need to interact and mutually reinforce each other to allow future C2 systems to function most effectively to meet Defence's future requirements.

[8] As outlined in the Integrated Operating Concept (IOpC). UK Ministry of Defence (2020a).
[9] This paper is referred to in footnotes throughout as Black et al. (2024).
[10] This paper is referred to in footnotes throughout as Lucas et al. (2024).
[11] This paper is referred to in footnotes throughout as Ellis et al. (2024).
[12] For more information about the demands of the FOE, see Black et al. (2024). For more information about the desired characteristics of the C2 enterprise, see Lucas et al. (2024). For a longer discussion of the importance of understanding C2 as a socio-technical system, see Ellis et al. (2024).

1.2.1. Research questions

The research questions (RQs) provided by DCDC for this paper are as follows:

- **RQ1: Technology-focused enablers.** What do the new challenges and demands of the FOE and desired characteristics of the C2 enterprise demand of future technology-focused C2 enablers? This RQ includes ten areas of specific technology interest for particular consideration. Further information on all of these areas is available in Chapter 2.
    - What is new, what remains relevant, and what has changed?
    - How will future C2 enablers need to operate or function differently from today?
- **RQ2: People- and organisation-focused enablers.** What do the new challenges and demands of the FOE and desired characteristics of the C2 enterprise demand of future people and organisation C2 enablers? This RQ also includes four specified areas of inquiry, elaborated upon in Chapter 3.
    - To what extent should other enablers remain people-centric?
    - What can we do for people who will become practitioners, as an enabler for better C2?
- **RQ3: Deprecated enablers.** Given the new challenges and demands of the FOE and desired characteristics of the C2 enterprise, what prior enablers need to be deprecated and removed or deleted from the C2 enterprise and its collective use and memory?
    - What C2 enabling functionality will become irrelevant?
    - How do we get rid of legacy ways of thinking and working (e.g. 'we have always done it this way')?

This paper also includes an overarching set of implications for DCDC and the UK MOD when thinking about how to design C2 in the future, based on the full series of four CPs.

1.3. Methodology

This paper relied extensively on internal workshops among the research team, as well as targeted literature reviews. Following consultations between RAND and DCDC, the team held a series of internal workshops to discuss the RQs and how they might best be addressed. This included leveraging the diverse expertise across the team, consulting with those individuals with relevant scientific and technological expertise. Team members then conducted a series of targeted literature searches to inform their allocated area of research. Following the completion of this research, the team conducted another round of internal workshops to ensure shared understanding and make a final determination about areas of focus for the research paper. At this stage, non-RAND members of the research team, including individuals from the University of Exeter and Aleph Insights, contributed written inputs for their allocated area of research. The RAND team then consolidated and streamlined these inputs into a single paper.

Following preparation of the paper, DCDC hosted a seminar in Shrivenham on 12 December 2023 with a range of people with expertise in C2 enablers. This included participants from across NATO and Sweden (which subsequently became a NATO member as of 7 March 2024). This provided an opportunity to

discuss and obtain feedback on an initial version of this paper, building on the model employed with seminars for each of the preceding CPs. Based on the expert feedback collected during the seminar, the research team produced a revised version of this paper.

1.4. Structure of the document

This paper is structured as follows:

- **Chapter 2** discusses technology-focused enablers, with a focus on specific technology areas followed by the capabilities and properties they offer (RQ1);
- **Chapter 3** examines people- and organisation-focused enablers, including defence culture, learning and training, ways of working, and resilience (RQ2);
- **Chapter 4** discusses deprecated enablers, including how to retire old functionalities that are no longer relevant and adopt new ways of working (RQ3); and
- **Chapter 5** sets out conclusions and key implications for UK Defence based on all four CPs.

A full bibliography is included, along with a full list of workshop participants as an annex.

2. Technology-focused enablers

This chapter seeks to explore a range of near-future and next-generation technologies that may serve as key enablers to C2 capability in the future. It considers how these technologies may impact the C2 enterprise – itself a complex socio-technical system – as well as the feasibility of implementation and associated risks.

Of note, the applications of the technologies discussed here are just potential ways in which they might be applied to improve the efficiency and utility of C2 systems. It is important to avoid techno-determinism, which is all too often a feature of discussions about the future of C2.[13] The future of C2 will be shaped as much, if not more, by human and organisational factors as by the availability of new technical solutions to operational challenges.[14] Further, increased reliance on technology comes with its own drawbacks. In CP1, it was noted that the introduction of new technologies could increase the complexity of the C2 system, leading to the emergence of critical dependencies and vulnerabilities.[15] The advancement of surveillance technology presents new challenges for survivability in a more transparent battlefield, while AI, through problematic feedback loops, cascading effects, and escalation risks, may lead to increased complexity and uncertainty in decision making.[16]

As such, technology should be understood as just one element of capability, and its translation into useful applications and use cases will be conditioned by actions taken across all Defence Lines of Development (DLODs). To this end, this chapter first provides a high-level outline of projected trends in relevant technology areas, before considering some of the capabilities and properties they may offer to the C2 enterprise of the future.

[13] DCDC Shrivenham Workshop, 12 December 2023.
[14] Ellis et al. (2024).
[15] Black et al. (2024).
[16] Black et al. (2024).

Table 2.1 Summary of technology enablers, capabilities and properties

Examples of relevant technology areas	Technology capabilities and properties
• Artificial intelligence (AI), machine learning (ML) and human–machine teaming (HMT) • Encryption • Sensing, observation and analysis • Computational approaches • Information and knowledge management • Synthetic environments	• Aids for decision making and sense making in complex situations • Support for more effective conduct of multi-domain operations (MDOs) and collaboration with partners across government (PAGs), international allies and partners, industry, academia and others • Automation and autonomy within C2 • Information processing and communications • Enablers of adaptability, agility and resilience

Source: SASC research in consultation with DCDC.

It is important to note that the intention of this chapter is not to create a comprehensive list of next-generation and generation-after-next technologies that may impact C2. Rather, it aims to consider how the disruptive effects of such technologies might have an impact on, and be leveraged by, the C2 organisations of the future as they seek to improve the quality of decision making.

2.1. Technology areas of interest

2.1.1. Artificial intelligence, machine learning and human–machine teaming

AI, ML and HMT are increasingly involved in C2 systems for a variety of purposes. Augmented decision support systems enable humans to maintain control over internal decision-making processes and work to improve decision making in the face of growing complexity of the FOE, while handing off certain tasks to machine agents or algorithms where possible to reduce the cognitive load on personnel involved in all levels of C2 systems. Such systems conceal the time-consuming training and data-processing stages from users but help to offer prioritised and actionable insights to assist humans in making informed decisions in the face of uncertainty and/or time constraints. However, there are still lingering concerns about trust in AI/ML, such as a lack of explainability, traceability or suitable validation and verification methods, which will be discussed further below.[17] There are a range of options to achieve HMT and to integrate AI and autonomy, presenting ranging benefits and trade-offs.[18] Examples are provided below.

Interactive optimisation

Interactive optimisation is a field that combines human decision making with optimisation methods to achieve a beneficial outcome for a specific task. The overall structure involves an optimisation model that specifies the decision variables, objectives, and constraints of the problem.[19] Upon instantiation, the system in question uses data provided to determine the bounds for possible outcomes of the optimisation model. Optimisation procedures then generate intermediate results and solutions that can be presented to the user

[17] This is highlighted as a cross-cutting impact facing C2 systems and organisations in Black et al. (2024).
[18] See Ellis et al. (2024) for a longer discussion of trade-offs related to having humans in or on the loop depending on the situation and decisions involved.
[19] Meignan et al. (2015).

in batches for validation. The user may either select one of the options provided or provide feedback, prompting the optimisation process to generate a new set of options that meet the new criteria.

While such collaboration can help models suggest a wider range of solutions to human decision makers, there are still key decisions that may restrict this approach's application in certain areas of C2. For example, the starting point for interactive optimisation is problem analysis, where the boundaries, criteria and limitations of the optimisation problem are established: this requires collecting relevant information, identifying useful data, and defining decision-making criteria.[20] However, creating a model that accurately represents all aspects of the decision makers' problem can be challenging. Clausewitz's fog and friction retain their power even in an increasingly transparent battlespace[21]; creating an accurate problem analysis is therefore often impossible or at least impractical in the time, resource and operating conditions on hand.[22] Establishing initial parameters could nevertheless enable these systems to be used for decision support in the near-term and evolve into greater roles in C2 systems over time.

Interactive machine learning

Interactive machine learning (IML) is an ML approach similar to interactive optimisation that involves active participation from humans in the model design and implementation process. End-users participate in model building from the start by providing training parameters, examining outputs and giving feedback on intermediate results in an iterative manner.[23] Human input can be further incorporated at different stages of the ML process, where the level of interactivity can be tailored to user requirements. IML can play an important role in helping to process and analyse the large amount of information on which C2 systems in the future are likely to rely.

While this solves some problems associated with interactive optimisation, obstacles remain. For example, it has been observed that users may struggle to interpret and modify a system's output effectively without sufficient explanations or guidance.[24] This issue is part of a larger, multi-decade debate on the relationship between interpretability, explainability and transparency, and how explanations can enhance human understanding of AI-based systems.[25] This issue and possible solutions are discussed in-depth in CP2: one key takeaway was the need to ensure that the necessary suitably qualified and experienced personnel (SQEP) and subject matter experts are positioned across Defence; technical SQEP in particular is a challenge given the shortage of relevant skills and high demand from the private sector for AI/ML skills.[26] If this barrier is overcome, however, IML may be particularly useful for C2 activities that involve processing large amounts of data, where both humans and ML systems lack a complete understanding of the situation. For example, users could interact with such systems to better identify areas of focus and eliminate incorrect data or

[20] Meignan et al. (2015).
[21] This is without considering how the combination of increased competition for access to the electromagnetic spectrum (EMS) and the proliferation of both kinetic and non-kinetic effectors to the UK's adversaries might in fact make the battlespace more opaque in some areas or respects – adding to fog and friction by making it harder for dispersed forces to communicate, and frustrating attempts to reach back to headquarters at higher echelons.
[22] Hughes (2020).
[23] Wondimu et al. (2022).
[24] Pfeuffer et al. (2023).
[25] Pfeuffer et al. (2023). For further discussion, see Gregor & Benbasat (1999).
[26] See Lucas et al. (2024), Sections 3.1.3 and 3.2.4, for an in-depth discussion of the required skills for the Defence enterprise to cope with this challenge.

findings; this would in turn enable such systems to provide comprehensive summaries or interactive visualisations to support decision making.

Decision support systems and interactive systems

Decision support systems are already able to engage in shared decision making to great effect across a variety of fields and applications, including C2.[27] As AI/ML technologies have continued to advance, so too has this technology rapidly grown in capability. For example, in 2020, a human–AI system for skin cancer diagnosis was demonstrated to outperform both the AI system and physician when they were operating separately.[28] While the effectiveness and design of such systems depend on the specific application, systems based on HMT have the potential to enhance outcomes, engage users and successfully leverage AI for complex decision-making tasks. These systems could highlight areas of risk or opportunity, raise alarms, suggest courses of action and evaluate a range of potential decisions.[29] Elements of prediction or forecasting might also be used to provide limited 'look-ahead' for decisions for resource use and decision effectiveness, while monitoring and tracking, as discussed in Box 2.1, provide information about asset availability.

Box 2.1 BAT advanced object-tracking method

The Bi-directional Adapter for Tracking (BAT) is a new advanced ML method for tracking objects in all-weather, complex and harsh environments. The BAT method is valuable for C2 applications as it offers flexibility and adaptability in real-time decision making. With a precise image tracking system, it's possible to monitor and track assets and movement accurately, providing real-time intelligence and highlighting potential threats or opportunities. Commanders can use this information to make informed decisions about resource allocation or mission planning in response to impending or ongoing events.

Source: Cao et al. (2023).

In contrast to automation, the aim for HMT is to complement and enhance the human operator's abilities, rather than replace them. Consequently, implementation is inherently a user-driven process. User-centred design principles should be applied to ensure that the technology is designed with the end-user in mind.[30] This requires that the user is intimately involved in the design process, participates in testing, and is able to provide feedback that is acted upon to improve the technology. This should be accompanied by sufficient and continuous training and support to help users learn how to use the technology effectively, improve and maintain proficiency over time, and induct new users.

Of note, decision support systems may not provide an irreplaceable capability within a C2 system, but rather play a supporting function. If, for example, an AI-augmented layer of decision-making capabilities were to fail, in an HMT system in which human analysis remains at its core, decision making could still occur.[31] Still, like all enabling technologies, the sudden loss of this added functionality could significantly degrade decision making if it induced paralysis or panic. Extensive training and established ways of working

[27] See Ellis et al. (2024) for a longer discussion of the importance of conceptualising C2, and any underpinning systems or technologies, as part of a socio-technical system.
[28] Tschandl et al. (2020).
[29] Naseem et al. (2017).
[30] Ottley et al. (2022).
[31] Aversa et al. (2018).

without the technology would therefore be needed to ensure agile decision making continued, albeit in a somewhat degraded form, even if technical systems failed.

Defence needs to continue to engage in defining the range of possible applications and uses for decision support technologies within C2 systems. This can then be used to inform the design of the automated aids, and evaluate their efficacy based on clearly delineated aims. Defence should continue to adapt the technology to changing needs and contexts, exploiting better and more advanced mechanisms as they are created, and as strategic priorities shift over time.

2.1.2. Encryption

Maintaining the security and confidentiality of communications is a key consideration for effective C2; encryption is therefore an important area of technology for developing the capability to conduct C2 effectively in the future. Future encryption is heavily impacted by new computational approaches. Extrapolating from current advances in quantum computing technology, it is expected that encrypted messages will be at risk of being decrypted within the next decade or two.[32] Traditional encryption methods, which use prime factor encryption, create an encryption key out of two prime factors 313 digits in length.[33] To decrypt a message, these two prime factors need to be known by the receiver; calculating these factors takes an estimated 16 million years even using a supercomputer – hardly a practical timeline. However, the rapid processing speeds enabled by quantum computing mean that this form of encryption will in time become vulnerable to quantum decryption. As discussed in Section 2.1.4, qubits may perform many calculations simultaneously, exponentially increasing the amount of information that can be processed; this dramatically reduces the time required to decrypt encryption based on prime factors from years to minutes. As a result, many hackers and military adversaries are collecting and saving vast troves of encrypted data now, with the hope that it will still be valuable once quantum decryption is possible.[34]

In response, many countries are working to rapidly develop and implement methods for 'post-quantum' cryptography (PQC). For example, the US National Institute of Standards and Technology (NIST) has been working since 2016 to develop global standards for PQC.[35] Following the initial publication of those standards, the US Congress has recently passed legislation recommending that all agencies should transition to an encryption method applying PQC by 2035.[36] The UK National Cyber Security Centre (NCSC) similarly issued guidance on the need for organisations across both the UK public and private sectors to migrate to PQC in a 2020 White Paper; the initial guidance was recently supplemented with additional information about algorithm and protocol choices.[37] In tandem with guidance, there has also been government-funded research and development (R&D) in this area: NIST has run programmes to develop PQC, for example, including a prize competition to find new encryption algorithms.[38] One example of the four algorithms that met NIST's standards can be seen in Box 2.2.

[32] Mosca & Piani (2022).
[33] Sarnaik & Ansari (2018).
[34] Townsend (2022).
[35] NIST (2023a).
[36] Parker (2023); The White House (2022).
[37] NCSC (2023)
[38] NIST (2022).

Box 2.2 Kyber-CRYSTALS

Kyber is a finalist in the NIST PQC project. Its security is dependent on the difficulty of solving the learning-with-errors problem, a widely used mathematical problem in the field of cryptography, over module lattices. Applying lattice-based cryptography is still considered quantum safe as so far there has been no difference in capabilities between traditional and quantum algorithms in solving these problems. This algorithm is already being applied by the private sector. Amazon now supports modes that apply Kyber in the Amazon Web Service's Key Management Service, while the Signal Protocol, which is utilised by WhatsApp and other messaging services, incorporated Post-Quantum Extended Diffie-Hellman (PQXDH), a post-quantum encryption algorithm based on Kyber, in 2023.

Source: Kyber (2023); Song et al. (2023); Newsroom (2023).

Post-quantum cryptography is a key enabler for future C2 systems. As C2 systems continue to rely heavily on the information and communication technologies discussed in this paper, it is imperative that sensitive data is encrypted appropriately using methods that maintain its confidentiality. Therefore, it is crucial to prioritise the implementation of PQC standard encryption in future C2 systems.

2.1.3. Sensing, observation and analysis

Novel advances in sensing, observation and analysis technologies provide an increasing number of inputs to C2 systems. Even in the current operating environment, advances in technology are significantly increasing the number of platforms, systems and resources available for intelligence, surveillance, target acquisition and reconnaissance (ISTAR). They therefore play a key role in forming a comprehensive picture of the FOE to inform decision making. Two areas where this is most relevant are uncrewed systems across the domains (e.g. uncrewed vehicles for persistent overwatch without exposing humans to hostile threat environments) as well as significant advances in novel sensors. Such sensors could be integrated into both crewed and uncrewed platforms.[39]

Such technologies are only expected to continue to advance in capability: progress in novel areas such as quantum sensing, which promises to be significantly more sensitive than current systems, could enable significant advances in certain areas of sensing, augmenting the existing mix of sensors in use with the military for different roles (e.g. electro-optical, infrared, thermal, acoustic, spectrometers, Ground Moving Target Indicator [GMTI] and Synthetic Aperture Radar [SAR] systems, etc.).[40] Additionally, progress has also been made towards the development of sensors for previously difficult-to-access areas and challenging environments. Examples include space-based sensors, such as space-based SAR; sensors for subterranean environments (e.g. tunnels, spaces beneath rubble or natural cave systems); or advances in magnetic, acoustic and gravity sensors to support anti-submarine warfare.[41]

Relatedly, new solutions for energy generation and/or storage also offer enhanced options for loitering, persistent surveillance, and research on microbe-based devices for environmental monitoring offer a host of opportunities to deploy more diverse, effective sensing technologies.[42] In short, technological advances are pointing to an FOE with the possibility of near-ubiquitous sensing across multiple domains – assuming

[39] Brand (2023).
[40] Wilson (2018); Van Amerongen (2021); Watling (2023).
[41] Van Amerongen (2021); Wilson (2018); DARPA (2023b).
[42] DARPA (2023a).

that the data generated can then be transmitted, processed, fused and made sense of at the speed of relevance, especially in the context of an increasingly contested electromagnetic environment.[43]

This proliferation of sensors, however, presents a significant challenge for C2 practitioners, given the volume of data that is going to be generated. Identifying relevant and valuable data points, triangulating information across multiple different networks, and determining with whom that information must be shared – with what level of priority, given competition for bandwidth and given the tactical risks associated with transmitting and thus exposing nodes in the network to possible detection and targeting by the adversary – will be a significant challenge.[44] Here, a third development regarding the use of AI to help analyse data from multiple sources and sensors becomes critical for enabling Defence to capitalise on the immense amounts of data being presented.[45] The use of AI and ML to process and synthesise data, and present findings to humans in a digestible manner, therefore represents a key enabler for exploiting the full potential benefits of new sensors in contributing to enhanced situational awareness and decision making. The use of non-AI novel technologies may also offer similar capabilities, an example of which is discussed in Box 2.3.

Box 2.3 Wetware technology

Wetware technology, currently under development by Koniku and Cortical Labs, is a method for processing information that combines silicon chips with living neurons. Wetware is reportedly capable of solving complex problems using hundreds or thousands of brain cells in a dish, which leads to a more efficient computing device that can learn complex tasks and improve performance more quickly than AI. This creates a platform for processing vast amounts of data coming from the web of sensors across all the military domains, leading to situational analysis and decision support for C2 in near-real-time and reducing information overload of decision-makers. This allows anyone to make on-the-fly decisions, not just commanders, which can give troops a competitive advantage. Moreover, Wetware technology could be used to improve early detection capabilities in a variety of ways. For instance, used as a smell-based sensor, Wetware devices could provide advancements in detecting explosives and toxins from distances much greater than currently possible.

Source: Koniku (2023); Cortical Labs (2023); Aruchami (2023); Le Page (2021); Hernandez (2022).

2.1.4. Computational approaches

C2 systems in the future are likely to need the ability to gather, synthesise and analyse vast amounts of information from diverse sources at speed; in fact, such a capability underpins many of the other technology areas discussed in this chapter. Present computing, however, suffers from limitations in terms of its speed and capacity, despite the progress made in recent years in both cloud and edge computing.[46] These limitations have driven a search for new computational approaches that enable the processing of more data, more quickly: examples include quantum computers,[47] Wetware,[48] the D-wave superconducting quantum

[43] Black et al. (2022); Watling (2023). Of note, the proliferation of sensing does not necessarily mean eliminating (or even significantly reducing) the fog of war. See Black et al. (2024) for a more detailed discussion of how complexity and uncertainty are expected to persist, and even increase, in the FOE.
[44] Hewlett Packard Enterprise (2023).
[45] Robinson et al. (2023).
[46] Present computing approaches are often characterised by a central processing unit (CPU) that executes instructions and data retrieved from its memory; computers with a CPU are constrained by a phenomenon known as the Von Neumann bottleneck. This limitation refers to the lag between when the CPU requests data and when it can receive that data from memory in order to execute an instruction. Rosenberg (2017); Castelvecchi (2023).
[47] Mandelbaum (2023).
[48] Koniku (2023); Cortical Labs (2023).

annealing system,[49] neuromorphic computers,[50] coherent Ising machines (CIMs),[51] polariton simulators[52] and the Analog Iterative Machine (AIM).[53] One example, neuromorphic computers, is discussed in further detail in Box 2.4.

Box 2.4 Loihi 2 neuromorphic computing chip

Intel's Loihi 2 neuromorphic computing chip is designed to simulate the human brain's structure and pattern-recognition ability. Loihi's architecture is designed to function more efficiently than conventional computing systems, allowing for real-time processing of sensor data to improve target recognition, optimise operations and improve resource allocation. The chip's low energy consumption and small size are intended to make it well-suited for use in handheld devices, enabling decision makers to process information and make quick decisions on the battlefield. The Loihi 2 chip may be particularly useful for pattern-recognition tasks, such as image recognition and classification, as well as natural language processing in applications such as sensors, drones and Internet of Things devices, ultimately increasing the tactical efficiency of C2 systems.

Source: Intel (2023); Cutress (2021).

As another example, CIMs can solve complex problems that are extremely demanding to solve with conventional computing architecture. Similarly to neuromorphic computing, this has the potential to greatly increase the speed of decision making in support of C2 systems such as communication network optimisation,[54] target detection,[55] resource allocation[56] and satellite constellation design.

Alongside developments in more traditional computing (e.g. attempting to continue the historic rate of progress in cost-vs-processing speed described in Moore's Law, despite recent struggles to build ever-denser chips), such approaches could therefore provide significant benefits for future C2 systems. These could potentially include improved situational awareness and faster decision making as part of the socio-technical C2 system, as discussed in the two examples above.[57] This section will explore how future computational approaches may benefit C2 specifically through the example of quantum computing.

Quantum computing and C2

Quantum computing presents alternatives to classical computers for certain specific applications, primarily providing the increased processing efficiency necessary to run specialised algorithms at high speed. Overall, it offers many potential benefits to the military across a range of applications in future C2 systems, from cryptography and secure communications to modelling and simulations, sensing, data processing, and more. While current commercial quantum computing capability and capacity are still limited, this is a rapidly

[49] D-Wave (2023).
[50] Intel (2023); IBM Research (2023a, 2023b and 2023c).
[51] Yamamoto et al. (2017); Honjo et al. (2021). The CIM is an analogue simulator specifically designed to efficiently tackle complex combinatorial optimisation problems based on the Ising model. The types of complex problems that the CIM can solve are computationally demanding to solve using conventional computing architectures, but the CIM leverages quantum annealing techniques to efficiently reach optimal solutions.
[52] Berloff et al. (2017).
[53] Ballani (2023).
[54] Resende (2003).
[55] Harrison et al. (2022).
[56] Menshikh et al. (2018).
[57] Such technologies include graphics processing units (GPU) and other Reduced Instruction Set Computer (RISC)-based approaches in classical computing. For more discussion of C2 as a socio-technical system, please see Ellis et al. (2024).

developing field, and perhaps subject to the highest expectations of all the novel computation approaches.[58] Quantum computing relies on qubits, which can hold both zeros and ones at the same time, known as a superposition. Unlike classical computers, which must perform a new calculation for each variable change, quantum computers can therefore explore numerous paths simultaneously due to their larger working space. This capability allows quantum computers to perform many calculations and functions significantly faster than classical computers.[59]

The advancement in computational capabilities will potentially entail a massive adjustment of capabilities and application. Quantum computing specifically can also enable much higher speeds of processing, including more accurate simulations of complex systems of the kind described in CP1.[60] These can be used to test and refine courses of action and strategies before they are implemented in the field, supporting C2 and decision making in the face of an uncertain and complex FOE. This will likely be tackled through traditional methods and the creation of customised systems to enable visualisation and interaction with large-scale datasets.

The promised capabilities of quantum computing have led to a race for quantum supremacy, largely by large private-sector actors but also involving state players such as China.[61] The MOD has recognised the importance of quantum computing in documents such as the Integrated Review (IR) and the IR Refresh.[62] However, additional attention and investment are needed.[63] The MOD could greatly enhance ongoing industry and academic efforts by offering access to testing and validation infrastructure, such as test centres, as well as providing end-user military operators with accelerated access to these technologies.[64]

2.1.5. Information and knowledge management

Among the most promising applications of AI/ML technologies is improving the efficiency of information management (IM) and knowledge management (KM), defined in the box below. IM and KM therefore provide significant support for the informed, robust decision making that underpins C2 systems.

Box 2.5 Definitions of Information and Knowledge Management

Information Management (IM) refers to the infrastructure and processes utilised for the collection, management, preservation, storage and delivery of information. Information includes hard data, such as facts and figures.

Knowledge Management (KM) refers to similar infrastructure and processes as IM, but instead relating to knowledge, broadly defined as practices, processes, and ways of behaviour. 'Knowledge' is a contested subject, and the applications of technologies in this space are still evolving.

Source: Association for Project Management (2024a); Association for Project Management (2024b).

[58] Note that there are multiple applications of quantum technologies, including the creation of novel sensors and encryption systems. These will be discussed throughout in the relevant sections.
[59] McKinsey (2023b).
[60] Black et al. (2024).
[61] Parker et al. (2022).
[62] UK Government (2021); UK Government (2023).
[63] McMahon (2022).
[64] Van Amerongen (2021).

As Box 2.5 outlines, the concepts do overlap. KM systems, however, are harder for organisations to successfully implement than IM systems, given the challenge in successfully translating knowledge for dissemination as opposed to information. KM as a process can generally be summarised into three steps:

- Knowledge creation, where organisations or individuals identify and document existing or new knowledge to be circulated;
- Knowledge storage, where the knowledge is held for future distribution, either using an IT system or within an individual (especially when tacit knowledge is involved); and
- Knowledge sharing, where a variety of processes (only some of which are technical) can be used to distribute knowledge to end-users across the organisation or enterprise.[65]

While technology may underpin KM systems, as with the C2 enterprise as a whole, these are still inherently socio-technical systems.[66] The technical means of creating, storing and sharing information are often underpinned by ML technology.[67] Systems using such technology can process and gather large amounts of data, keep content up to date, and leverage important metrics. Of note, emerging KM systems can already collate, find and share key processes, vastly speeding up the knowledge-sharing step of the process.[68] Additionally, generative AI (e.g. large language models) has taken this a step further by moving from accessing and compiling existing information to analysing and synthesising data, generating summaries, frequently asked questions, and answers to questions.[69] These processes are likely to only continue to advance, increasing the amount of data they are able to accommodate and the speed at which they can process as relevant technologies continue to improve.

While these advances allow significantly expanded and accelerated access to knowledge, they have also created new pitfalls. The greatest of these may be instances where such systems generate inaccurate information, including so-called hallucinations.[70] There therefore needs to be oversight of KM systems, which would require a balancing of efficiency and accuracy, as well as clear guidance over when generation, as opposed to the access and analysis of primary source data, is acceptable. Continuous feedback as well as quality assurance mechanisms with human monitoring could reduce risk of inaccurate information or data, as well as ensuring that IM and KM practices are continuously improved to benefit C2 capability in the future.[71] The fact that Defence operates in a context in which adversaries will be proactively trying to poison datasets and subvert AI and KM systems to undermine the UK's C2 – reducing trust in decision making – adds yet further challenges on top of those facing commercial and civilian organisations, necessitating both technical solutions and Tactics, Techniques and Procedures (TTPs) to help mitigate this risk to C2 in military operations.[72]

[65] IBM (2023c).
[66] See Ellis et al. (2024) for a lengthy discussion of the importance of viewing C2 as a socio-technical system.
[67] Eliyahu (2020).
[68] Eliyahu (2020).
[69] McKinsey (2023a).
[70] IBM (2023a)
[71] Eliyahu (2020).
[72] Black et al. (2022).

Systems also need to focus on maximising accessibility to ensure that the proposed benefits of KM systems are realised fully, addressing the human and organisational factors that determine uptake of any new technology, especially in a unique setting such as Defence. For example, while users across the international defence community have frequently attempted to use KM systems to support logistics, these have often generated a mixed user experience and therefore have not remained in use.[73] Box 2.6 discusses previous efforts to improve logistics through KM systems, and the perceived reasons for failure.

Box 2.6 Battle Command Sustainment Support System (BCS3)

The US Army previously used the Battle Command Sustainment Support System (BCS3) as an automated materiel management system. The system displayed a three-dimensional picture using topographic details selected by the user, augmented with analytical and decision support tools to ultimately provide a worldview of tactical units. Despite its promises to provide key C2 capabilities to the Army Battle Command System, BCS3 was largely abandoned in favour of basic spreadsheets and databases after its widespread deployment in 2010. Post-deployment interviews from Operation Iraqi Freedom revealed negative attitudes towards BCS3, with personnel expressing frustration with the system and choosing to use it sparingly or not at all.

Source: Sachariason (2009); Poland (2012).

Like all technologies discussed in this paper, developing the SQEP required to properly understand and utilise the technology is necessary to realise any benefits for C2: without personnel who can manage and interpret the results of these KM systems, and without appropriate levels of trust (mixed with healthy scepticism) in those systems' outputs, the technology alone is often insufficient.[74]

2.1.6. Synthetic environments

Creating immersive environments is a critical element in providing impactful training and mission rehearsal, which are important for effective C2.[75] Advances in computing, data science and analytics, and virtual (VR), augmented (AR) and mixed reality (MR) technologies (collectively known as XR) all create new opportunities for delivering this in a more realistic and cost-effective way, alongside more traditional live training and exercises. There are also considerable investments being made by a number of militaries, as well as the private sector, with the goal of expanding the use of synthetic environments (SEs) to include other purposes that support C2. These include sophisticated modelling and simulation (M&S) and probabilistic analysis to inform capability, force development or operational planning decisions, or – at a higher level of ambition and technical difficulty – live analysis of data feeds from the battlespace and exploration and visualisation of the likely outcomes from possible Courses of Action (COAs) as part of real-time decision support to headquarters.[76] One example of this is discussed in Box 2.7 below.

[73] Sachariason (2009); Poland (2012).
[74] Balis & O'Neill (2022). For more discussion of the challenges of doing so, as well as recommendations for how it might be achieved, please see Lucas et al. (2024) and Ellis et al. (2024).
[75] See Lucas et al. (2024) and Ellis et al. (2024) for longer discussions about the importance of training, mission rehearsal and exercises, as well as creating low-stakes environments for experimentation and failure.
[76] BAE Systems (2023).

Box 2.7 Meta and Reality Labs

The MOD and NATO have highlighted the trend of an increased development of blended simulations of live, virtual and synthetic environments, in which the boundaries between these three domains becoming increasingly blurred. Leading the way in consumer application of this technology is Reality Labs, the VR development division of tech conglomerate Meta. In 2023, the newest consumer VR headset, Meta Quest 3, was released with a new focus on mixed reality, combining domains and allowing for the visual mapping of virtual assets over the real world. Meta plans to take this technology a step further through the planned 2025 release of 'AR glasses', which would allow for augmented reality free from the physical burden of current VR headsets. This technology could allow for access to critical information and data in real-time, without having to take eyes off the battlefield.

Source: Robertson (2023); Lloyd & Kearse (2023); Heath (2023).

Today, there are two broad variants of synthetic environments, though the state of the art continues to advance at pace. Low-temporality and -resolution SEs, for example modelling brigade-level scenarios, are used to train military leaders and assist tasks such as wargaming.[77] This approach has been used for decades, but is limited in comparison to the high-fidelity SEs, sometimes referred to as Computer Generated Forces, which can model real-time force movements and interactions in immersive settings such as flight simulators.[78] Militaries thus currently have access to either highly detailed, physics-based modelling and simulation of low-level tactical units (e.g. between opposing combat aircraft and their onboard sensors and weapons), or a lower level of analytical granularity and robustness when simulating how larger numbers or sizes of unit interact in a battlespace, let alone integrating influences that cannot easily be distilled into physics-based models (e.g. human decision making or political, social and economic system dynamics).

Once moving beyond such models, the complexity and dynamism of the FOE, as well as the availability of data, become key challenges. In addition – and despite positive efforts under way through entities such as NATO to promote standards in areas such as High-Level Architecture Interoperability to enable federated simulation – legacy SEs and the models that underpin them are still all too often stove-piped, unable to integrate and interact with each other due to either technical, commercial, policy or other barriers (e.g. classification).

To address these challenges, and exploit the opportunities offered by advances in technology, new programmes seek to bring together both tactical and operational- or strategic-level simulations, as well as to integrate simulators from across the domains and Services.[79] Advances in computing, cloud technology, data science and AI are all expected to provide significant advancements in M&S capabilities and complexity, potentially leading to SEs that are inherently scalable where previous constraints related to processing power and connectivity have been eliminated.[80] Further, it is possible that the current generation of virtual SE tools is the last to be developed by specialist defence simulation companies.[81] Consumer gaming offers superior engines, tools and processes, such as the VR technologies discussed in Box 2.7, providing increased accessibility and application. Synthetic environments could also provide a cost-effective training resource for domains that have traditionally been resource-heavy to train for – such as space and the deep ocean.[82]

[77] Perey et al. (2022).
[78] Perey et al. (2022).
[79] BAE Systems (2023).
[80] Perey et al. (2022); Lloyd & Kearse (2023).
[81] Lloyd & Kearse (2023).
[82] BAE Systems (2023).

SEs therefore offer myriad opportunities for C2 practitioners to practice and test their approaches and ideas. As discussed in previous CPs, such opportunities are key for a variety of C2 purposes, including education, learning from failure in low-stakes environments, and acquiring comfort with complexity.

2.2. Capabilities and properties offered by emerging technologies

In addition to exploring specific technology areas that seem promising, Defence is also working to combine multiple new and old technologies, alongside other DLODs, to produce novel capabilities of relevance to C2 in the future. These systems can, in turn, be combined into systems of systems, and associated concepts, doctrine and TTPs developed to support their use on operations. This more challenge-driven approach to developing technological enablers is also an important path to pursue, and one that complements the more 'blue skies' approaches to technology development discussed in the previous section. It further offers a way of organising the relevance and urgency of the technology areas discussed in the previous section.

2.2.1. Aids for sense making and decision making in the face of complexity

As discussed in the previous CPs in this series, the need for more effective or efficient C2 decision-making processes and supporting models has risen. One suggested approach for modelling C2 networks themselves is applying a physics-inspired model to simulate a C2 decision-making network.[83] One such model, the Kuramoto model, is a well-established numerical model in the field of condensed matter physics, designed to simulate complex interacting systems.[84] As discussed in CP1, the complexity and dynamism of the FOE is likely to require personnel at multiple levels[85]; this results in a complex C2 network with multiple decision makers, as well as myriad data sources and nodes across networks (e.g. sensors, forward-deployed military forces, PAGs, allies, industry, etc.).[86]

Models such as the Kuramoto model therefore treat each human and information entity as agents with unique objectives and constraints. Each of these agents continuously cycles between perception and action states while communicating with other agents in the network. Based on these assumptions, this model is able to provide an evaluation of agents' potential actions and interactions; this often serves to highlight the need for short network paths and multiple alternative paths in order to create robust C2 networks.[87]

At present, such optimisation models are computationally heavy, and take a long time to run; this prevents them from providing real-time decision support. Such challenges are known as 'combinatorial optimisation problems'.[88] However, there is currently significant research ongoing to develop alternative computing architectures that can solve these types of simulation problems at speeds many orders of magnitude faster than current computers.[89] These systems, known as analogue simulators, use the inherent properties of

[83] Kalloniatis et al. (2020).
[84] Kalloniatis et al. (2020).
[85] See Grisogono (2020) for a discussion on how AI could be used to address complexity across multiple scales.
[86] Black et al. (2024).
[87] Dekker (2017).
[88] Hoos & Stützle (2005).
[89] For an outline of intended aims of these simulations, see Cirac & Zoller (2012).

nature to simulate the mathematical optimisation problem.[90] Examples include CIMs,[91] polariton simulators,[92] and AIM,[93] the latter discussed further in Box 2.8.

Box 2.8 Analog Iterative Machine

The AIM is a type of photonic computer developed by Microsoft Research in Cambridge, UK, that can solve complex optimisation problems with a 100 times speed-up compared to the latest GPU. The AIM uses different intensities of light to compute multiple sources of data in the same location, making it faster and more efficient than binary computing. With the ability to process vast amounts of data and solve complicated problems, the AIM holds significant potential in supporting C2 in military operations. The AIM's efficient optimisation capabilities can be used to solve numerous C2 problems, such as allocating resources, scheduling military operations, optimising energy usage and sustainability, and optimising weapon–target pairing, leading to increased survivability through speed. Additionally, a cloud-based service provides decision makers with immediate access to the computational power of the AIM without carrying the physical device, which could be targeted by adversaries, on the battlefield.

Source: Kalinin et al. (2023); Welch (2023); Microsoft Research (2023).

A number of the technology areas discussed in Section 2.1 can therefore be used to support effective C2 in the FOE by providing support to decision makers. Further advances play a key role in increasing the speed and processing power available for highly complex models to provide such support in a more timely manner.

2.2.2. Support for more effective conduct of Multi-Domain Operations (MDO) and collaboration with partners

C2 in the future will likely need to support MDO, the aim of which is to apply novel combinations of capabilities and effects across multiple dimensions to achieve desired outcomes. It also intends to create multiple dilemmas and vulnerabilities for an adversary.[94] Technology can serve as a key enabler for achieving this objective. The modern battlespace demands a more comprehensive understanding of a complex and dynamic FOE that can be shared across different stakeholders. Progress towards this can be achieved through a network of sensors that detect pertinent changes in the environment and adversary activities, track personnel and weapons, and locate additional assets as needed, across multiple domains. Users can then filter information based on what is needed to make decisions across different echelons and settings.[95]

While this sea of information may seem overwhelming, it could be made manageable by the alternative computing architectures discussed in Section 2.1.4. Such advances should enable computing devices to fuse and analyse vast amounts of data in real-time, providing informed predictions or forecasts and presenting COAs or recommendations to help commanders make the best decisions for the given situation, while potentially providing a more complete picture (or pictures) of the environment and activity across multiple domains.[96] Box 2.9 provides one example of how this might be achieved.

[90] Johnson et al. (2014).
[91] Yamamoto et al. (2017); Honjo et al. (2021).
[92] Berloff et al. (2017).
[93] Ballani (2023).
[94] See Black et al. (2024) for a longer discussion of the relevance and importance of MDO in the FOE.
[95] Bellasio et al. (2021).
[96] For further discussion of how the FOE will likely remain a congested space and the fog of war will very much remain a challenge, please see Black et al. (2024).

Box 2.9 Leidos' Edge to Cloud (E2C) ecosystem

Leidos' Edge to Cloud (E2C) ecosystem consists of an edge processing component, tactical cloud processing and strategic cloud processing. These components can enable the integration of data from various sources, including integrated sensors and devices, to enable real-time data analytics and enhanced situational awareness to support decision making. The E2C ecosystem can provide network control, secure data and interface with a broad range of data sources, including voice, video and data. In a multi-domain operating environment, E2C can support C2 through real-time intelligence, surveillance, reconnaissance and precision targeting, providing military decision makers with timely and accurate situational awareness of the operating environment.

Source: Leidos (2023a, 2023b); Shepherd Media (2023); Edwards (2023).

Additionally, it is hoped that advanced ML algorithms will provide insights that allow commanders from different dispersed units or domains to draw upon weapons, personnel and equipment as needed to overcome any challenges they may face during conflict – moving towards Joint All-Domain Command and Control (JADC2)'s ambitious vision of seamless integration between 'any sensor, any shooter'. Algorithms trained on real conflict data, for example, may be able to detect potential escalations in conflict earlier than is currently possible, increasing resilience through preparedness against specific adversary actions.[97]

There is a great deal of optimism that future technologies will provide commanders with a real-time, live feed of the battlefield, allowing them to make informed decisions and stay ahead of the adversary, and enabling the optimisation not only of ISTAR, fires and manoeuvre complexes, but also of logistics, sustainment, and replenishment of expended materiel through automated procurement from industry. However, aside from questions of whether or not this is in itself a desirable goal, achieving anything like this is an ambitious – some might say unrealistic – vision in the real world and will require careful integration and assurance of SQEP as part of a user-centric development approach. This will help to ensure that the outputs of AI and autonomous systems are properly considered and integrated into decision-making processes, so that they may best analyse and predict patterns within the data, raise alerts, and suggest COAs for human consideration. Similarly, implementation will require associated changes in organisational structures and institutional culture, as discussed in CP3; such changes must therefore be considered as part of the design process.[98]

2.2.3. Automation and autonomy within C2

C2 automation refers to the use of technical systems and technologies that can operate with potentially very limited human intervention to support decision making and coordination in military operations. Such systems may eventually have a significant degree of autonomy, with AI agents operating largely independent of human intervention. Alternatively, they could be semi-autonomous, meaning that the machines operate with a more significant level of human oversight and control (i.e. with the human either 'on the loop', monitoring and vetoing systems' actions where needed, or 'in the loop', exercising more direct control).[99] As examined in Box 2.10, ML can now rapidly surpass human capabilities in problem-solving scenarios, possibly bringing tactical and operational advantages to significant automation of certain tasks.

[97] Trivedi et al. (2021).
[98] See Ellis et al. (2024).
[99] Scharre (2018).

Box 2.10 MuZero and Efficient Zero Algorithms

A new algorithm with planning capabilities that can respond to unknown situations has been developed by researchers at DeepMind and University College London. Although existing planning algorithms have successfully defeated humans at games like chess, they all rely on knowledge of the environment, such as the rules of the game. MuZero was tested on the games Go, chess and shogi, and despite not being given the rules of the games, it performed equally as well as other planning algorithms. Building off this model, the EfficientZero algorithm was applied to Atari games, and with two hours of in-game training achieved 194.3 per cent of mean human performance and 109.0 per cent of median performance.

Source: Schrittwieser et al. (2019); Ye et al. (2021).

While automation can be extremely valuable in certain areas of C2, such as automated logistics systems that can track and manage supplies and equipment in real-time, the application of near complete automation of C2 in combat settings has undergone frequent criticism. A recent report exploring the use of AI and ML in operational decision making in the Russia–Ukraine War, for example, observes that the current technologies can benefit military decision making only when paired with human analysts who understand the context behind a problem.[100] Further, AI consistently fails in capturing or responding to human intangibles in decision making, namely ethical and moral considerations that are highly relevant for C2 decision making.[101] There are many examples of these in the literature, with the most famous being the 'self-driving trolley problem', which questions how AI should weigh human lives, amidst a range of intervening variables, such as age, social value, and compliance.[102] Additionally, decisions about kinetic action executed without sufficient human input currently violate international humanitarian law (IHL) and the Law of Armed Conflict (LOAC) rules on lethal autonomy. The development or deployment of Fully or Lethal Autonomous Weapons Systems (FAWS or LAWS), either now or in the future, is therefore an especially contentious topic.[103] The UK's Defence AI Strategy represents the UK's aspirations for safe and responsible use of AI; as technology continues to evolve, however, so too will the guidance around it.[104]

In addition to the constraints of IHL and LOAC, ethical concerns have surged with the rise of AI and the growth of AI-assisted and automated decision making. As such, there are a range of advisory policies that aim to mitigate this risk. In the UK, this research is led by organisations such as the Ada Lovelace Institute, the Alan Turing Institute, the Open Data Institute and the Oxford Internet Institute, which all produce studies, surveys, reviews and policy positions regarding AI ethics. Additionally, the government guidance has been active on this issue, participating in debate and publishing a National AI Strategy and framework for the ethical use of AI in 2021; issuing the Defence AI Strategy and set of associated ethical principles in 2022; and hosting the world's first AI Safety Summit at Bletchley Park in 2023.[105] To best mitigate ethical risks, experts have cautioned that it is essential that the future C2 enterprise is held accountable to a specific framework to guide implementation without overly stifling innovation.

[100] Robinson et al. (2023).
[101] McKendrick & Thurai (2022); Retter et al. (2016); House of Lords (2023).
[102] Thomson (1985). To explore this problem in further depth, see Moral Machine (2023).
[103] Davison (2017); Krause (2021).
[104] UK Ministry of Defence (2022).
[105] Central Digital and Data Office, Cabinet Office & Office for Artificial Intelligence (2021); UK Ministry of Defence (2022); HM Government (2022); HM Government (2023).

2.2.4. Information processing and communications

Communications capabilities are intrinsically tied to the concept of C2, sometimes to the point of extending the acronym to C4, i.e. command, control, communications, and computing. Through providing the function of necessary interaction to enable effective command, communication capabilities are essential for successful coordination between tactical units, and between tactical, operational and strategic units of command. Given the fast pace of development of information processing, handling and communications systems, ensuring their continued resilience is essential to ensure that these capabilities continue to serve as an enabler, rather than a barrier.

As has been discussed in previous CPs, Defence will need to collaborate with organisations outside of Defence, and even outside of government.[106] Working in collaboration where capabilities already exist in PAGs or the private sector can be significantly more time- and cost-efficient than trying to cultivate such capabilities within Defence. However, it requires Defence to continuously foster connections with a diverse range of organisations. Such relationships can be fostered through a range of mechanisms, as discussed in CP2 and CP3.[107] It is again necessary to highlight that Defence must adopt a collaborative approach for effective coordination between stakeholders partaking in the future C2 enterprise; depending on the context, it may not be possible or appropriate to try to control its partners, and Defence will therefore need to compromise effectively to navigate differences and ensure successful outcomes.[108]

Equally, Defence requires ways of communicating and sharing information and networks with diverse actors who may lack necessary permissions to enable access, while maintaining appropriate levels of security.[109] This becomes particularly important in the complexity of the FOE as the UK and its allies and partners seek to integrate operations across multiple domains. This is both a technical/architectural and a cultural and policy challenge. One potential solution, for example, could include shifting from a philosophy and architecture based on securing networks towards one focused on differential levels of security for packets of data within shared networks, i.e. exploiting data-centric security or zero-trust architectures. This would enable a greater diversity of users to collaborate seamlessly despite differing levels of access, and support work across all levels of classification.[110] Similarly, Defence might wish to strike a new balance between the risks of not securing classified information and the risks of not sharing it with PAGs, allies and partners in a timely manner and thus missing windows of opportunity to secure the tactical or strategic advantage – a change in mindset for a risk-averse organisation like Defence.[111]

Another option to improve information processing is through edge computing. Edge computing refers to the computer framework that brings processing and analytical capabilities close to the 'edge' of the cloud, near the edge devices: devices that are deployed in the physical world to carry out tasks such as sensing, actuating and controlling.[112] Through this process, edge computing accelerates access to data from video,

[106] For more information, see Lucas et al. (2024).
[107] See Ellis et al. (2024) and Lucas et al. (2024) for discussions of the importance of collaboration and recommendations for how this can be achieved through education, exercises and other means.
[108] See Lucas et al. (2024) for a discussion of the SQEP that may be required to build and foster these relationships.
[109] Marrow (2023).
[110] Cook et al. (2022).
[111] Hitchens (2020).
[112] Xiao et al. (2019); IBM (2023b).

voice, sensors, targeting and reconnaissance.[113] As discussed in Section 2.1.3, the military operates a vast network of sensors, which alongside vehicles containing large amounts of microchips constitute a massive network of edge devices.

However, edge computing has challenges with integration in existing technical systems: due to diverse operating systems and software, different network topologies and disparate protocols, traditional security frameworks cannot be directly migrated to edge computing systems.[114] Consequently, to implement edge computing, the priority objective must be to enable the military to leverage edge computing technology without having to completely overhaul their current infrastructure. One option to achieve this is to focus edge computing on a specific category of edge devices, such as those which enable rapid information transfer across different geographic locations, for example, as the range of devices may be less diverse.[115] Other options may include enhancing sensor processing at the edge.

When considering the enablers examined in this paper, the challenge of how to apply them in practice should be in the forefront. This is a matter of designing and implementing the appropriate systems in the appropriate places – considering the scale of computing power needed, the infrastructure needed, signature management and expeditionary requirements. This is not a new issue, but a persistent challenge: ensuring successful military planning for the implementation of technology.[116] However, contemporary military planning has a self-reinforcing relationship with the other enablers discussed so far in this paper. While good planning is required for successful implementation, these enablers can help to achieve good planning. Determining the optimal allocation of resources in a C2 context requires a holistic approach that considers a variety of enabling factors, such as data analytics, simulation, decision support systems and human expertise.[117] This allocation should be consistent with existing military organisational goals and objectives, including policies on resource allocation, decision-making processes and performance metrics. However, both processes and output are still vulnerable to disruption by adversaries or natural phenomena, threatening implementation. One possible solution to this is discussed in Box 2.11.

Box 2.11 Quantum Key Distribution (QKD) trial network

Toshiba and BT's landmark QKD trial network between EY's two offices in London enables the secure transmission of data over public networks, future-proofing data communication and ensuring reliable and ultra-secure quantum cryptography solutions. This innovative technology applies the fundamental laws of quantum physics for ultra-secure encryption, protecting networks and data from cyber-attacks, making QKD an important component for military security. This technology could support C2 by enabling reliable communications of data over long distances and increasing the data transmission rate. For example, with QKD, military personnel could use real-time data analytics to assess a situation or capability from a remote location. Moreover, through its unique transmission of quantum keys, QKD can also be used to ensure a military's infrastructure is safe by detecting attempted cyber-attacks and responding to them promptly.

Source: EY (2022); Toshiba (2023).

One solution to this may be system robustness. In this context, a resource allocation is considered robust if it can maintain specified system performance features even when there are disruptions in specified system

[113] Molinari (2023).
[114] Xiao et al. (2019).
[115] Molinari (2023).
[116] Størdal (2020).
[117] DCDC Shrivenham Workshop, 12 December 2023.

parameters.[118] Robustness applies to both processes and outputs: diversity, modularity and redundancy may provide this from a technical process perspective, while ensuring the generation of outputs may require political will or contextual SQEP.[119]

2.2.5. Enablers of adaptability, agility and resilience

Previous papers in this series have considered the importance of agility, adaptability and resilience for C2 in the future. Besides the wider complexity of the FOE, as discussed in CP1, a consistent driver of the need for these attributes is the impact of emerging technologies on the C2 enterprise. However, it is also necessary to consider how emerging technologies can also serve as an enabler for this process, by creating a feedback loop where appropriately integrating new technologies can help support better practices and preparedness for absorbing future technology.

As outlined in CP3, it is important to recognise that C2 capability is ultimately human-centred whilst at the same time we desire to utilise and take advantage of the most advanced technology available and appropriate.[120] As a result, the primary technological enablers to achieve this are tools and platforms that effectively facilitate collaboration and communication within Defence, as well as tools that can encourage training and development for staff at all levels.[121]

Further, as was discussed in CP1, communications and connectivity in the FOE are likely to be denied and degraded.[122] Future C2 systems and their underpinning technologies must therefore be built with resilience in mind, and that might include, for example, exploiting the blockchain technology introduced in Box 2.12.

Box 2.12 Blockchain: resilience against cyber-attacks and system failures

Blockchain is a decentralised, digital ledger technology that is designed to enable secure, transparent and tamper-proof transactions and data storage. This resilient technology can continue to function even in the event of a cyber-attack or system failure. This is because blockchain utilises decentralised and distributed storage, verification and encryption mechanisms that make it extremely difficult to manipulate or corrupt data. Even if one node in the network fails or is compromised, the other nodes can still maintain a copy of the ledger, ensuring data integrity and system resilience. In a military setting, blockchain could be used to create a distributed ledger of all logistics transactions, allowing different military units and divisions to track the location, status and availability of resources such as fuel, ammunition and food supplies in near-real-time. This could help to optimise distribution and allocation of critical resources across multiple domains of operation, improving the efficiency, speed and safety of military operations.

Source: Sharma et al. (2023); Gaur et al. (2023).

Additionally, the rapid pace of technological change means that systems may need to adapt to both new threats and new opportunities. This can be fostered through performing different types of analysis, including user testing and vulnerability analysis, and integrating feedback to enhance the technology, as well as designing for ease of updating (e.g. with key aspects of C2 capability being more dependent on software than hardware, and with prudent procurement practices such as avoidance of vendor lock-in and establishment of contracting mechanisms that enable rapid delivery of updates). Education, training and exercises can also expand user comfort with alternative ways of operating and develop the necessary SQEP

[118] Ali et al. (2004).
[119] Capano & Woo (2018).
[120] See Ellis et al. (2024), Chapter 4, for an in-depth discussion of how this may be achieved.
[121] See Section 2.8 for discussion of this topic.
[122] See Black et al. (2024) for further discussion of likely barriers to communications technologies in the FOE.

for dealing with complex situations.[123] Again, technology is not a silver bullet; it introduces its own vulnerabilities and dependencies, as well as sources of fog and friction, that Defence must mitigate against.

2.3. Conclusion

This section considered a series of different technology areas that were identified as being of interest for C2 systems in the future. It also considered a series of capabilities and properties of interest to C2 that emerging technologies may offer. While it by no means pretends to be a comprehensive overview of the field, it aims to provide sufficient information to provoke consideration of what different technology fields may offer in terms of enabling C2 in the future. However, significant investment of resource, as well as research, testing and experimentation, will be necessary to optimise and adapt C2 systems.[124]

[123] See Lucas et al. (2024) on the importance of education, testing and experimentation in developing personnel comfort with uncertainty and reversionary modes.

[124] See Black et al. (2024), Lucas et al. (2024) and Ellis et al. (2024) for additional conversations about the type of effort and resource likely to be needed to incorporate these and other areas of emerging technology into effective C2 systems.

3. People- and organisation-focused enablers

While the technology areas discussed in Chapter 2 are certainly key enablers for C2 systems in the future, the previous CPs have discussed at length the importance of conceptualising C2 as a socio-technical system, and of cultivating C2 as a capability that must be nurtured continuously over time. To this end, it will be equally important for Defence to ensure that it has appropriate SQEP in place for both its uniformed military and civilian personnel, as well as the requisite organisational structures and institutional culture to support the C2 workforce's continuous learning, development and performance.

As these topics are covered in more detail in the previous CPs, this chapter provides brief explanations, along with cross-references to the appropriate CPs.

3.1. Nurturing a culture in Defence that supports operating effectively in the face of complexity, uncertainty and change

Given that the FOE is likely to be characterised by complexity and uncertainty, a culture that supports personnel operating in that environment will be a key enabler for C2 systems in the future.[125] GSP personnel who worked on this paper, as well as participants in the three DCDC seminars held for this project, agree that changes to institutional culture are a prerequisite for successful C2 systems in the future.[126] The experts consulted for this project concurred that, throughout Defence, the culture will need to better acquire, enable, incentivise and retain personnel with the requisite perspectives, approaches and SQEP.[127]

Additionally, cultural change will be necessary to support an environment of continuous learning, development and experimentation that will enable C2 systems to continuously adapt to the challenges and opportunities presented by the FOE. CP2 argued the need for both technical skills, which allow for the ability to critically engage with emerging technologies and incorporate them within the C2 workflow, and 'soft' skills, such as relationship building, empathy, cultural understanding and the ability to exert influence.[128] Further, CP2 included a detailed discussion of the importance of increasing risk tolerance to experiment with new organisational structures, technologies, and approaches to designing and

[125] For further discussion of complexity in the FOE, please see Black et al. (2024).
[126] DCDC Canberra Workshop, June 2023; DCDC Stockholm Workshop, March 2023; DCDC Shrivenham Workshop, December 2024.
[127] See Ellis et al. (2024) for more discussion of this topic.
[128] Lucas et al. (2024).

implementing the C2 enterprise.[129] Building on this, CP3 described ways to create designated spaces for incentivising risk-taking and experimentation, such as sandpits, sandboxes and prize competitions.

3.1.1. Ensuring career paths that incentivise development and maintenance of expertise and technical ability

Meeting the need for appropriate SQEP, particularly in dynamic teaming, critical systems thinking and key technology areas, is widely recognised as a challenge for Defence.[130] However, there has simultaneously been recognition that current career paths in Defence do not necessarily incentivise or even enable personnel to develop and maintain these skill sets.[131] Previous RAND research has identified the need for creating career tracks that not only reward personnel for the development and maintenance of critical skills, but also enable individuals to continuously grow and achieve seniority in experience, professionalism and leadership without leaving their more specialist roles.[132] For example, research pertaining specifically to the cyber workforce has identified the importance of enabling personnel to 'stay on the keyboard'.[133] RAND surveys of US Air Force personnel found that 'the majority of interviewees supported…corresponding flexibility' offered by alternative promotion paths.[134] Such changes would enable Defence to keep individuals in particular areas where they can apply their expertise, rather than requiring a transfer to more supervisory roles to achieve seniority. It would also enable Defence to better reward personnel for developing both the technical and soft skills that previous papers have identified as critical for C2 in the future.[135]

This need for more tailored career tracks has already been recognised in the Haythornthwaite Review: recommendations 50 to 52 speak to the importance of identifying and designing appropriate career tracks, as described in Box 3.1 below.

Box 3.1 Summary of relevant recommendations from the Haythornthwaite Review

- **Recommendation 50:** 'Heads of professions should immediately identify where skills-based career pathways should be established in their areas of responsibility.'
- **Recommendation 51**: 'Design career paths that holistically incentivise skills acquisition, reskilling and upskilling by using all elements of a total reward approach…Each career pathway must clearly define what separate skills and rank-based progression looks like.'
- **Recommendation 52**: 'Reorganise career management around skills groups rather than rank groups for these professions…This will also have to operate alongside rank-based career management elsewhere in the organisation.'

Source: UK Ministry of Defence (2023).

Despite this recognition, effort and resource will need to be dedicated to ensuring that such pathways are available in the appropriate areas.[136] Additionally, as new technology areas and requirements continue to

[129] See Ellis et al. (2024) for more discussion of this topic.
[130] DCDC Shrivenham Workshop, December 2024; UK Ministry of Defence (2023); Galai et al. (2020); Muravska et al. (2021).
[131] DCDC Shrivenham Workshop, December 2024; UK Ministry of Defence (2023); Matthews et al. (2021); Hardison et al. (2021); Lucas et al. (2024).
[132] UK Ministry of Defence (2023); Matthews et al. (2021); Hardison et al. (2021). RAND Europe was heavily involved in the Haythornthwaite Review.
[133] Hardison et al. (2021).
[134] Matthews et al. (2021).
[135] See Lucas et al. (2024) for more information about the importance of both technical and soft skills.
[136] DCDC Shrivenham Workshop, December 2024.

emerge, Defence will need to ensure that it has a means for identifying and introducing new pathways as needed.[137]

3.2. Overhauling approaches to education and training on C2 to support continuous learning and adaptation

Both CP2 and CP3 talk at length about the importance of education and training. Specifically, CP2 talks about the types of soft and technical skills that personnel are likely to need to enable C2 systems in the future; while some of this can be recruited externally, training and education will be needed across the Defence enterprise.[138] Even for those individuals recruited for their preexisting skills, continuing education will be a key enabler for maintaining, refreshing and updating the necessary knowledge, expertise and skills.

Education and training settings are also where it may be most appropriate to encourage personnel to challenge existing concepts, approaches, behaviours and ways of working, providing a safe space to think creatively without threatening existing authority. Training venues may also provide key opportunities for experimenting with new technologies.[139] It could also enable personnel to become more comfortable with different approaches to sensemaking and decision making, including those that may be necessary in denied and degraded environments.[140] Training events and exercises can similarly provide opportunities to learn how to work with partners in different configurations, reinforcing relationships and helping identify and subsequently mitigate any practical barriers and cultural frictions when working across organisational seams.[141]

Learning lessons from allies and partners as they also work to improve their crisis and conflict management capabilities will also be an important enabler for the UK's defence C2 capability in the future. CP2 and CP3 both incorporated examples from different countries as they sought to improve their C2 capabilities (e.g. the US's JADC2 vision) or related educational approaches (e.g. New Zealand's new approach to officer training).[142] Given that the FOE will impact all countries and other actors seeking to operate within it, albeit in different ways depending on factors such as geography or national strategic priorities, having processes for identifying and incorporating relevant lessons from others will be a key enabler for the UK's C2 capability. While there is a potential 'first mover advantage' to the UK from leading the way in developing and implementing novel approaches to C2, there are also substantial potential benefits from learning from others' successes and mistakes ('second mover advantage'). As such, the UK should consider how much it wants to lead or diverge from allies' legacy approaches in this respect, versus plugging into the US's JADC2 vision or seeking to influence the (likely slower, given the many stakeholders involved) evolution of NATO's thinking on C2.

[137] See Lucas et al. (2024) and Ellis et al. (2024) for further discussion of how professionalising C2 can best be achieved across the Defence enterprise.
[138] Lucas et al. (2024).
[139] Ellis et al. (2024).
[140] Lucas et al. (2024).
[141] Ellis et al. (2024).
[142] Lucas et al. (2024); Ellis et al. (2024).

3.3. Promoting new ways of working across the C2 enterprise that both helps integrate new technologies and gets the most from personnel

Previous CPs explored the importance of organisational change and new ways of working in order to support effective C2 systems and fully leverage the advantages of new technologies.[143] Additionally, new ways of working are going to be critical as Defence expands the individuals involved in the C2 enterprise, as discussed in CP2.[144] This will necessarily involve partners over whom Defence does not have command or control; therefore collaboration and cooperation will be required, going beyond traditional military conceptions of hierarchical 'command' and 'control' to embrace alternative models of networked and non-hierarchical 'collaboration', to get the most from diverse teams or teams from different organisations.[145] As discussed in CP2, this will require personnel to have much improved interpersonal skills; however, Defence as a whole will also need to identify and implement ways of working that support this more fluid approach while simultaneously retaining clear and decisive C2 in settings where a formalised hierarchy and allocation of responsibilities is still required (e.g. nuclear C2).

3.4. Bolstering resilience at all levels of the enterprise to support delivery of C2 even in degraded and denied environments

The FOE is likely to include significant efforts by adversaries to deny and degrade communications, especially those that underpin C2.[146] Therefore, resilience and mission assurance should not only be vital considerations in the design of future C2 systems and networks, and the technologies that underpin them, but also a key concern for the personnel, processes, TTPs, structures and culture that form the C2 enterprise. As explored in previous CPs, personnel will need to be comfortable operating under uncertainty, complexity and duress, and in a variety of ways of operating. Established alternative modes could be critical to ensuring that activities can continue, even in the face of extremely degraded communications. As elaborated in Section 3.2, training and exercises are a key method for practising operations under such conditions and enhancing personnel expertise and comfort in doing so.

3.5. Designing different headquarters functions that are fit for a variety of purposes and contexts

As discussed in CP1, there are numerous predicted characteristics of the FOE that are going to change the way in which headquarters (HQ) will need to operate if they are to be both effective and survivable.[147] Given the changes discussed in this section, it is further likely that, rather than a single, large-footprint HQ, there will be an increasing need for more dispersed and disaggregated HQs (some physical and some virtual) serving different purposes, operating under different conditions that determine the appropriate trade-offs.[148]

---

[143] Lovelock et al. (2023).
[144] See Lucas et al. (2024) for a discussion of the expanding nature of the Defence enterprise.
[145] Lucas et al. (2024).
[146] Black et al. (2024).
[147] For a more detailed discussion of the changes to the FOE that will necessitate this change, please see Black et al. (2024).
[148] For a longer discussion of the types of trade-offs that may be involved with the design of HQ functions, see Lucas et al. (2024).

These HQs may appear in diverse shapes, sizes and configurations based on the needs of a particular context. Areas of variation could include mobility, connectivity, concealment, access to information and expertise, and the relative types of automation introduced into their processes.[149] It will be important to make such trade-offs carefully to ensure that each of these HQs is fit for its respective purpose, and that these design choices for different types of HQ are mutually reinforcing rather than being in significant tension.[150]

The increasing threat posed by adversaries' improved sensor and fires complexes, including precision fires, offensive cyber and electronic warfare, means that HQs will need to operate in a way markedly differently from that possible in the more benign environments experienced over the last 30 years. Previous studies from both RAND and other organisations predict that HQs will need to be designed in ways that maximise survivability: being smaller, more agile and better concealed, particularly through more careful signature management and clever use of camouflage, decoys, terrain and urban environments to avoid detection.[151] While such considerations apply to the wider force as a whole, they are particularly complicated for HQs to achieve, given the requirements for HQs to collect information, fuse and analyse that information, and communicate orders out to the field – a HQ that is far from the battlespace, but so heavily hardened and concealed that it is not able or willing to communicate with lower echelons is of no use to anyone.[152]

Additionally, it is important to note that in future, UK Defence is likely to be engaged in a competition for sensor dominance: the aim of which will be to build a better understanding of the battlespace than the adversary possesses.[153] UK Defence must recognise that neither side will ever have an ideal understanding, due to the attrition of sensors, as well as efforts to deny spectrum access through jamming and electronic warfare (EW) or create confusion through the use of deception and spoofing. However, improving this picture will be a key consideration as the basis for developing sufficient understanding to make timely and effective command decisions. In contrast with the signature management considerations for concealment and survivability, this will require increased connectivity and computing power, not only to access data from sensors, but also to process and analyse that information.[154] It also necessitates a clearer understanding of how to prioritise finite bandwidth and what data to move around the battlespace when, how, with what urgency and in what form, given that certain messages need to be communicated urgently if UK forces are to exploit a tactical opening or mitigate an imminent threat. However, every broadcast risks exposing both individual nodes and the entire network to adversary detection or attack. Design decisions for future HQs, then, must go hand in hand with wider thinking about what constitutes necessary and sufficient sensemaking and situational understanding, developing HQ approaches and processes to enable this, and only then devising the architecture, security, and use of the communication and information systems that will support them.

[149] Black et al. (2021); Watling (2023); Brennan (2023).
[150] Beagle et al. (2023).
[151] Black et al. (2021); Zabrodskyi et al. (2022).
[152] Zabrodskyi et al. (2022); Beagle et al. (2023).
[153] Zabrodskyi et al. (2022).
[154] While it does not eliminate the overall problem, edge computing is a technology that offers significant promise in this area. See Sections 2.1.4 and 2.2.4 for more information.

3.5.1. Creating bespoke solutions for different types of headquarters

This need for both connectivity and concealment, as well as a host of other requirements affecting HQs' relationships with time, space, risk and uncertainty, will inevitably require hard choices.[155] Based on the function(s) that different types of HQ are asked to perform, the weighting given to different considerations will vary between HQs, including at different levels or when deployed on different types of operation in more or less contested environments. Additionally, different types of SQEP and technology will be needed for HQs to perform their different roles; decisions will need to be made with regard to what these should be, and how they should interact.[156]

Box 3.2 provides an example of how these trade-offs might be managed for a notional fires command centre, given its requirements; there will be no one-size-fits-all solution. This offers only one example of the types of trade-offs that may be made for a particular type of HQ. As different capabilities are dispersed and disaggregated across multiple HQs, Defence will need to be mindful of the need for HQs that address various support functions (including increasingly automated logistics to deal with the challenges of sustaining increasingly dispersed forces and in a more contested threat environment for logistics assets), as well as higher-level, strategic HQs.[157] This latter type of HQ is explored in the following section, given its unique importance for C2 in the FOE.

[155] Beagle et al. (2023). See Lucas et al. (2024) for a longer discussion of some of the types of trade-offs that will be required for C2 systems more broadly, many of which also apply specifically to the question of HQ design.
[156] See Ellis et al. (2024) and Lucas et al. (2024) for more detailed discussions about the importance of ensuring that selected technologies are fit for purpose.
[157] See Brennan (2023) for an example of how Australia's Royal Australian Air Force (RAAF) and Army are addressing this challenge.

Box 3.2 Fires Command Centre

Fires command centres are tasked with both proactively targeting Blue fires and reacting to Red fires (i.e. counter-battery fires), responding at pace to a Red force that is likely to be increasingly mobile, agile and automated. In short, Blue will be required to shoot Red before Red can shoot back and/or move to a new concealed position or out of range. This places a premium on a high speed of decision making; however, while these decisions will frequently be complicated, they will be significantly less complex than more strategic-level campaign planning.[158] This will therefore require trade-offs that might not necessarily apply to other types of HQs, to prioritise speed of decision making and access to real-time understanding of both Blue and Red movements:

- The need for high-speed decision making likely means higher levels of automated data analysis and decision making, potentially even including humans on rather than in the loop.
- The need for near-instantaneous decision making in response to certain stimuli (e.g. Red fires from a particular location) will likely need to be prioritised over a steady tempo and rhythm of decision making.
- Equally, quick decision making with imperfect information is likely to be of more use in some scenarios (e.g. counter-battery fire missions) than slower decision making that might account for more information.
- Given the need for high-speed, often reactive decision making, information will need to be fed to this HQ in as close to real-time as possible; this will likely require prioritising communications from sensors and higher-level HQs despite the potential for this to detrimentally affect concealment.
- The lower level of concealment entails that such a command centre will need to be physically extremely agile, to enable them to fire quickly and rapidly move out of range after being detected. Physical and electronic decoys may also be required both to conceal the HQ and more broadly to help complicate adversary efforts to understand pattern-of-life behaviours and what nodes do what within a network.

In addition to implications for the physical and electronic construction of this centre, such considerations will also affect which types of SQEP are required, as well as the level of engagement with non-Defence partners (which is likely more limited for this more narrowly focused HQ than for HQs at higher operational and strategic levels).

Source: RAND Europe research based on Black, Lucas et al. (2021); Watling (2023); Brennan (2023); Zabrodskyi et al. (2022); Beagle et al. (2023).

3.5.2. Improving functionality for higher-level, strategic headquarters

Strategic headquarters play a key role in C2 in the FOE, with both requirements and threats driving an HQ potentially designed very differently from that discussed in Box 3.2. Such a headquarters will need to be able to think and plan for multiple simultaneous complex environments, building on the themes of CP1. This means not only collecting a much broader range of information and employing different techniques to try to understand as much as is possible for complex adaptive systems, but also taking the time to raise, consider and model second- and third-order effects of different courses of action.[159] This will necessarily slow the pace of decision making if it is to be done in a way that allows sufficient time for proper exploration, testing and iteration. Equally, decisions are less likely to need the same kind of real-time action-reaction feedback loop that might occur at a lower-echelon HQ. It will likely also need to accommodate a more diverse set of personnel, bringing together expertise from all domains and services across Defence. Depending on the mandate of the HQ, allies and partners, PAGs and even private-sector partners or academic subject matter experts may also play key roles in a more diverse workforce. Given the importance of the individuals in this HQ, concealment and signature management are likely to be a much higher priority. Ideally, such a HQ would be out of range of Red's kinetic effectors altogether.[160]

[158] See Black et al. (2024) for a more detailed discussion about the difference between 'complicated' and 'complex' decision making.
[159] Watling (2023).
[160] Beagle et al. (2023); Zabrodskyi et al. (2023).

3.5.3. Ensuring the design choices and trade-offs for headquarters at different echelons reinforce rather than frustrate efforts to ensure interoperability

To ensure that the whole C2 enterprise functions effectively, it will not be sufficient to design each HQ to optimise for its own individual tasks in isolation. Instead, HQs at different levels and in different roles must be mutually reinforcing and supportive of one another, as well as the wider Defence C2 enterprise.[161] As one example, the need for concealment at more tactical commands may require extremely intermittent communications. Higher echelon commands, such as that described, will therefore need to anticipate that and become more comfortable with delegating authority and articulating commanders' intent downwards, while clarifying the timing, nature and scale of updates from tactical headquarters, which will sometimes have to be constrained to the bare minimum necessary. Moving between different modes or states of C2 as the communications landscape changes and reachback becomes more or less feasible, for example due to Red jamming and EW capabilities, will also need to be something that HQs can do in a concerted fashion.

3.6. Conclusion

This section looked at the enablers for C2 systems in the future that are likely to be needed across the Defence enterprise. Perhaps the most important of these are the types of personnel and skills that are likely to be needed, as well as how the organisation incentivises its staff to behave, including being willing to commit to the organisation and develop professionally over the longer term. Previous CPs dealt with some of these issues in more detail; however, this section aimed to provide an overview from the perspective of enabling more effective development and sustainment C2 capability in the future.[162]

[161] See Lucas et al. (2024) for additional discussions of the Defence enterprise, as well as Ellis et al. (2024) for the importance of considering C2 as a capability across the entirety of Defence.

[162] See Black et al. (2024), Lucas et al. (2024) and Ellis et al. (2024) for further and more detailed discussion of many of the points touched upon in this chapter.

4. Deprecated enablers

This chapter discusses how the enablers of C2 capability can be adapted and changed over time to accommodate new technologies and ways of thinking and working. In particular, this chapter focuses on how Defence can recognise the need for improvement and change and move beyond existing ways and means to adapt with the necessary speed. Of note, as with Chapter 3, many of these topics have been touched on in the previous three CPs; therefore, much of this section focuses on drawing those insights together and cross-referencing to where more detail can be found.

The first section concerns how Defence can identify when legacy C2 capabilities or enablers become out of date, retiring or reappropriating them to support the transition to new systems and ways of doing things as quickly as time and resource permit. The second section looks at how Defence can ensure that it continues to adapt at the speed of relevance, which includes recognising and adopting new and novel ways of working.

4.1. Retiring out-of-date enablers for C2

This section considers how Defence can recognise, retire or repurpose certain components of current C2 capability and related enablers as they become less relevant. At the very least, Defence needs to understand and better mitigate the risks associated with any identified and remaining obsolescence. With the rapid change of the environment that continues apace, it is likely that current ways of thinking and operating will become increasingly unfit for purpose. Similarly, with the rapid technological change predicted in CP1, over time it is inevitable that technologies underpinning C2 systems and networks will become obsolete.[163] Consequently, ways of working that were designed to accommodate and leverage those technologies may need to be removed or redesigned to ensure that C2 remains efficient and effective. In summary, given the pace of technological change, and the myriad changes and evolving threats faced in the FOE, Defence C2 will need to adapt at an increasingly rapid pace.

One key method for recognising where technologies or ways of working may need to be replaced or repurposed is observing how partners and allies, both within the UK and across the international landscape, are adapting their own C2 systems. As discussed in CP3, lessons from allies and partners, as well as the private sector and PAGs, play an important role here.[164] This will enable the UK to not only improve its own C2 systems, but also ensure that they maintain interoperability with allies and partners. The pace of change in the private sector is important for tracking innovation: as discussed in CP2, horizon-scanning

[163] Black et al. (2024).
[164] Ellis et al. (2024).

methodologies can be used to identify new scientific, technological, management and organisational approaches, as well as approaches for dealing with complex and wicked problems that might offer benefit.[165] Additionally, partners and allies can offer lessons on how to repurpose old technologies: the US Strategic Capabilities Office, discussed in CP2, provides one example of how this is being done.[166]

It is important to note that the things most difficult to remove within an organisation are those that are culturally embedded. Frequently, even when an improved way of working is brought in, it is not sustained due to an organisational push towards the existing status quo. This is an issue more broadly addressed in CP3's discussion of cultural change. To make this kind of change stick, a number of enabling conditions need to be put in place, including leaders committed to the change, buy-in from individuals at all levels, and the space to fail and learn.[167]

Creating a clear understanding of what 'good' looks like, along with clear metrics and benchmarks for success, is also key in order to make objective determinations of where certain enablers are no longer as effective.[168] They are also important in understanding how repurposed legacy technologies or restructured C2 systems offer advantages compared to those that preceded them, and where they still have room for improvement or can be reconfigured for alternative use (e.g. shifting from being the primary system to becoming a reversionary mode, or being used in a more disposable manner).[169] Finally, such metrics help to direct investment in new systems and measure progress and success as they transition into the joint force.

Continuing to train and exercise with existing C2 systems will be an important way for Defence to determine whether systems are still fit for purpose, and where they may be in need of improvement.[170] Additionally, exercises are an important opportunity to experiment with integrating new technologies into existing infrastructure and ways of working, and determining how efficiency and effectiveness can be improved across these and legacy systems.[171] A cultural emphasis on persistent learning and development to facilitate continuous improvement (as well as appropriate incentives for doing so) can play a key role here in encouraging personnel to think about how certain networks or systems could work better, and could evolve over time.[172] The importance of this mindset will be discussed further in the next section.

4.2. Moving beyond the status quo

Building on the theme of CP3, it is essential not only to continuously cultivate C2 as a capability, but also to cultivate Defence's ability to move through the full capability lifecycle at much greater pace (and to drive enhanced value for money, so as to ensure affordability when more rapidly procuring, deploying and disposing of all aspects of C2 systems in future).

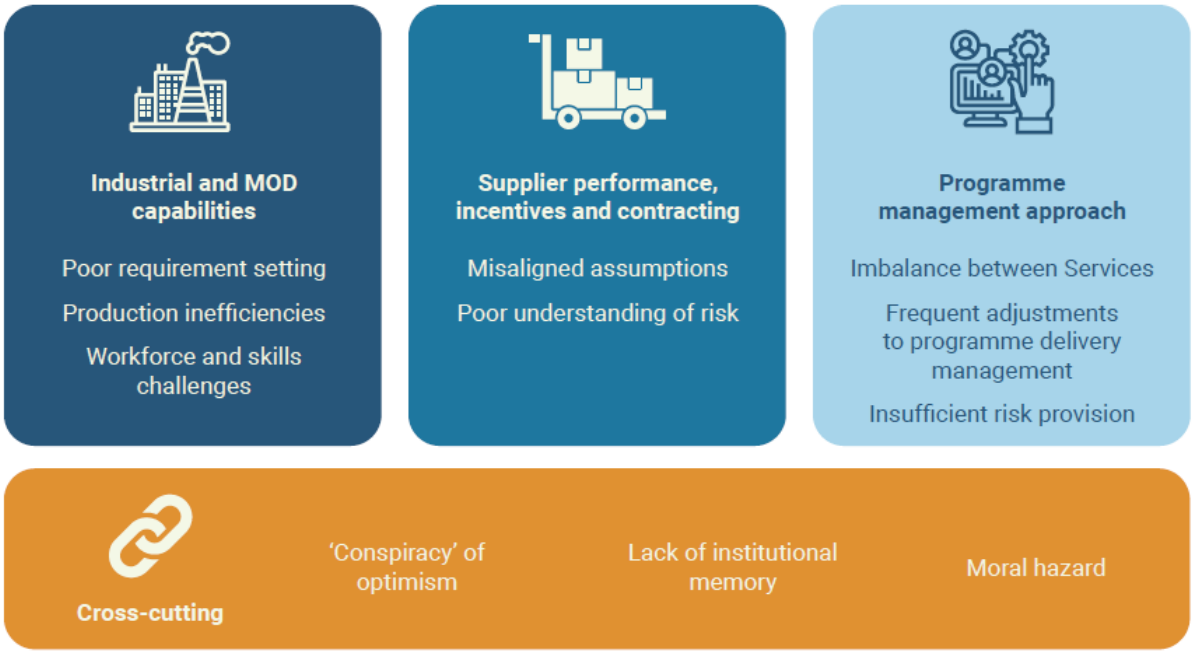
---

[165] Lucas et al. (2024). RAND Europe is currently supporting Dstl in its work to develop just such a system, including a spin-off project focused specifically on command, control, communication, computers, cyber and intelligence (C5I), of which C2 is a component.
[166] Lucas et al. (2024).
[167] Ellis et al. (2024).
[168] Ellis et al. (2024).
[169] Ellis et al. (2024).
[170] Lucas et al. (2024).
[171] Ellis et al. (2024).
[172] Ellis et al. (2024).

This necessitates a different approach to capability development, procurement, through-life support, upgrade and disposal, overcoming the bottlenecks and barriers that persist within current approaches to defence acquisition and management of the capability lifecycle.[173] It also entails a novel philosophy around the likely duration of the lifecycle for C2 systems and the underlying technologies; designing these to be continuously updated, iterated upon and disposed of, with appropriate enablement in terms of architectures, system modularity and upgradeability, rapid software patches and updates (perhaps underpinned by provision of software as a service), avoidance of vendor lock-in, management of intellectual property, etc. At a higher level, it also means getting more from domestic industrial policy and innovation initiatives in technology areas associated with C2 (see Chapter 2), as well as from multinational cooperative programmes with allies and partners, such as AUKUS or the NATO Science & Technology Organization.[174]

Prior RAND research has examined this capability development and acquisition challenge at length, observing that substantial structural and cultural barriers to reform of the MOD's approach must be overcome if the UK is to fully embrace innovation and rapid capability delivery.[175] Examples of recurring issues that cause delays, cost overruns and other problems with Defence procurement (including for traditional military hardware but especially for software and digital technologies) are shown in Figure 4.1.

Figure 4.1 Persistent challenges in acquisition to be overcome to deliver C2 capability at pace



Source: Retter, Muravska et al. (2021).

[173] For more of RAND's work on Defence's acquisition challenges and how they can be mitigated, see Retter, Muravska et al. (2021).
[174] Retter, Muravska, et al. (2021).
[175] Wong et al. (2022).

Of direct relevance here, CP3 provided a useful guide on models for organisational and cultural change management, including identification of good practices and conceptual frameworks successfully employed in the private sector and other public-sector or military settings (SAFe, Burke-Litwin, etc.).[176]

The role of cultural change in encouraging and incentivising a culture of continuous improvement cannot be overstated. CP3 talked in detail about the kind of SQEP that will enable Defence to innovate, both in terms of soft skills and perspective, as well as technical capabilities.[177] Across the seminars held by DCDC for this series of papers, a culture that encourages appropriate challenge, creativity and continuous improvement was seen as a key enabler for this SQEP to develop, and to retain personnel in Defence.[178]

Similarly, CP3 offered a detailed discussion about how Defence might be able to leverage lessons learned in the private sector and other large public-sector organisations to change both the organisational structure and the less tangible norms and behaviours of Defence in order to bring about this cultural change.[179] CP3 also discussed some of the ways in which Defence might create the necessary spaces for risk-taking and experimentation, such as sandboxes and exercises.[180] Benchmarks and metrics, the importance of which is also emphasised in CP3, again play a key role here in terms of being able to objectively demonstrate the advantages of new approaches.

[176] A more detailed discussion of these frameworks and their applicability to Defence is available in CP3. Ogden et al. (2023) in Ellis et al. (2024).
[177] Lucas et al. (2024); Ellis et al. (2024).
[178] DCDC Canberra Workshop, June 2023; DCDC Shrivenham Workshop, October 2023.
[179] Ellis et al. (2024).
[180] Ellis et al. (2024).

5. Conclusion and implications

This chapter concludes not only CP4, but also this wider series of four concept papers on the possible characteristics of C2 in the future. As such, it begins by summarising this particular paper, before moving into a set of recommendations that draw on the findings of all four papers.

5.1. Summary

This fourth and final paper in the series began by describing the context, namely the three preceding CPs under the context of Project Mimisbrunnr, and the working conception of C2. It then moved into a discussion of technological enablers of C2 systems in the future that DCDC has determined to be of interest. This section focused on particular technical areas that show great promise for C2 systems, as well as specific applications and thus capabilities that emerging technologies seem likely to be able to offer.

While technology is a key topic of conversation, these papers have emphasised the importance of avoiding techno-determinism and instead seeing C2 as a socio-technical system, with a heavy emphasis on the enduring salience of the human element and a recognition of the need for sustained change to ways of organising and to institutional culture to enable Defence to move towards novel approaches to C2 that are more suited to the punishing conditions expected in the FOE out to 2040 and beyond.

As such, Chapter 3 talked about C2 enablers resulting from the people and organisation of Defence. These include cultural change, persistent learning and development, new ways of working, and the bolstering of resilience across all levels of the C2 enterprise through both technical and non-technical means. Many of these enablers were examined at length in previous CPs; this paper therefore provides a summary and cross-referencing to direct readers to those discussions.

Given the dynamism of the FOE, Defence will also likely require C2 systems to be more adaptable in future. To this end, Chapter 4 discussed how Defence can move away from capabilities that are no longer effective and improve its ways of working: understanding when existing technical systems are becoming obsolete, and ensuring that Defence has the capacity to develop, acquire, field and upgrade new capabilities at pace, while phasing out and disposing of legacy technical systems in a responsible manner. Achieving such adaptability would not only enable the C2 enterprise to continue to learn and adapt over time while staying resilient to the rapid pace of change that experts believe will characterise the FOE, but would also benefit Defence more widely (e.g. supporting the rapid development and fielding of novel capabilities for fires, logistics or other functions), given that many of the underpinning procedural or cultural enablers would not be unique to C2.

The last section of this final paper presents recommendations from all four CPs.

5.2. Implications

Based on the findings of the previous three CPs, as well as the topics explored here, the GSP team has generated a range of key implications for DCDC and the MOD to consider.

These implications are not presented in order of importance: rather, many of these changes are mutually dependent or reinforcing. For example, recruiting the necessary SQEP will be insufficient if the culture of Defence does not support their retention within the organisation. Similarly, these findings are not meant to present a prescriptive and definitive answer on which specific technical solutions, architectures or force structures should be adopted. Such decisions fall outside of the scope of this study, or indeed of concept development, and are contingent on a much wider set of factors, including changes made to other aspects of the joint force (e.g. fires, logistics) and the availability of resource (e.g. financing, personnel, time).

Parallel ongoing work by DCDC to develop the UK's Capstone Concepts, supported by various studies through the SASC, should serve to help clarify the wider vision of how Defence will operate and thus configure itself out to 2040 and beyond. DCDC's continuing work on defining a new Joint Concept Note for C2 in the future must plug into and build upon this overarching vision – much as UK Defence's thinking should also seek to influence, and in turn be influenced by, the evolving approach to multi-domain operations and C2 at the NATO level.

These considerations notwithstanding, this series of four concept papers has emphasised the following:

- **To cope with the challenges of the FOE, the Defence C2 enterprise of the future will not be a single entity, but rather a more fluid assemblage of varying combinations of individuals and organisations.** To this end, it will be necessary that Defence remains flexible and adaptable in its thinking in order to facilitate and enable a variety of different types of relationships and arrangements, based on changing conditions, new technological possibilities, and the need to adopt different structures, processes and ways of working depending on operational requirements and the partners involved.
- **Collaboration with diverse partners is going to be a key enabler of C2 systems in the future.** Defence will often need to work with partners that it can neither command nor control. Instead, Defence will need to be more comfortable and capable when it comes to building non-hierarchical relationships to enable partnership, cooperation and coordination with a more diverse set of actors, including PAGs, international allies and partners, industry, NGOs and broader society.
- **The Defence C2 enterprise will therefore need to consist of multiple, parallel C2 systems and must be able to adapt effectively, possibly moving flexibly between C2 approaches to handle diverse challenges and circumstances.** This will need to include the ability to add and integrate new partners quickly, while selectively sharing information to protect confidentiality. It will also need to include alternative modes to enable resilience in denied and degraded environments, such as reversionary modes or more hardened methods of communication. It is likely that multiple C2 modes will exist in parallel: for example with C2 in more benign settings (e.g. non-combat operations or other more permissive environments) configured rather differently from C2 in

degraded and denied environments, (e.g. where the proliferation of kinetic and non-kinetic threats and the imperative need for UK forces to operate concealed, dispersed and on the move to survive will necessarily restrict reach back to better staffed and equipped headquarters at higher echelons). Crucially, C2 in these different modes and configurations will require different soft and technical skills from Defence personnel, as well as bespoke processes and technical enablers. The cultivation of such a range of competences within its organisations and personnel presents a significant challenge for Defence, and being able to move beyond predefined C2 modes/states depending on need will help the UK achieve the diverse set of ways and means it needs if it is to grapple with the complex problems it expects to face in the FOE.

- **To make this more flexible and adaptable C2 enterprise work in practice, Defence will need to undergo profound change both to ways of organising and to more intangible aspects of culture**. This is unlikely to be a one-time shift, but rather will require a long-term effort to transition to a culture of continuous learning and development in order to adapt at a more rapid pace to changing circumstances. At a minimum, Defence culture will need to support increased tolerance for risk, experimentation and challenge (where appropriate), as well as increased comfort with complexity and uncertainty, among its personnel. Equally, Defence must understand in which areas more traditional, hierarchical culture and formalised ways of working will remain appropriate (e.g. nuclear C2) and find a way for new and old to coexist.
- **The necessary organisational changes will not be possible without a united effort from Defence, including clear endorsement and investment from leadership.** In order to bring the whole Defence enterprise along in this change, leadership is going to need to clearly communicate desired changes across Defence, and be open to feedback and challenge from all levels of the organisation.
- **Training, education and rigorous exercises will be key enablers for a range of capabilities,** including fostering cooperation and collaboration both across Defence and with PAGs and international allies and partners; practising operating under uncertainty; testing and integrating new technologies and ways of working; and challenging existing ways of working. Moving towards a novel approach to C2 is about experimentation, iteration and continuous improvement, from the macro-level of the Defence enterprise right down to individual personnel at all levels of seniority.
- **To guide this process of learning and iteration, and support resource prioritisation, Defence is going to need metrics and a shared understanding of what 'good' looks like** in different contexts in order to make the difficult decisions and trade-offs that will be inherent in developing new C2 systems. Additionally, these metrics will be needed to adjust and adapt to changing circumstances, making C2 systems – and the enterprise that cultivates and fields them – resilient to the pace of FOE and technological change.
- **Defence will need to put in greater effort to attract and recruit a variety of skills crucial to C2 systems in the future**, including a range of more advanced skills and knowledge; comfort with decision making under uncertainty; 'soft' interpersonal, management or communication skills; and a willingness and ability to challenge existing models or decisions appropriately and constructively.

- **Given intense competition for such skills from across Defence, PAGs and the private sector, Defence must also consider how best to motivate, develop and retain this talent.** This may involve consideration of how to get the most from a Whole Force approach– and from use of human–machine teaming, AI and automation to bolster workforce productivity and offset a potential lack of resource (e.g. manpower). It also may require changes to incentivisation or career progression to foster the appropriate skills and abilities among the Defence workforce.
- **Defence will need to understand C2 as a socio-capability that needs to be continuously cultivated in a holistic and proactive manner in order to join up efforts from across Defence and achieve shared goals.** The efforts that will need to be coordinated are extremely diverse, but certainly include training and exercises, professional military education, reforms to the organisation's structure and culture, scientific and technological knowledge, changes to force and concept development, acquisition and procurement, use of industrial policy levers, and relationship and partnership building. This requires a Senior Responsible Owner, empowered with appropriate authority and resources, as well as incentives to drive accountability and coherence for those tasked with delivering associated activities at lower levels.
- **Defence cannot simply 'purchase' new C2 systems off-the-shelf and should be wary of promises of any technological 'silver bullet', but rather will need to invest in and iterate new capabilities and systems over time while responsibly managing the transition away from legacy capabilities.** 'Investment' here refers both to financial resource and support for research and development, but also investment in relationships with industry to increase their understanding of Defence's requirements; investment in end-user testing and iteration; training for personnel to ensure that they can use systems effectively; and planning for how new technologies or approaches can be integrated with existing systems, or how systems that are no longer appropriate will need to be phased out gradually. Equally, if Defence can get this right when it comes to C2, this could yield not only significant strategic and operational advantage, but also wider benefits such as enhanced productivity and thus value for money from the joint force, with improved C2 enabling Defence to get more out of its finite assets, employing them to maximum effect and at reduced risk of destruction or failure, on account of the UK's enhanced situational understanding and decision advantage over adversaries.
- **Achieving these objectives will require collaboration and cooperation across the whole of the Defence enterprise, including industry and academia.** As discussed in CP2, the Defence enterprise cannot only include government departments. Particularly given the importance of an iterative approach to technology, Defence will need to work closely with industry and academia to help them to understand Defence's requirements and see that these needs are met. Additionally, Defence will need to work with external subject matter experts to ensure that it is adopting the most effective and appropriate approaches to C2.

The authors hope that identifying these implications will contribute to Defence's thinking more broadly, as well as DCDC's specific thinking regarding revisions to the current JCN 2/17 on C2.

References

Aruchami, Jagatheesh. 2023. 'What Is a Wetware Computer?' Turbo Future, 9 January. As of 5 June 2024: https://turbofuture.com/computers/what-is-organic-computer

Association for Project Management. 2024a. 'Knowledge and why it matters?' As of 5 June 2024: https://www.apm.org.uk/resources/find-a-resource/knowledge-management/what-is-knowledge-anyway-and-why-does-it-matter/

——. 2024b. 'What is information management?' As of 5 June 2024: https://www.apm.org.uk/resources/what-is-project-management/what-is-information-management/

Atherton, Kelsey. 2021. 'Loitering munitions preview the autonomous future of warfare.' Brookings, 4 August. As of 5 June 2024:

https://www.brookings.edu/articles/loitering-munitions-preview-the-autonomous-future-of-warfare/

Aversa, Paolo, Laure Cabantous, & Stefan Haefliger. 2018. 'When decision support systems fail: Insights for strategic information systems from Formula 1.' *The Journal of Strategic Information Systems* 27(3): 221–36. As of 5 June 2024:

https://www.sciencedirect.com/science/article/abs/pii/S096386871630138X

BAE Systems. 2023. 'The future of military training: Synthetic environments and the military metaverse.' As of 5 June 2024:

https://www.baesystems.com/en-us/feature/the-future-of-military-training-synthetic-environments-and-the-military-metaverse

Balis, Christina, & Paul O'Neill. 2022. 'Trust in AI: Rethinking Future Command.' *Royal United Services Institute Occasional Paper*, 23 June. As of 5 June 2024:

https://www.rusi.org/explore-our-research/publications/occasional-papers/trust-ai-rethinking-future-command

Ballani, Hitech. 2023. 'Unlocking the future of computing: The Analog Iterative Machine's lightning-fast approach to optimization.' Microsoft Research Blog, 27 June. As of 5 June 2024: https://www.microsoft.com/en-us/research/blog/unlocking-the-future-of-computing-the-analog-iterative-machines-lightning-fast-approach-to-optimization/

Beagle, Lt Gen. Milford, Brig. Gen. Jason C. Slider, & Lt Col. Matthew R. Arrol. 2023. 'The Graveyard of Command Posts: What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations.' *Army University Press Military Review*, May–June. As of 5 June 2024:

https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2023/Graveyard-of-Command-Posts/

Behme, Faris, & Sandy Becker. 2021. 'The new knowledge management.' Deloitte, 29 January. As of 5 June 2024:

https://www2.deloitte.com/us/en/insights/focus/technology-and-the-future-of-work/organizational-knowledge-management.html

Bellasio, Jacob, Linda Slapakova, Luke Huxtable, James Black, Theodora Ogden, & Livia Dewaele. 2021. 'Innovative technologies shaping the 2040 battlefield.' European Parliamentary Research Service. As of 5 June 2024: https://data.europa.eu/doi/10.2861/620590

Berloff, Natalia, Matteo Silva, Kirill Kalinin, Alexis Askitopoulos, Julian D. Toepfer, Pasquale Cilibrizzi, Wolfgang Langbein, & Pavlos G. Lagoudakis. 2017. 'Realizing the classical *XY* Hamiltonian in polariton simulators.' *Nature Materials* 16: 1120–26. As of 5 June 2024: https://doi.org/10.1038/nmat4971

Black, James, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paillé, & Fiona Quimbre. 2022. *Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea*. Santa Monica, Calif.: RAND Corporation. RR-A528-1. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA528-1.html

Black, James, Rebecca Lucas, John Kennedy, Megan Hughes, & Harper Fine. 2024. *Command and Control in the Future: Concept Paper 1: Grappling with Complexity*. Santa Monica, Calif.: RAND Corporation. RR-A2476-1. As of 5 June 2024:

https://www.rand.org/pubs/research_reports/RRA2476-1.html

Black, James, Rebecca Lucas, Sam Stockwell, & Paula Fusaro. 2021. *Warfighting at Reach: Conceptual Approaches to Power Projection and the Delivery of Military Effects from Standoff*. Santa Monica, Calif.: RAND Corporation. PR-A1112-1. Unpublished RAND Corporation research.

Brand, Aron. 2023. 'Data dominance: the weapon of the future.' Military Embedded Systems, 3 August. As of 5 June 2024:

https://militaryembedded.com/ai/big-data/data-dominance-the-weapon-of-the-future

Brennan, Major Roger. 2023. 'First for brigade air and land integration.' Australian Government: Defence, 11 August. As of 5 June 2024:

https://www.defence.gov.au/news-events/news/2023-08-11/first-brigade-air-and-land-integration

Cao, Bing, Junliang Guo, Pengfei Zhu, & Qinghua Hu. 2023. 'Bi-directional Adapter for Multi-modal Tracking.' As of 5 June 2024: https://arxiv.org/abs/2312.10611

Capano, Giliberto, & Jun Jie Woo. 2018. 'Designing policy robustness: outputs and processes.' *Policy and Society* 37(4): 422–40. As of 5 June 2024: https://doi.org/10.1080/14494035.2018.1504494

Castelvecchi, Davide. 2023. '"Mind-blowing" IBM chip speeds up AI.' *Nature* 623(17). As of 5 June 2024: https://doi.org/10.1038/d41586-023-03267-0

Central Digital and Data Office, Cabinet Office, & Office for Artificial Intelligence. 2021. 'Ethics, Transparency and Accountability Framework for Automated Decision-Making.' 13 May. As of 5 June 2024:

https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making

Cirac, J. Ignacio, & Peter Zoller. 2012. 'Goals and opportunities in quantum simulation.' *Nature Physics* 8: 264–66. As of 5 June 2024: https://doi.org/10.1038/nphys2275

Cook, Cynthia, Rose Butchart, Gregory Saunders, & Alexander Holderness. 2022. 'Pathways to Implementing Comprehensive and Collaborative JADC2.' Center for Strategic and International Studies. As of 5 June 2024:

https://www.csis.org/analysis/pathways-implementing-comprehensive-and-collaborative-jadc2

Cortical Labs. 2023. 'Home Page.' As of 5 June 2024: https://corticallabs.com/

Cutress, Ian. 2021. 'Intel Rolls Out New Loihi 2 Neuromorphic Chip.' AnandTech, 30 September. As of 5 June 2024: https://www.anandtech.com/show/16960/intel-loihi-2-intel-4nm-4

D-Wave. 2023. 'How D-Wave Systems Work.' As of 5 June 2024: https://www.dwavesys.com/learn/quantum-computing/

Defense Advanced Research Projects Agency (DARPA). 2023a. 'Developing Agile, Reliable Sensing Systems with Microbes.' As of 5 June 2024: https://www.darpa.mil/news-events/2023-04-21

——. 2023b. 'New Sensors with the HOTS for Extreme Missions.' As of 5 June 2024: https://www.darpa.mil/news-events/2023-05-12

Dekker, A. H. 2017. 'C2 and the Kuramoto Model: An Epistemological Retrospective.' 22nd International Congress on Modelling and Simulation, 3–8 December. As of 5 June 2024: https://mssanz.org.au/modsim2017/D3/dekker.pdf

Edwards, Jane. 2023. 'Leidos' Chad Haferbier: Open Architecture Could Help Agencies Advance Multidomain Operations, Improve Mission Outcomes.' GovConWire, 9 May. As of 5 June 2024:

https://www.govconwire.com/2023/05/leidos-chad-haferbier-open-architecture-could-help-advance-multidomain-ops/

Eliyahu, Sagi. 2020. 'Machine Learning Powers Knowledge Management.' *Forbes*, 28 July. As of 5 June 2024:

https://www.forbes.com/sites/forbestechcouncil/2020/07/28/machine-learning-powers-knowledge-management/

Ellis, Conlan, Rebecca Lucas, Stella Harrison, James Black, Ben Fawkes, Martin Robson, Alan Brown, & Edward Keedwell. 2024. *Command and Control in the Future: Concept Paper 3: Conceptualising Command and Control as a Capability.* Santa Monica, Calif.: RAND Corporation. RR-A2476-3. As of 24 July 2024: https://www.rand.org/pubs/research_reports/RRA2476-3.html

EY. 2022. 'BT and Toshiba launch first commercial trial of quantum secured communication services – EY becomes first commercial customer.' 27 April. As of 5 June 2024: https://www.ey.com/en_uk/news/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services

Galai, Katerina, Lucia Retter, Julia Muravska, Marta Kepe, Alice Lynch, Anna Knack, Jacopo Bellasio, Antonia Ward, Arya Sofia Meranto, Davide Maistro, Liga Baltina, & Terence Hogarth. 2020. *Understanding skills gaps in the European defence sector.* Santa Monica, Calif.: RAND Corporation. RB-10094-EC. As of 6 June 2024: https://www.rand.org/pubs/research_briefs/RB10094.html

Gaur, Vishal, & Abhinav Gaiha. 2020. 'Building a Transparent Supply Chain.' *Harvard Business Review*, May–June. As of 5 June 2024: https://hbr.org/2020/05/building-a-transparent-supply-chain

Gregor, Shirley & Benbasat, Izak. 1999. 'Explanations from Intelligent Systems: Theoretical Foundations and Implications for Practice.' *MIS Quarterly* 23(4): 497-530. As of 10 June 2024: https://www.jstor.org/stable/249487

Grisogono, Anne-Marie. 2020. 'How Could Future AI Help Tackle Global Complex Problems?' *Frontiers in Robotics and AI* 7. As of 5 June 2024:

https://www.frontiersin.org/articles/10.3389/frobt.2020.00050/full

Hardison, Chaitra M., Leslie Adrienne Payne, Julia Whitaker, Anthony Lawrence, & Ivica Pavisic. 2021. *Building the Best Offensive and Defensive Cyber Workforce: Volume II, Attracting and Retaining Enlisted and Civilian Personnel.* Santa Monica, Calif.: RAND Corporation. RR-A1056-2. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA1056-2.html

Harrison, S. L. H. Sigurdsson, S. Alyatkin, J. D. Topfer & P. G. Lagoudakis. 2022. 'Solving the Max-3-Cut Problem with Coherent Networks.' *Physical Review Applied* 17: 024063. As of 5 June 2024: https://doi.org/10.1103/PhysRevApplied.17.024063

Heath, Alex. 2023. 'This is Meta's AR / VR hardware roadmap through 2027.' *The Verge*, 28 February. As of 5 June 2024:

https://www.theverge.com/2023/2/28/23619730/meta-vr-oculus-ar-glasses-smartwatch-plans

Hernandez, Daniela. 2022. 'High-Tech Smell Sensors Aim to Sniff Out Disease, Explosives – and Even Moods.' *The Wall Street Journal*, 16 July. As of 5 June 2024:

https://www.wsj.com/articles/high-tech-smell-sensors-scientists-develop-11657914274

Hewlett Packard Enterprise. 2023. 'What is Data Deluge?' As of 5 June 2024: https://www.hpe.com/us/en/what-is/data-deluge.html

Hitchens, Theresa. 2020. 'JADC2 Needs Pentagon To Overhaul Data Management Policies.' *Breaking Defense*, 19 October. As of 5 June 2024:

https://breakingdefense.com/2020/10/jadc2-needs-pentagon-to-overhaul-data-management-policies/

HM Government. 2022. 'National AI Strategy.' Gov.uk. As of 5 June 2024: https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf

———. 2023. 'The Bletchley Declaration by Countries Attending the AI Safety Summit, 1–2 November 2023.' Gov.uk, 1 November. As of 5 June 2024:

https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Honjo, Toshimori, Tomohiro Sonobe, Kensuke Inaba, Takahiro Inagaki, Takuya Ikuta, Yasuhiro Yamada, Takushi Kazama, Koji Enbutsu, Takeshi Umeki, Ryoichi Kasahara, Kenichi Kawarabayashi, & Hiroki Takesue. 2021. '100,000-spin coherent Ising machine.' *Science Advances* 7(40). As of 5 June 2024: https://doi.org/10.1126/sciadv.abh0952

Hoos, Holger H., & Thomas Stützle. 2005. 'Introduction.' In *The Morgan Kaufmann Series in Artificial Intelligence,* edited by Morgan Kaufmann, 13–59. As of 5 June 2024: https://www.sciencedirect.com/science/article/pii/B9781558608726500184

House of Lords. 2023. 'Proceed with Caution: Artificial Intelligence in Weapon Systems.' House of Lords AI in Weapon Systems Committee Report of Session 2023–2024. As of 5 June 2024: https://committees.parliament.uk/publications/42387/documents/210740/default/

Hughes, Megan, James Black, & Lucia Retter. 2023. *FE5: Global Complexity and Future C2.* Santa Monica, Calif.: RAND Corporation. PR-A2521-01. Unpublished RAND Corporation research.

Hughes, Zach. 2020. 'Fog, Friction, and Thinking Machines.' *War on the Rocks*, 11 March. As of 5 June 2024: https://warontherocks.com/2020/03/fog-friction-and-thinking-machines/

IBM. 2023a. 'What are AI hallucinations?' As of 5 June 2024:

https://www.ibm.com/topics/ai-hallucinations

———. 2023b. 'What is edge computing?' As of 5 June 2024: https://www.ibm.com/topics/edge-computing

———. 2023c. 'What is knowledge management?' As of 5 June 2024: https://www.ibm.com/topics/knowledge-management

IBM Research. 2023. 'Neuromorphic Devices & Systems.' As of 5 June 2024: https://www.zurich.ibm.com/st/neuromorphic/architecture.html

Intel. 2023. 'Loihi 2: A New Generation of Neuromorphic Computing.' As of 5 June 2024: https://www.intel.com/content/www/us/en/research/neuromorphic-computing.html

Johnson, Tomi H., Stephen R. Clark, & Dieter Jaksch. 2014. 'What is a quantum simulator?' *EPJ Quantum Technology* 1(10). As of 5 June 2024: https://doi.org/10.1140/epjqt10

Kalinin, Kiril, George Mourgias-Alexandris, Hitesh Ballani, Natalia G. Berloff, James H. Clegg, Daniel Cletheroe, Christos Gkantsidis, Istvan Haller, Vassily Lyutsarev, Francesca Parmigiani, Lucinda Pickup, & Antony Rowstron. 2023. 'Analog Iterative Machine (AIM): using light to solve quadratic optimization problems with mixed variables.' Microsoft Research. As of 5 June 2024: https://doi.org/10.48550/arXiv.2304.12594

Kalloniatis, Alexander, Timothy A. McLennan-Smith, & Dale O. Roberts. 2020. 'Modelling distributed decision-making in Command and Control using stochastic network synchronisation.' *European Journal of Operational Research* 284: 588–603. As of 5 June 2024: https://doi.org/10.1016/j.ejor.2019.12.033

Karako, Tom, & Masao Dahlgren. 2022. 'Complex Air Defense: Countering the Hypersonic Missile Threat.' Center for Strategic and International Studies, 7 February. As of 5 June 2024: https://www.csis.org/analysis/complex-air-defense-countering-hypersonic-missile-threat

Koniku. 2023. 'Home Page.' As of 5 June 2024: https://koniku.com/

Krause, Juljan. 2021. 'Trusted autonomous systems in defence: A policy landscape review.' UKRI Trusted Autonomous Systems Hub. As of 5 June 2024:

https://www.kcl.ac.uk/policy-institute/assets/trusted-autonomous-systems-in-defence.pdf

Kyber. 2023. 'CRYSTALS.' As of 5 June 2024: https://pq-crystals.org/kyber/

Leidos. 2023a. 'Bring Warfighter Capabilities To The Tactical Edge.' As of 5 June 2024: https://www.leidos.com/sites/leidos/files/2021-10/PDF-Edge-To-Cloud-Fact-Sheet-2021.pdf

———. 2023b. 'The Edge to Cloud Ecosystem.' As of 5 June 2024: https://www.leidos.com/interactives/edge-to-cloud/index.html

Le Page, Michael. 2021. 'Human Cells in a Dish learn to play pong faster than AI.' *New Scientist*, 17 December. As of 5 June 2024:

https://www.newscientist.com/article/2301500-human-brain-cells-in-a-dish-learn-to-play-pong-faster-than-an-ai/

Lloyd, Jon, & James Kearse. 2023. 'Generation After Next for Defence Simulation and Synthetic Environments.' NATO STO-MP-MSG-197-01, 23 February. As of 5 June 2024: https://www.sto.nato.int/publications/pages/results.aspx?k=STO-MP-MSG-197-01

Lovelock, Ben, Luke Huxtable, Lin Slapakova, Sam Stockwell, & Stephanie Blair. 2023. *Defence Guidance for Integrated Working*. Defence Science and Technology Laboratory. As of 5 June 2024: https://www.gov.uk/government/publications/defence-guidance-for-integrated-working

Lu, Qiuchen, Xiang Xie, Ajith K. Parlikad, & Jennifer M. Schooling. 2020. 'Digital twin-enabled anomaly detection for built asset monitoring in operation and maintenance.' *Automation in Construction* 118. As of 5 June 2024:
https://www.sciencedirect.com/science/article/pii/S0926580520303654

Lucas, Rebecca, Benedict Wilkinson, James Black, Paola Fusaro, & Sam Stockwell. 2022. *Future Command and Control*. Santa Monica, Calif.: RAND Corporation. PR-A1755-2. Unpublished RAND Corporation research.

Lucas, Rebecca, Conlan Ellis, James Black, Peter Carlyon, Paul Kendall, John Kendall, Stephen Coulson, & Louis Jeffries. 2024. *Command and Control in the Future: Concept Paper 2: The Defence C2 Enterprise*. Santa Monica, Calif.: RAND Corporation. RR-A2476-2. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA2476-2.html

Mandelbaum, Ryan. 2023. 'A useful application for 127-qubit quantum processors with error mitigation.' IBM Research Blog. As of 5 June 2024:

https://research.ibm.com/blog/utility-toward-useful-quantum

Marrow, Michael. 2023. '"Network-centric" security "killing us" on JADC2 initiatives: USAF general.' *Breaking Defense*, 11 July. As of 5 June 2024:

https://breakingdefense.com/2023/07/network-centric-security-killing-us-on-jadc2-initiatives-usaf-general/

Matthews, Miriam, John A. Ausink, Shirley M. Ross, Matthew Walsh, Albert A. Robbert, John S. Crown, David Schulker, Philip Armour, Irina A. Chindea, Emily Hoch, & Sean Robson. 2021. *Championing the Agile Air Force Officer Career: Examining the Potential Use of New Career Management Flexibilities*. Santa Monica, Calif.: RAND Corporation. RR-4439-AF. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RR4439.html

McKendrick, Joe, & Andy Thurai. 2022. 'AI Isn't Ready to Make Unsupervised Decisions.' *Harvard Business Review*, 15 September. As of 5 June 2024:

https://hbr.org/2022/09/ai-isnt-ready-to-make-unsupervised-decisions

McKinsey & Company. 2023a. 'What is generative AI?' 2 April. As of 5 June 2024: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai

———. 2023b. 'What is quantum computing?' 5 April. As of 5 June 2024: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

McMahon, Liv. 2022. 'Ministry of Defence acquires government's first quantum computer.' *BBC*, 9 June. As of 5 June 2024: https://www.bbc.co.uk/news/technology-61647134

Meignan, David, Sigrid Knust, Jean-Marc Frayret, Gilles Pesant, & Nicolas Gaud. 2015. 'A Review and Taxonomy of Interactive Optimization Methods in Operations Research.' *ACM Transactions on Interactive Intelligent Systems* 5(3). As of 5 June 2024: https://dl.acm.org/doi/10.1145/2808234

Menshikh, V., A. Samorokovskiy, & O. Avsentev. 2018. 'Models of resource allocation optimization when solving the control problems in organisational systems'. *Journal of Physics: Conference Series* 973: 012040. As of 5 June 2024: https://doi.org/10.1088/1742-6596/973/1/012040

Microsoft Research. 2023. 'AIM (Analog Iterative Machine).' As of 5 June 2024: https://www.microsoft.com/en-us/research/project/aim/

Molinari, Michael G. 2023. '5G & Edge Computing: The Future of the DoD and JADC2.' Air Land Sea Space Application Center, 1 July. As of 5 June 2024: https://www.alsa.mil/Portals/9/Documents/articles/230701_ALSSA_Article_Molinari.pdf

Moral Machine. 2023. 'Home Page'. As of 5 June 2024: https://www.moralmachine.net/

Mosca, Michele, & Marco Piani. 2022. '2021 Quantum Threat Timeline Report: Global Risk Institute.' Global Risk Institute, 24 January. As of 5 June 2024: https://globalriskinstitute.org/publication/2021-quantum-threat-timeline-report-global-risk-institute-global-risk-institute/

Muravska, Julia, Anna Knack, Rebecca Lucas, & Ben Williams. 2021. *Challenges and barriers that limit the productivity and competitiveness of UK defence supply chains.* Santa Monica, Calif.: RAND Corporation. PE-A117-1. As of June 10, 2024:

https://www.rand.org/pubs/perspectives/PEA117-1.html

Naseem, Afshan, Syed Tasweer Hussain Shah, Shoab Ahmed Khan, & Asad Waqar Malik. 2017. 'Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future direction.' *Annual Reviews in Control* 43: 169–87. As of 5 June 2024:

https://www.sciencedirect.com/science/article/abs/pii/S1367578816300979

National Cyber Security Centre. 2023. 'Migrating to post-quantum cryptography.' National Cyber Security Centre, 3 November. As of 6 June 2024:

https://www.ncsc.gov.uk/blog-post/migrating-to-post-quantum-cryptography-pqc

Newsroom. 2023. 'Signal Messenger Introduces PQXDH Quantum-Resistant Encryption.' The Hacker News, 20 September. As of 5 June 2024:

https://thehackernews.com/2023/09/signal-messenger-introduces-pqxdh.html

NIST. 2022. 'Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.' Information Technology Computer Security Resource Center, July. As of 5 June 2024: https://csrc.nist.gov/pubs/ir/8413/upd1/final

———. 2023a. 'Commons Requested on Three Draft FIPS for Post-Quantum Cryptography.' Information Technology Computer Security Resource Center, 24 August. As of 5 June 2024: https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography

———. 2023b. 'Post-Quantum Cryptography.' Information Technology Computer Security Resource Center, 16 November. As of 5 June 2024:

https://csrc.nist.gov/projects/post-quantum-cryptography

Ottley, Sue, Jaina Mistry, Kerry Tatlock, & Chris Vance. 2022. 'Human Machine Teaming and Human Centred Design.' *Ergonomics & Human Factors.* As of 5 June 2024: https://publications.ergonomics.org.uk/uploads/2_19.pdf

Parker, Edward, Daniel Gonzales, Ajay K. Kochhar, Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, Richard Silberglitt, Joan Chang, Christopher A. Eusebi, & Scott W. Harold. 2022. *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology.* Santa Monica, Calif.: RAND Corporation. RR-A869-1. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA869-1.html

Parker, Edward. 2023. *Promoting Strong International Collaboration in Quantum Technology Research and Development.* Santa Monica, Calif.: RAND Corporation. PE-A1874-1. As of 5 June 2024: https://www.rand.org/pubs/perspectives/PEA1874-1.html

Perey, Philippe, Nick Giannias, Máté Koch, Jean-Sebastien Dion, Jonathan Labonté, & Dave Sexton. 2022. 'Leveraging Digital Era Technologies for a new Synthetic Environment – a Panacea?' NATO STO-MP-MSG-197-03, 10 October. As of 5 June 2024: https://www.sto.nato.int/publications/pages/results.aspx?k=STO-MP-MSG-197-03

Pfeuffer, Nicolas, Lorenz Baum, Wolfgang Stammer, Benjamin M. Abdel-Karim, Patrick Schramowski, Andreas M. Bucher, Christian Hügel, Gernot Rohde, Kristian Kersting, & Oliver Hinz. 2023. 'Explanatory Interactive Machine Learning.' *Business & Information Systems Engineering* 65: 677 - 701. As of 5 June 2024: https://link.springer.com/article/10.1007/s12599-023-00806-x#citeas

Poland, David A. 2012. 'Making BCS3 Work in a Deployed Environment.' *Army Sustainment*, September–October. As of 5 June 2024: https://alu.army.mil/alog/PDF/SeptOct12/BCS3.pdf

Priebe, Miranda, Douglas C. Ligor, Bruce McClintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, & Bryan Rooney. 2020. *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control.* Santa Monica, Calif.: RAND Corporation. RR-A381-1. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA381-1.html

Resende, Mauricio G. C. 2003. 'Combinatorial optimization in telecommunications'. In *Optimization and Industry: New Frontiers*, edited by Panos M. Pardalos, & Victor Korotkich, 59–112. As of 5 June 2024: https://link.springer.com/chapter/10.1007/978-1-4613-0233-9_4

Retter, Lucia, Alexandra Hall, James Black, & Nathan Ryan. 2016. *The moral component of cross-domain conflict*. Santa Monica, Calif.: RAND Corporation. RR-1505-MOD. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RR1505.html

Retter, Lucia, Rebecca Lucas, Luke Huxtable, & Livia Dewale. 2021. *Human component of robotic and autonomous systems: Summary of workshop discussions*. Santa Monica, Calif.: RAND Corporation. RR-A1185-2. Unpublished RAND Corporation research.

Retter, Lucia, Julia Muravska, Ben Williams, & James Black. 2021. *Persistent Challenges in UK Defence Equipment Acquisition*. Santa Monica, Calif.: RAND Corporation. RR-A1174-1. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA1174-1.html

Robertson, Adi. 2023. 'The Meta Quest 3 is sharper, more powerful, and still trying to make mixed reality happen.' *The Verge*, 27 September. As of 5 June 2024: https://www.theverge.com/2023/9/27/23890731/meta-quest-3-headset-hands-on-mixed-reality-connect

Robinson, Eric, Daniel Egel, & George Bailey. 2023. *Machine Learning for Operational Decisionmaking in Competition and Conflict: A Demonstration Using the Conflict in Eastern Ukraine*. Santa Monica, Calif.: RAND Corporation. RR-A815-1. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA815-1.html

Rosenberg, J. 2017. 'Chapter 6 – Security in embedded systems.' In *Rugged Embedded Systems*, edited by Augusto Vega, Pradip Bose, & Alper Buyuktosunoglu, 149–205. As of 5 June 2024: https://www.sciencedirect.com/science/article/abs/pii/B9780128024591000063

Sachariason, Thomas E. 2009. 'The Battle Command Sustainment Support System: The Army's Command and Control System for Logistics.' School of Advanced Military Studies United States Army Command and General Staff College. As of 5 June 2024: https://apps.dtic.mil/sti/pdfs/ADA506268.pdf

Sarnaik, Sonal, & Basit Ansari. 2018. 'Prime Numbers: Foundation of Cryptography.' In *Cyber Security: Advances in Intelligent Systems and Computing* 729, edited by Bokhari, M., Namrata Agrawal, & Dharmendra Saini. As of 5 June 2024:

https://link.springer.com/chapter/10.1007/978-981-10-8536-9_31#Sec4

Scharre, Paul. 2018. *Army of None: Autonomous Weapons and the Future of War.* New York: W. W. Norton & Company.

Schrittwieser, Julian, Ioannis Antonoglou, Thomas Hubert, Karen Simonyan, Laurent Sifre, Simon Schmitt, Arthur Guez, Edward Lockhart, Demis Hassabis, Thore Graepel, Timothy Lillicrap, & David Silver. 2019. 'Mastering Atari, Go, Chess and Shogi by Planning with a Learned Model.' Deep Mind & University College London, 11 September. As of 5 June 2024: https://arxiv.org/pdf/1911.08265.pdf

Sharma, Gaurav, Deepak Kumar Sharma, & Adarsh Kumar. 2023. 'Role of cybersecurity and Blockchain in battlefield of things.' Internet Technology Letters. As of 5 June 2024: https://doi.org/10.1002/itl2.406

Shepherd Media. 2023. 'Winners "will be the people who can do multi-domain integration at the speed of the digital age."' Universal Defence, 28 September. As of 5 June 2024:

https://www.universal-defence.com/blog/winners-will-be-the-people-who-can-do-multi-domain-integration-at-the-speed-of-the-digital-age

Song, Gyeongju, Kyungbae Jang, Siwoo Eum, Minjoo Sim, & Hwajeong Seo. 2023. 'NTT and Inverse NTT Quantum Circuits in CRYSTALS-Kyber for Post-Quantum Security Evaluation.' *Applied Sciences* 13(18): 10373. As of 5 June 2024: https://doi.org/10.3390/app131810373

Stone, John. 2020. 'Strategic lessons from military planning under conditions of uncertainty, complexity and risk.' *Journal of Mega Infrastructure & Sustainable Development* 2(1): 32–46. As of 5 June 2024: https://doi.org/10.1080/24724718.2021.1984689

Størdal, John-Mikal. 2020. 'Technological trends and their impact on defence planning.' Norwegian Defence Research Establishment (FFI), 11 January. As of 6 June 2024:

https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2663/20-00228.pdf

The White House. 2022. 'Migrating to Post-Quantum Cryptography.' Executive Office of The President: Office of Management and Budget, 18 November. As of 5 June 2024: https://ve42.co/PQCWhiteHouse

Thomson, Judith Jarvis. 1985. 'The Trolley Problem.' *The Yale Law Journal* 94(6): 1395–1415. As of 5 June 2024: https://doi.org/10.2307/796133

Toshiba. 2023. 'Quantum Key Distribution.' As of 5 June 2024:

https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html

Townsend, Kevin. 2022. 'Solving the Quantum Decryption "Harvest Now, Decrypt Later" Problem.' SecurityWeek, 16 February. As of 5 June 2024:

https://www.securityweek.com/solving-quantum-decryption-harvest-now-decrypt-later-problem/

Trivedi, Anusua, Kate Keator, Michael Scholtens, Brandon Haigood, Rahul Dodhia, Juan Lavista Ferres, Ria Sankar, & Avirishu Verma. 2021. 'How to Handle Armed Conflict Data in a Real-World Scenario?' *Philosophy & Technology* 34(1): 111–23. As of 5 June 2024: https://doi.org/10.1007/s13347-020-00424-5

Tschandl, Philipp, Christoph Rinner, Zoe Apalla, Giuseppe Argenziano, Noel Codella, Allan Halpern, Monika Janda, Aimilios Lallas, Caterina Longo, Josep Malvehy, John Paoli, Susana Puig, Cliff Rosendahl, H. Peter Soyer, Iris Zalaudek, & Harald Kittler. 2020. 'Human–computer collaboration for skin cancer recognition.' *Nature Medicine* 26: 1229–34. As of 5 June 2024: https://www.nature.com/articles/s41591-020-0942-0

UK Government. 2021. *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy.* Gov.uk, 16 May. As of 5 June 2024: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

———. 2023. *Integrated Review Refresh 2023: Responding to a more contested and volatile world*. Gov.uk. As of 5 June 2024:

https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world

UK Ministry of Defence. 2017. 'Future of Command and Control (JCN 2/17).' 8 September. As of 5 June 2024: https://www.gov.uk/government/publications/future-of-command-and-control-jcn-217

———. 2018a. 'Human Machine-Teaming (JCN 1/18).' 21 May. As of 5 June 2024: https://www.gov.uk/government/publications/human-machine-teaming-jcn-118

———. 2018b. 'Information Advantage (JCN 2/18).' 18 September. As of 5 June 2024: https://www.gov.uk/government/publications/information-advantage-jcn-218

———. 2020a. 'Integrated Operating Concept'. 30 September. As of 5 June 2024: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025

———. 2020b. 'Multi-Domain Integration (JCN 1/20).' 2 December. As of 5 June 2024: https://www.gov.uk/government/publications/multi-domain-integration-jcn-120

———. 2022. 'Defence Artificial Intelligence Strategy'. 15 June. As of 5 June 2024: https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy

———. 2023. 'Agency and Agility: Incentivising People in a New Era – A Review of UK Armed Forces Incentivisation by Rick Haythornthwaite.' 19 June. As of 5 June 2024: https://www.gov.uk/government/publications/agency-and-agility-incentivising-people-in-a-new-era-a-review-of-uk-armed-forces-incentivisation

Van Amerongen, Michiel. 2021. 'Quantum technologies in defence & security.' *NATO Review*, 3 June. As of 5 June 2024:

https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html

von Clausewitz, Carl. 1874. *On War*. Project Gutenberg Ebook, released 2006. As of 30 May 2023: https://www.gutenberg.org/files/1946/1946-h/1946-h.htm

Watling, Jack. 2023. 'Supporting Command and Control for Land Forces on a Data-Rich Battlefield.' *RUSI Occasional Paper*. As of 5 June 2024:

https://static.rusi.org/Supporting-command-and-control-for-land-forces-on-a-data-rich-battlefield.pdf

Welch, Chris. 2023. 'Building a computer that solves practical problems at the speed of light.' Microsoft, 27 June. As of 5 June 2024:

https://news.microsoft.com/source/features/innovation/building-a-computer-that-solves-practical-problems-at-the-speed-of-light/

Wilson, J. R. 2018. 'Electro-optical sensors key to missile defense.' *Military + Aerospace Electronics*. 1 January. As of 5 June 2024:

https://www.militaryaerospace.com/communications/article/16707380/electrooptical-sensors-key-to-missile-defense

Wondimu, Natnael A., Cédric Buche, & Ubbo Visser. 2022. 'Interactive Machine Learning: A State of the Art Review.' As of 5 June 2024: https://arxiv.org/abs/2207.06196

Wong, Jonathan P., Obaid Younossi, Christine Kistler LaCoste, Philip S. Anton, Alan J. Vick, Guy Weichenberg, & Thomas C. Whitmore. 2022. *Improving Defense Acquisition: Insights from Three Decades of RAND Research*. Santa Monica, Calif.: RAND Corporation. RR-A1670-1. As of 5 June 2024: https://www.rand.org/pubs/research_reports/RRA1670-1.html

Xiao, Yinhao, Yizhen Jia, Chunchi Liu, Xiuzhen Cheng, Jiguo Yu, & Weifeng Lv. 2019. 'Edge computing security: State of the art and challenges.' *Proceedings of the IEEE* 107(8): 1608–31. As of 5 June 2024: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8741060

Yamamoto, Yoshihisa, Kazuyuki Aihara, Timothee Leleu, Ken-ichi Kawarabayashi, Satoshi Kako, Martin Fejer, Kyo Inoue, & Hiroki Takesue. 2017. 'Coherent Ising machines—optical neural networks operating at the quantum limit'. *NJP Quantum Information* 3: 49. As of 5 June 2024: https://doi.org/10.1038/s41534-017-0048-9

Ye, Weirui, Shaohuai Liu, Thanard Kurutach, Pieter Abbeel, & Yang Gao. 2021. 'Mastering Atari Games with Limited Data.' *Advances in Neural Information Processing Systems* 34. As of 5 June 2024: https://paperswithcode.com/paper/mastering-atari-games-with-limited-data

Zabrodskyi, Mykhaylo, Jack Watling, Oleksandr V. Danylyuk, & Nick Reynolds. 2022. 'Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022.' *RUSI Special Resources*. As of 5 June 2024:

https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-conventional-warfighting-russias-invasion-ukraine-february-july-2022

Annex A. Workshop participants

The fourth expert workshop on C2 in the future was held at DCDC in Shrivenham on 12 December 2023. Attendees at this workshop were as follows:

Table A.1 List of workshop participants

Name	Organisation
Alec Bain	Dstl
Paul Baller	Thales
Ralph Dekker	Ministry of Defence of The Netherlands
Maj. Mark Dobson	MOD
Christopher Goodsell	MOD
James Hanson	MOD
Robert Hercock	BT
Jim Hill	Dstl
Professor Ed Keedwell	University of Exeter
Robert Kemplay	MOD
Jack McEvoy	Dstl
Gorden Niven	Dstl
Damien K. Trower	Lockheed Martin
P. J. Turner	QinetiQ
Rebecca Lucas	RAND Europe
Stella Harrison	RAND Europe
Cdr Leif Hansson	DCDC
Peter Houghton	Dstl
Lt Col. Robert Kace	DCDC
Lt Col. Ed Vickers	DCDC