Ministry
of Defence

Joint Capability Concept Note 1/25

Developing Command and Control: now and into the future

Joint Capability Concept Note 1/25

Developing Command and Control: now and into the future

Joint Capability Concept Note (JCCN) 1/25,
dated September 2025,
is promulgated as directed by the Chiefs of Staff

Director Integrated Warfare Centre

Conditions of release

Authorisation

If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals.

Email: UKStratCom-DFutures-Pubs@mod.gov.uk

Copyright

Front cover image © Peshkova/Shutterstock.com

If contacting Defence Intellectual Property Rights for authority to release outside of the UK government and MOD, the Patent Officer should be informed of any third party copyright within the publication.

Crown copyright and Merchandise Licensing, Defence Intellectual Property Rights, Central Legal Services, MOD Abbey Wood South, Poplar 2 #2214, Bristol, BS34 8JH. Email: DIPR-CC@mod.gov.uk

Distribution

Our publications are available internally to MOD staff from the Leidos Forms and Publications Team using the Millie Online Portal.

Email: leidos-formspublications@teamleidos.mod.uk

Digital versions of our publications can be viewed and downloaded on defnet at: https://modgovuk.sharepoint.com/sites/IntranetUKStratCom/SitePages/defence-futures.aspx

This publication is also available at: www.gov.uk/mod/dcdc

Preface

Purpose

1. The purpose of Joint Capability Concept Note (JCCN) 1/25, *Developing Command and Control: now and into the future* is to provide a conceptual basis to inform command and control (C2) developments that will enable an integrated force to overcome challenges and seize opportunities in an evolving operating environment. This JCCN provides the rationale for developing C2 within Defence over the next five years. It also seeks to promote alignment of C2 capability across Defence and prevent disjointed solutions.

Context

2. JCCN 1/25 steps beyond Joint Concept Note (JCN) 2/17, *Future of Command and Control*, which recognised the need for future C2 systems to be designed for escalating global power competition and to be able to adapt to a broad range of crisis and conflict situations. It called for greater agility and the necessary changes to military culture, C2 structures and processes. The ideas proposed remain valid but are insufficient to appropriately gear C2 capability to meet the future needs of Defence. JCCN 1/25 reflects on the increased complexity in the operating environment, and envisages new C2 approaches, adopting new technologies and drawing upon the assertions of Defence's Capstone Concepts.[1]

Scope

3. Whilst this JCCN follows the strategic guidance of the Defence Capstone Concepts, it is written to inform C2 developments out to circa 2030. Conceptualising C2 beyond 2030 is considered highly speculative as the rate of change in technology and the operating environment over the next decade will likely invalidate key assumptions made now. Although this concept does not prescribe solutions for the longer-term future, further work is recommended to investigate certain properties and trends that are expected to impact C2 beyond 2030. Further work is also required to develop the ideas in this JCCN alongside ongoing C2 projects across Defence. Post-publication, this will lead to the development and agreement of a practical concept implementation plan.

[1] The Defence Capstone Concepts are the *Campaigning Capstone Concept 2040* and the *Warfighting Capstone Concept 2040*.

Audience

4. JCCN 1/25 is primarily aimed at those in Defence developing policy and strategic capabilities or undertaking force design. It is intended to inform strategic thinking across Defence, other government departments, industry, science and technology organisations, and allies and partners.

Structure

5. The concept is divided into five chapters with a supporting lexicon. The content is outlined below.

a. **Chapter 1 – Introduction.** Chapter 1 introduces the Defence Capstone Concepts and what that means for new ways of operating. It also introduces the key themes for C2, including terminology.

b. **Chapter 2 – Context and the military problem.** Chapter 2 provides a baseline description of the changing character of conflict and operating environment. It then explores the implications of these changes for C2 and the C2 requirements for an integrated force. This leads to identifying the military problem.

c. **Chapter 3 – Addressing the challenges.** Chapter 3 breaks the military problem into three specific challenges for C2. Each challenge is then explored to identify the attributes of C2 that are required and their enabling functions.

d. **Chapter 4 – Concept proposals.** Chapter 4 describes what needs to be done to cultivate and maintain these enabling functions and thus embed the attributes of C2 required. These proposals will provide a conceptual basis to inform C2 developments across Defence.

e. **Chapter 5 – Further work.** Chapter 5 outlines the further work required to develop themes in this concept and to conceptualise C2 beyond 2030.

Linkages

6. JCCN 1/25 is underpinned by several publications and documents that provide context to this publication. These include:

- *Strategic Defence Review – Making Britain Safer: secure at home, strong abroad* (referred to as *Strategic Defence Review 2025* throughout);

- *Global Strategic Trends – Out to 2055*;

- *Campaigning Capstone Concept 2040*;

- *Warfighting Capstone Concept 2040*;

- Joint Doctrine Publication (JDP) 0-01, *UK Defence Doctrine*;

- JDP 02, *UK Operations: The Defence Contribution to Resilience*;

- JCN 1/18, *Human-Machine Teaming*;

- JCN 2/18, *Information Advantage*;

- Concept information note 1, *Complexity Implications for Defence, and Command and Control*;

- Concept information note 2, *Emergent Defence Organising*;

- Concept information note 3, *The concept of C2 as a capability*;

- Concept information note 4, *Decision-making: How do human-machine teamed decision-makers, make decisions?*;

- Concept information note 5, *If not command and control, then what?*; and

- Joint Service Publication 440*, The Defence Manual of Security.*

Developing command and control – a summary

The implications of:

- the changing character of conflict and operating environment; and
- the need for Defence to enhance operational effectiveness and achieve competitive advantage (drawing on the assertions of the Defence Capstone Concepts) ...

Reveals a military problem:

Existing command and control capability is inadequate for an integrated force approach and is not designed to cope with the complex dilemmas and challenges expected in the operating environment.

The military problem is broken down into three specific challenges:

Command and control capability must be developed to:

- support an integrated force (#1);
- cope with complexity in the operating environment (#2); and
- mitigate the risks from new methods of attack (#3).

To address these challenges, command and control must be:

- resilient;
- artificial intelligence-enabled;
- networked;
- adaptable; and
- integrated.

To embed these attributes, this concept proposes:

- tangible and achievable 'aiming points' that will provide a conceptual basis to inform command and control developments across Defence; and
- further work to develop these ideas alongside other command and control projects within Defence.

The purpose is to:

- develop a command and control capability that will enable an integrated force to overcome challenges and seize opportunities in an evolving operating environment; and
- promote alignment of command and control capability across Defence and avoid disjointed solutions.

Contents

NATO
OTAN

Chapter 1

Introduction

New ways of operating

1.1. The *Campaigning Capstone Concept 2040* proposes a Defence Enterprise[1] that is unified, collaborative and increasingly acts in concert with allies and partners across government.[2] The *Warfighting Capstone Concept 2040* characterises the operating environment as more complex, lethal and transparent, and calls for a force able to create coordinated effects across all operational domains[3] whilst being interoperable with the North Atlantic Treaty Organization (NATO).[4] The *Strategic Defence Review 2025* sets out the ambition for a 'NATO first' policy, noting the UK's strategic strength comes from our Allies and that 'NATO is the bedrock of our defence'.

1.2. For Defence to operate in these ways, its command and control (C2) capability must support a unified, integrated force.[5] It must enable Defence to synchronise activities with partners across government and NATO, and to amplify lethal and non-lethal effects. It must remain effective when faced with the range of dilemmas and pressures of an increasingly complex operating environment.

!

The operating environment is described as increasingly 'complex' due to the rising number of factors impacting it and their interconnectedness. The number of variables will not be manageable and small changes could have unpredictable outcomes. The consequence is a growing presence of non-linearity, meaning that situations are more difficult to comprehend and problems within them may not be controlled or solvable within the traditional sense.

[1] The 'Defence Enterprise' is all of Defence and the supporting agencies, industries, commercial partners and suppliers.

[2] The way Defence, in support of government and in partnership with allies and partners, achieves competitive advantage in pursuit of national interest is described in the *Campaigning Capstone Concept 2040*.

[3] The five operational domains are maritime, land, air, space, and cyber and electromagnetic.

[4] The necessity for a unified force, which can seamlessly operate across the operational domains whilst being interoperable with NATO, is outlined in the *Warfighting Capstone Concept 2040*.

[5] In line with the *Strategic Defence Review 2025*, Defence must be 'integrated by design', capable of operating in different configurations, designed and directed under the authority of the Chief of the Defence Staff with a focus on maximising the effectiveness of the 'whole force' fighting as one across all five operational domains.

© Alexandros Michailidis / Shutterstock.com

1.3. Defence's existing C2 capability will not fully meet these requirements. C2 is generally underpinned by process, policies and hierarchies that are not adaptive and are difficult to understand (particularly for those external to Defence). C2 systems are not suitably networked or 'informationalised'.[6] Equally important is the development of people who have the ability to critically engage with emerging technology in C2 systems, and the skills to embrace alternative models of non-hierarchical collaboration where needed.

Command and control terminology and its functions

1.4. C2 takes place dynamically throughout the assessment, planning, preparation and execution of activities. C2 can be considered a process, capability or system. It can also be treated as a single whole, 'command and control', with a different meaning to the separate words 'command' and 'control'.[7]

a. **Command.** Command is defined as: the authority vested in a member of the armed forces for the direction, coordination, and control of military forces.[8]

b. **Control.** Control is defined as: the authority exercised by a commander over part of the activities of subordinate organizations, or other organizations not normally under their command, encompassing the responsibility for implementing orders or directives.[9]

1.5. There are essential functions commanders need C2 to accomplish to achieve its purpose. These include, but are not limited to:

- creating shared awareness (including awareness of shared purpose);
- allocating resources to create effects;
- assessing progress; and
- providing C2 adaptability to recognise and conduct a change of approach or plan of action.[10]

[6] 'Informationalised' is a consequence of the Information Age and the proliferation of information technology. It is the ability to gather, store, manage and transmit information. Information resources and information networks are the foundation; information technology and talent are enablers.

[7] See Allied Joint Publication (AJP)-01, *Allied Joint Doctrine*, Edition F, Version 1.

[8] NATOTerm.

[9] NATOTerm.

[10] See AJP-01, *Allied Joint Doctrine*, Edition F, Version 1 for more information.

Command and control approach

1.6. For military operations, C2 is based on the existence of 'a commander' who holds authority and exercises overall 'control'. Such an approach does not meet all the needs of a force that must integrate across operational domains and synchronise activities with partners and NATO.

> … the difference between command and control on the one hand, and adapt and collaborate on the other, was the difference between success and failure.
>
> General Stanley McChrystal

1.7. Depending on the nature of partners (or neutral actors) different C2 organisational approaches will be required. In some cases, the control (the 'authority exercised by the commander over the activities of subordinate organisations') may be extremely limited or non-existent, for example, when working with non-Defence entities or with a mix of multiple partners across government and other actors (see C2 enterprise description in paragraph 1.10 for more details). In such scenarios, control may be largely reliant on influence won through cooperation. In other cases, it may be necessary for military entities to devolve a level of control to a non-military authority to integrate decision-making. The appropriate C2 organisational approach will depend on the partners and the degree of integration needed to shape the engagement space. Given that interaction with partners may be fluid and alter in response to dynamic challenges, it is important the C2 approach can be changed with pace and ease ('adaptability' is discussed further in Chapter 3). The C2 approach must also change depending on the operating environment (which is discussed further in Chapters 3 and 4). Table 1.1 provides example C2 organisational approaches dependent on the degree of integration with partners. These example C2 organisational approaches are aligned with NATO recommended approaches.[11]

[11] See AJP-01, *Allied Joint Doctrine*, Edition F, Version 1 for more information.

Example C2 organisational approaches	Degree of integration with partners
Coexistence	• Organisations have no interaction; two or more actors are aware of each other's presence but will not directly interact.
Consultation	• Different organisations will seek the opinion or advice of other actors. • While some information will be shared, decisions are made independently.
Deconfliction	• Formal communication will take place and decisions are coordinated, but actions are conducted independently. • The aim is to ensure that the best organisation available will undertake the required tasks. • Organisations will avoid undesirable interference between actors, especially where they perform the same function or occupy the same space.
Coordination	• To be used to bring together different elements of a complex activity or organisation into an efficient relationship. • Organisations share information and frequent communication occurs. • Some shared decision-making will take place, fostered by shared objectives.
Cooperation	• Organisations will work together for mutual benefit. • A shared decision-making process may exist between organisations. • Cooperation does not mean giving up authority or autonomy.
Coalition	• Partners that operate within a formalised task and responsibilities structure. • Coalition partners devolve a defined level of their authority and autonomy to a single authority to integrate decision-making and actions towards the end state.

Table 1.1 – Example command and control organisational approaches

Command and control capability

1.8. This joint capability concept note conceptualises C2 capability as a dynamic, adaptive socio-technical system that emerges from its attributes forged by enabling functions. These functions are 'things' that result from complex interactions between people, processes, structures, technology and data. This conceptualisation is illustrated at Figure 1.1.

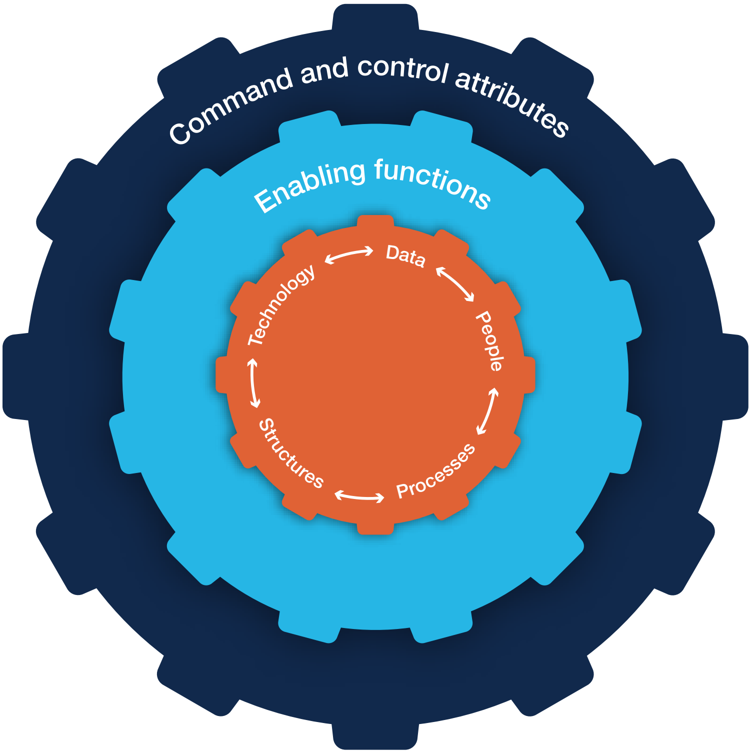


Figure 1.1 – Conceptualisation of command and control capability

1.9. This concept seeks to determine the C2 attributes needed and then propose enabling functions that serve to cultivate and maintain them. The aim is to develop a C2 capability that will enable Defence's integrated force to design and execute multi-domain operations, be interoperable with NATO and synchronise activities with partners.

The command and control enterprise

1.10. The ‘C2 enterprise’ is the span of organisations that might be engaged to design and execute activities or operational actions.[12] Extending beyond the traditional Defence-centric organisations to collaborate with non-Defence organisations is essential to generate a wider perspective of complex problems and converge effects using all levers of influence. Prospective partners in the wider ecosystem (beyond Defence) include partners across government, international partners, defence industry, other private sector entities, academia and non-governmental organisations. Contributions from these organisations include, but are not limited to:

- sensing and awareness;
- networks, relationships and influence;
- knowledge and understanding;
- specialist effectors (in a given operational domain or area of activity);
- basing and supply chains; and
- underlying intellectual property, technology, industrial or financial resources.

1.11. The specific organisations that comprise the C2 enterprise are not fixed. To confront a given problem or exploit an opportunity, Defence must determine the appropriate configuration of actors and seek to integrate with them through formalised arrangements or negotiated agreements.

[12] RAND Europe, *Command and Control in the Future – Concept Paper 2: The Defence C2 Enterprise*, 2024.

Notes

ROYAL NAVY
ZP526

Chapter 2

Context and the military problem

The changing character of conflict

2.1. Future conflicts will be characterised by ubiquitous sensors with mass data collection and processing abilities that minimise the opportunity for military forces to hide.[13] Wider adoption of commercial imagery, behaviour-tracking data and artificial intelligence-augmented analysis tools will accelerate the ability to sense and make sense of the environment.[14] Combined with artificial intelligence-driven weapon systems, and long-range precision strike complexes, the find and fires revolution of the past decade continues at pace.[15] Inexpensive drones, loitering munitions and precision-guided munitions with increasing speed, range and accuracy will reduce the time it takes to close the kill chain.[16] The increasing development of space and cyber platforms and capabilities, both lethal and non-lethal, ensure the next war's decisive terrain will be across the physical, information and human dimensions.[17]

The changing operating environment

2.2. The character of the future operating environment is clouded by significant uncertainty.[18] Evolving threats and responses are not constrained to the physical dimension or even military spheres.[19] Our adversaries compete in non-traditional ways, with a growing tendency to challenge our political will

[13] General Mark A. Milley, 'Strategic Inflection Point: The Most Historically Significant and Fundamental Change in the Character of War Is Happening Now–While the Future Is Clouded in Mist and Uncertainty', *Joint Force Quarterly*, Issue 110, 3rd Quarter, 2023.

[14] Ibid.

[15] *The Land Operating Concept – A New Way of Winning*, February 2023.

[16] The kill chain describes three fundamental steps that militaries do on the battlefield or wherever they compete: the first is gaining an understanding about what is happening; the second is making a decision about what to do; the third is taking action that creates an effect to achieve an objective. Christian Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare*, 2020.

[17] General Mark A. Milley, 'Strategic Inflection Point: The Most Historically Significant and Fundamental Change in the Character of War Is Happening Now–While the Future Is Clouded in Mist and Uncertainty', *Joint Force Quarterly*, Issue 110, 3rd Quarter, 2023.

[18] RAND Europe, *Command and Control in the Future, Concept Paper 1: Grappling with Complexity*, January 2024.

[19] *Campaigning Capstone Concept 2040.*

to respond through the virtual and cognitive dimensions. The wide variety of factors and trends contributing to a more complex operating environment range across all areas of political, economic, social, technological, legal, environmental and military (PESTLE-M) frameworks.[20] Complexity will arise from these multiple factors converging in unknown and unpredictable ways, with particular emphasis on the following macro-level trends.

a. **Increasing global interconnectivity, multipolarity and global competition.** Geopolitical and geo-economic trends are seen as driving complexity by heightening the number of concurrent and converging challenges facing societies and, by extension, governments and militaries.

b. **The impact of a changing climate.** Environmental trends interlinked with social trends could lead to greater disorder, instability and ultimately future conflict.

c. **The impact of technological change.** As digitalisation continues worldwide, technological connections and interdependencies within systems, organisations and broader society continue to grow.

d. **The blurring of operational domains, both traditional and novel.** Traditional distinctions between operational domains are diminishing as global systems and networks across the PESTLE-M spectrum multiply and become increasingly interconnected.

e. **The shifting of international norms and value sets.** The impact of broader trends occurring within politics and shifting cultural norms are driving instability. For example, growing political instability, the increasing power of non-state and non-governmental organisations, and the rise of opinion-forming and influencing communities beyond the control of conventional media and authorities, unconstrained by geography.

[20] RAND Europe, *Command and Control in the Future – Concept Paper 2: The Defence C2 Enterprise*, 2024.

Implications for command and control

2.3. Mitigating the complex web of interacting PESTLE-M trends will continue to challenge Defence's existing command and control (C2) capability. No single military force or government department can tackle these issues on their own; the expertise of a range of organisations (including non-Defence entities) will be needed. To develop the responses necessary, Defence must be able to reach into new pools of intuition, creativity and innovation.

2.4. Existing approaches are not designed to make the best possible sense of ambiguity and non-linearity, which are by-products of a complex operating environment. Under such circumstances, it is unlikely that a decision-maker can fully comprehend a situation and develop a solution through simple causal reasoning. People must be trained to work amidst complexity where solutions are not standardised[21] and depend on collaboration and adaptive decision-making.[22] C2 structures and authorities must enable the agility (the pace and ease) of decision-making needed for increasing global power competition and for warfighting in new ways.[23]

Complexity is a condition in which multiple variables, some of which are unknown and/or unmeasured, interact in unknown ways to create inherently unknowable outcomes. Complexity in the operating environment results in increased unpredictability and non-linearity.

2.5. Emerging technology presents a number of opportunities to enhance C2 capabilities. Advances in data-to-decision technology, powered by artificial intelligence, machine learning and human-machine teaming offer the potential to transform sense-making and decision-making. Novel computing, fifth generation (5G) technology, low Earth orbit satellites, mesh networks and ultra-broadband solutions can support delivery of advanced networks, as needed to evolve C2 from its current form to an informationalised and integrated enterprise. It is important to consider new vulnerabilities that will arise from using new technologies. Legal and policy issues related to using

[21] Noting that in complex situations problems cannot be definitively solved in the traditional sense.

[22] Adaptive decision-making describes the process of revisiting, adjusting and reapplying decisions in line with the recommended 'probe–sense–respond' Cynefin approach for complex environments. See Chapter 4 for more information.

[23] New ways of warfighting are detailed in the *Warfighting Capstone Concept 2040*.

new technologies will also need to be identified. Despite the onset of artificial intelligence and digital data tools, people must remain at the heart of C2 to capitalise on their judgement, maintain ethical boundaries and provide resilience where technology is degraded or lost.

2.6. The attributes of warfighting organisations are rapidly developing. Lethal effect will increasingly be created through a widely dispersed mix of crewed, uncrewed and autonomous assets underpinned by data flows and able to periodically mass to create military effect when required.[24] C2 must be able to support the operational activities of highly mobile military forces over an expanded engagement space. Defence's C2 capability must also be resilient, with organisations and their supporting systems able to provide a variety of ways to mitigate hostile efforts to disrupt them.

Command and control requirements for an integrated force

2.7. Existing C2 capability has not been designed to support an integrated force that operates as one across the five operational domains, and with the North Atlantic Treaty Organization (NATO) or non-military partners as required. Existing C2 structures and processes are shaped to deliver military-centric solutions; they generally default to a one-size fits all model with hierarchical authorities controlled at the operational level. This can result in 'task overlap' and conflicting priorities between operations that impede the orchestration of military activities across operational domains. This is exacerbated by a Defence tendency for short-term focus and a crisis mentality.

2.8. For an integrated force to achieve operational effectiveness and achieve competitive advantage, the key C2 requirements (discussed in more detail in Chapter 3) include:

- command structures with the authorities and people skills to enable planning and execution of cross-domain military activities, synchronisation with the activities of non-military partners, and interoperability with NATO;

- new organisational approaches depending on the nature of our partners (or neutral actors) where control may be limited and influence must be won; and

[24] As described in the *Strategic Defence Review 2025*.

- a common digital foundation to share data in support of sense-making, assessment, planning and decision-making across the C2 enterprise.[25]

The military problem

2.9. Implications of the changing character of conflict and operating environment, and the requirements for an integrated force, lead to identifying the military problem. The problem is that existing C2 capability is:

- inadequate for an integrated force approach; and

- not designed to cope with the complex dilemmas and challenges expected in the future operating environment.

[25] In line with the *Strategic Defence Review 2025*.

Chapter 3

Addressing the challenges

3.1. Chapter 3 takes the military problem identified in Chapter 2 and breaks it down into three specific challenges. Command and control (C2) capability must be developed to:

- support an integrated force approach;
- cope with complexity in the operating environment; and
- mitigate the risks from new methods of attack.

Each of these challenges is explored to identify the attributes of C2 that are required and their enabling functions. Chapter 4 will detail specific proposals to cultivate and maintain the enabling functions and, in doing so, embed the C2 attributes that will address the military problem.

Challenge 1 – support an integrated force

3.2. The ability to control the weight of effort in each operational domain is central to the integrated force and to the alignment with the North Atlantic Treaty Organization (NATO). Through all levels of military command (strategic, operational and tactical), the nominated commanders must have the necessary authorities and resources to orchestrate military activities across the five operational domains. The supporting command structures must be dynamic, adjustable to fit specific environments, domain agnostic and interoperable with NATO multi-domain operations. Interoperability with NATO also requires alignment with developing NATO command principles and their information sharing architecture.

3.3. A key challenge is enhancing Defence's ability to synchronise military and non-military activities to achieve synergy through converging effects. This requires Defence to collaborate with partners (military and non-military)[26] and contribute to unity of purpose across an effective C2 enterprise. New relationships must be fostered to help Defence understand the abilities, approaches and cultures of our partners. New ways of operating should be developed to help Defence staff function effectively in a C2 enterprise where military responsibilities are bounded within a wider system. Defence

[26] Table 1.1 illustrates examples of the C2 organisational approaches that support collaboration at varying degrees of integration.

must accept that 'command' is largely limited to military entities (noting that functions and authorities are already hard to exert across Defence itself given the wide range of organisations that often have different visions, reflecting differences in mission objectives, remit, culture and available means).

3.4. The collection, processing and distribution of data must take place on a far greater scale and be faster.[27] Some of our adversaries have invested heavily in developing sophisticated networks to support multi-domain precision strike complexes. To compete, our networks must be enhanced to support rapid data flow from sensors, deciders (headquarters, operational teams, allies and partners) and effectors. Defence must develop a common digital foundation of data that provides all partners (within the appropriate C2 enterprise) with a coherent understanding about what is happening and what can be achieved. To be effective across the C2 enterprise, this must be supported by the ability to declassify information and modify access permissions to enable rapid data sharing. A robust means of communicating at all classification levels with military stakeholders and political strategic decision-makers is necessary. A summary of attributes needed to address Challenge 1 is shown at Table 3.1.

[27] In line with the *Strategic Defence Review 2025*, it is through dynamic data networks of crewed, uncrewed and autonomous assets and data flows that lethality and military effect are now created.

Attributes needed	Enabling functions
Integrated The ability to collaborate, forge unity of purpose, synchronise activities and orchestrate military activities across the C2 enterprise.	• Empowered commanders with the necessary authorities and resources to orchestrate military activities across the five operational domains. • Dynamic command structures that are adjustable to fit specific environments. • Interoperability with NATO multi-domain operations. • New relationships and new ways of operating that help Defence function effectively within the wider C2 enterprise. • Unity of purpose across diverse stakeholders of the C2 enterprise.
Networked The C2 enterprise must be underpinned by a common digital foundation providing the necessary communications, shared information and access to artificial intelligence-enabled decision aids.	• Rapid data flow from sensors, deciders (headquarters, operational teams, allies and partners) and effectors. • A common digital foundation of data that provides all partners (within the appropriate C2 enterprise) with a coherent understanding about what is happening and what can be achieved. • Controlled data access underpinned by the ability to rapidly declassify information and modify access permissions. • A robust means of communicating at all classification levels with military stakeholders and political strategic decision-makers.

Table 3.1 – The attributes needed to address Challenge 1 and their enabling functions

Challenge 2 – cope with complexity in the operating environment

3.5. Complexity will manifest as a range of dilemmas and pressures resulting from cross-cutting effects of the political, economic, social, technological, legal, environmental and military (PESTLE-M) trends. Complexity will result in a greater prevalence of uncertainty, ambiguity, information overload, high-tempo fast-moving events and non-linearity[28] in the operating environment. It is not the case that we will always be operating in a complex operating environment and any environment can morph into, or away from, complexity. The challenge is to develop a C2 capability that can adapt to a changing environment and can be effective in mitigating complexity where required. A framework is needed to guide the right approach depending on complexity of the environment and the degree of integration with partners (see paragraph 1.7). Such adaptability is largely dependent on the people who must be developed to understand different C2 approaches and when they should be applied.

3.6. People must be developed to work amidst complexity where solutions are not standardised and depend on collaboration, innovation and adaptive decision-making. This requires relationships that support an expanded C2 enterprise to be grown and maintained. There is potential synergy between mitigating complexity and delivering an integrated force in that both are dependent on a C2 enterprise comprising non-military entities to provide a broader perspective and deliver a sophisticated response.[29]

3.7. Artificial intelligence tools should be developed to help people make the best possible sense of large volumes of information, ambiguity and non-linearity at machine speeds. Artificial intelligence-supported decision-making would help protect against faulty decisions, drive conformity with strategy and protect against non-compliance with policy, regulation and law. This is not to say that all aspects of C2 should be artificial intelligence-enabled; the benefits of artificial intelligence must be weighed against its limitations. These limitations include cost, energy demands and risks, for example, technical failure and the potential to be deceived or spoofed. It will be important to develop legal and policy frameworks to support human-machine teaming and the appropriate skills within our workforce. A summary of attributes needed to address Challenge 2 is shown at Table 3.2.

[28] Non-linearity in this context refers to systems whose outputs are not directly proportional to their inputs.
[29] In line with the *Strategic Defence Review 2025*, a key feature of the integrated force is collaboration with other government departments to achieve maximum effect in response to national security challenges.

Attributes needed	Enabling functions
Adaptable C2 approaches must be changeable depending on the complexity of the environment and the level of interaction with partners.	• A framework to guide the right approach depending on complexity of the environment and the degree of integration with partners. • People who are adaptable and who understand different C2 approaches and when they should be applied. • People who can work amidst complexity where solutions are not standardised and depend on collaboration, innovation and adaptive decision-making.
Artificial intelligence-enabled Develop artificial intelligence tools that can be integrated into C2 networks to improve speed and quality of human understanding, reasoning, knowledge representation and planning.	• Artificial intelligence tools that support people to make sense of large volumes of information, ambiguity and non-linearity at machine speeds. • Legal and policy frameworks that support human-machine teaming. • Develop workforce with appropriate skills to support working with artificial intelligence and human-machine teaming.

Table 3.2 – The attributes needed to address Challenge 2 and their enabling functions

Challenge 3 – mitigate the risks from new methods of attack

3.8. The current deployed force model usually requires the provision of J1–J9 functions to enable routine campaign management and multi-domain operations. On recent coalition operations this has resulted in large operational headquarters in fixed locations. These are increasingly vulnerable to new methods of attack, such as long-range precision strike, autonomous swarming or cyberattack. Headquarters must aspire to be smaller, more mobile and/or dispersed. C2 nodes should also be increasingly dispersed. Larger numbers of small elements with fewer functions are desired to complicate adversary targeting and decrease pay-off for adversary strike. Greater emphasis must be placed on assessing the risks to C2 and implementing necessary measures for force protection and survivability.

3.9. Most communication and information systems are vulnerable to electromagnetic attack or cyberattack. Some legacy systems are likely to be detected as soon as they are activated, creating risks of both physical and non-physical attack. Other key nodes, such as satellites in orbit, are inherently difficult to hide and will likely be targeted immediately. C2 systems and organisations must offer a variety of ways of operating that can mitigate hostile efforts to disrupt them. A summary of attributes needed to address Challenge 3 is shown at Table 3.3.

Attributes needed	Enabling functions
Resilient C2 nodes should be increasingly dispersed. Larger numbers of small elements with fewer functions are desired to complicate adversary targeting and decrease pay-off for adversary strike. The vulnerabilities of communication and information systems need to be mitigated.	• Establish a clear means of assessing the risks to C2 and the resilience required. • Enhance force protection and survivability. • C2 systems and organisations must offer a variety of ways of operating that can mitigate hostile efforts to disrupt them.

Table 3.3 – The attributes needed to address Challenge 3 and their enabling functions

Notes

Chapter 4

Concept proposals

4.1. Chapter 3 broke down the military problem into three specific challenges for command and control (C2) and explored each one to identify the attributes of C2 needed and their enabling functions. The concept proposals in Chapter 4 are intended to cultivate and maintain these enabling functions and, in doing so, embed the C2 attributes that will address the military problem. The proposals are tangible and achievable 'aiming points' that provide a conceptual basis to inform C2 developments across Defence.

Section 1 – Developing integrated command and control

Establish unity of purpose

4.2. For the integrated force to work effectively with partners, Defence should seek to foster unity of purpose across diverse stakeholders. Unity of purpose starts with agreeing the strategic-level objectives. Where appropriate, this must include agreements with partners who are external to Defence. In such cases, clear decision authorities should be established and military staff must be mindful of the limits of their authorities. Defence activity should be planned and prioritised accordingly with resources ring-fenced from short-term crisis tasks. Whilst the central role of a military commander will remain 'the direction, coordination and control of military forces',[30] when seeking unity of purpose with organisations external to Defence a mindset of 'enabling and catalysing' is required. The importance of unity of purpose and the impact of behaviours should be emphasised to Defence staff through training and organisational frameworks.

New relationships and new ways of operating

4.3. Defence should develop people who are suitably qualified and experienced to undertake C2 roles in an integrated force. Joint competencies should be developed to ensure all aspects of military influence alongside other

[30] See Allied Joint Publication-01, *Allied Joint Doctrine*, Edition F, Version 1 for more information.

levers of influence are understood, as well as how synchronised activities can be used to amplify lethal and non-lethal effects. New career options should be established to incentivise people to develop C2 specialist skills, preparing them to operate effectively in the political, social and information dimensions. New ways of operating are required that allow military commanders to shape the focus and influence of a diverse range of partners. This requires a change in perspective and embracing our roles as subjective, co-creative agents within a C2 enterprise. Professional training should include the soft skills that are essential for collaboration, such as relationship building, empathy, cultural understanding and the ability to influence. Through training and experience, people should learn to understand the abilities and approaches of partner organisations, the technologies and information tools at their disposal and the limit of their authorities.

4.4. To grow and maintain an effective C2 enterprise, Defence should gain a deeper understanding of the structures and cultures of the interacting organisations and act to nurture collaboration. The following proposals are intended to address organisational barriers and build relationships.

a. Multi-domain awareness amongst military people should be enhanced. Decision-makers must understand the capabilities, ways of operating and limitations of each operational domain. This is a challenge that can only be addressed through joint opportunities, consistent education and regular multi-domain exercises.

b. Opportunities for greater collaboration with partners across government should be developed. Defence already works across government in core capability areas such as cyber defence, aerial surveillance and maritime security operations. Defence should seek to widen its contributions to government initiatives and ‘grow’ collaboration through mechanisms such as exchange tours, joint training and exercising. The aim must be for Defence personnel to better understand the approaches and cultures within other departments, and learn how to navigate and influence these systems.

c. Greater efforts are required to forge effective relationships with the network of diverse, non-government stakeholders that comprise the C2 enterprise (or might do so in the future). Each organisation will have their own value systems, structures, hierarchies, ways of working and capabilities that can be brought to bear to address problems of national interest. Cultural and organisational barriers may exist, such as ethical concerns about Defence approaches and confusion around military organisations and ways of working. Defence should break down such barriers through sharing information and lessons. To cultivate a better understanding of non-governmental organisations, an increase in burden sharing and partnering arrangements will be needed.

Empowered commanders

4.5. An integrated force relies on commanders who are empowered to orchestrate activities across operational domains and synchronise activities with non-military partners. Defence should ensure the necessary authorities and autonomies are granted to empower decision-making at every level. At the strategic level, commanders need to shape the overall strategic direction of conflict and interface with political leadership to determine phasing and controlling conflict scale. At the operational level, commanders must ensure all activities within a campaign are coordinated and arranged to support the overarching strategic military objectives and direct activities to that end. At the tactical level, the principles of mission command remain valid, but commanders also require decision-making authority to direct and employ capabilities from other operational domains within their area of responsibility. Authorities and autonomies should be established based on the notion that decision-makers with proximity to the specific operation, mission or activity will likely have the situational awareness and on-site knowledge to adaptively make informed, faster and ultimately better decisions. It remains critical that the responsibilities, authorities and accountability for actions must be clearly understood at all times and by all commanders. This criticality is not only a legal and ethical necessity, but it also ensures that there are no delays in creating effects as a result of ambiguity.

Dynamic command structures

4.6. Defence should establish dynamic command structures. Primarily, these must enable effective interoperability between operational domains, military entities and North Atlantic Treaty Organization (NATO) Allies. They must also be tailorable to the required levels of authorities and autonomies, interoperability between operational domains and connections within the wider C2 enterprise. They must be rapidly reconfigurable to establish new connections that enhance partnering with non-military entities and collaborative decision-making. For resilience, it must be possible to dynamically manoeuvre from centralised command structures to a more dispersed model based on threat conditions (see paragraph 4.23 for more information on dispersal).

Interoperability

4.7. Defence should deliver deeper interoperability with NATO Allies.[31] To support interoperability, this joint capability concept note seeks to drive alignment with the NATO command imperatives of dynamic command, collective understanding, technological adaptation and resilience.[32] Defence, through the force development cycle, should continue to drive technical interoperability into capability development from the outset. To achieve a multi-domain operations-enabled integrated force, there are also requirements to develop procedural and human interoperability with NATO. Defence should continue to collaborate with Allies through strategic force development activities and joint exercises to determine how we should integrate, operate and warfight together. Critical to interoperability is access to common data and the secured distribution of relevant information and intelligence. Defence must develop a common digital foundation (see paragraph 4.10 for more information). Defence should continue to influence the NATO principles of cross-domain command, driving interoperability through national concepts, doctrine, training and equipment.

	Enabling functions	Concept proposals for Defence
Command and control must be integrated	Unity of purpose	• Establish strategic objectives in collaboration with partners (including those external to Defence where necessary). • When operating as an integrated force, clear decision authorities must be established and respected. • Defence activity should be prioritised, planned and apportioned with resources ring-fenced from short-term crisis tasks. • Military commanders should adopt a mindset of 'enabling and catalysing' with non-military partners. • Training and process need to emphasise to staff the importance of unity of purpose and the impact of behaviours.

[31] Recommendation 2 of the *Strategic Defence Review 2025* requires Defence to establish 'a roadmap for delivering this deeper interoperability with NATO Allies and for leading the way on shared approaches and standards by January 2026.'
[32] As detailed in NATO's *Cross-Domain Command Concept*, which is currently being developed (latest draft May 2025).

	Enabling functions	Concept proposals for Defence
Command and control must be integrated (continued)	New relationships and new ways of operating	• Develop people who are suitably experienced and qualified to undertake C2 roles in an integrated force. • Develop ways of operating that allow military commanders to shape the focus and exert influence over a diverse range of partners. • Gain a deeper understanding of structures and cultures of interacting organisations (within the C2 enterprise) and act to nurture collaboration.
	Empowered commanders	• Ensure the necessary authorities and autonomies are granted to empower decision-making at every level. • Authorities and autonomies should be established based on the notion that decision-makers with proximity to the specific operation, mission or activity will likely have the situational awareness and on-site knowledge to adaptively make informed, faster and ultimately better decisions.
	Command structures	• Establish dynamic command structures: o tailored to the required levels of authorities and autonomies, interoperability between operational domains, and connections within the wider C2 enterprise; o that enhance partnering with non-military entities and collaborative decision-making; and o that deliver effective interoperability between operational domains, military entities and NATO Allies.
	Interoperability	• Defence, through the force development cycle, should continue to drive technical interoperability into capability development from the outset. • Continue to collaborate with Allies and through strategic force development activities and joint exercises to determine how we should integrate, operate and warfight together. • Develop a common data foundation. • Continue to influence the NATO principles of cross-domain command, driving interoperability through national concepts, doctrine, training and equipment.

Section 2 – Developing networked command and control

Digital targeting web

4.8. Defence should establish a digital targeting web that enables data from any sensor to be rapidly linked to any shooter. The model should be capable of fusing vast data resources at the appropriate classification across national assets and NATO resources to enhance situational awareness, decision-making and real time operations. It should leverage artificial intelligence and machine learning to facilitate rapid data processing, predictive threat analysis and target identification. Using the 'any-any' principle to link any sensor to any effector and its deciders will have a catalytic effect and increase the lethality of target-based kill webs.[33] A common digital foundation capable of rapid data processing should be considered a critical enabler for operational advantage.

4.9. To support this model, it is necessary for Defence to transform its approach to data and elevate the importance of data. Defence should implement a more efficient, coherent enterprise approach to intelligence mission data (IMD)[34] and mission data.[35] The enterprise should encompass all IMD and mission data developers, producers and users across all operational domains. It should seek to coordinate all intelligence inputs to deliver IMD as a single version of the truth that can underpin timely and accurate mission data for effectors and their deciders. Accurate multi-domain mission data produced at speed will ultimately become a key component of warfighting and the ability to optimise kill webs.

Common digital foundation

4.10. Defence should establish an advanced, secure and interoperable common digital foundation, designed to be accessible from any location and during any threat condition. A common digital foundation will enable game-changing analysis and collaborative decision-making at an appropriate tempo. To drive compatibility,

[33] An adaptive kill web offers redundant and multiple paths through functional nodes, thus increasing the quantity and resilience of potential kill chains. This approach is being developed from the linear kill chain methodology to counter the impacts of advanced technologies and artificial intelligence on warfighting.

[34] IMD is defined as: 'a coherent, machine-readable, intelligence-derived data set required to deliver the designed operational capability of platforms, weapons and systems.' Joint Doctrine Publication 0-01.1, *UK Terminology Supplement to NATOTerm*. For example, technical parameters, characteristics and performance, and order of battle.

[35] Mission data is the data that populates detection and self-protection systems of military platforms, allowing operators to understand their environment better and correctly mitigate potential threats.

Defence should agree shared, ubiquitous standards for software and hardware with partners across the C2 enterprise. To compete with sophisticated adversaries, emerging technology should be incorporated. Cloud technologies, fifth generation (5G) wireless networks and ultra-broadband should be investigated for their potential to support a diverse range of connectivity options. Defence should continue to support and influence developments to NATO's federated mission networking[36] as an enabling single information framework for Allies and partners. The UK digital foundation must be compatible, designed as an affiliated network.

Controlled data access

4.11. An imperative for data sharing and operational effectiveness is an ability to declassify information and modify access permissions to enable rapid data sharing. Defence should continue to align with ongoing international programmes to develop data-centric security and zero trust architectures. These initiatives will deliver access to cloud-based data via controlled permissions not hardware. This will allow data access to partners on an as-required basis with data encryption underpinning security of the common digital foundation.

Robust communications

4.12. Defence should ensure interoperable communication channels that provide timely access to relevant and accurate information. These are essential to ensure a broad comprehension of the operating environment across operational domains and a thorough understanding of the commander's intent. Defence should continue to align with NATO by adopting mission threads to define the specific communication, data sharing and activity requirements for any mission. Defence must maintain a highly resilient military messaging system to include a non-repudiation facility, which is critical to conducting operations that require high levels of legal accountability and to ensure a 'last system standing' communication capability. Novel computing, semiconductors, low Earth orbit satellites and mesh networking should be investigated for their potential to enhance the performance and resilience of communication systems. An acknowledged risk to resilience is the vulnerability of space-based assets that are crucial for effective functioning of military communication systems and positioning, navigation and timing (PNT) information. Defence should continue work to develop alternative PNT capabilities and secure, effective terrestrial-based communications systems to mitigate the risk of denial of space-based communications and PNT information.

[36] Further information on NATO's federated mission networking is available at: NATO Allied Command Transformation Federated Mission Networking.

	Enabling functions	Concept proposals for Defence
Command and control must be networked	Rapid data flow	• Establish a digital targeting web that enables data from any 'sensor' to be rapidly linked to any 'shooter'. • Leverage artificial intelligence and machine learning to facilitate rapid data processing, predictive threat analysis and target identification. • Implement a more efficient, coherent enterprise approach to IMD and mission data.
	Common digital foundation	• Establish an advanced, secure and interoperable common digital foundation, designed to be accessible from any location and during any threat condition. • Agree shared, ubiquitous standards for software and hardware with partners across the C2 enterprise. • Review emerging technologies for their potential to support a diverse range of connectivity options. • Continue to support and influence developments to NATO's federated mission networking as an enabling single information framework (the UK common digital foundation must be compatible). • Continue to align with ongoing international programmes to develop data-centric security and zero trust architectures.
	Robust communications	• Ensure interoperable communication channels that provide timely access to relevant and accurate information. • Continue to align with NATO by adopting mission threads to define the specific communication, data sharing and activity requirements for any mission. • Maintain a highly resilient military messaging system to include a non-repudiation facility, which is critical to conducting operations that require high levels of legal accountability and to ensure a 'last system standing' communication capability. • Review emerging technologies for their potential to enhance the performance and resilience of communication systems. • Continue work to develop alternative PNT capabilities and secure, effective terrestrial-based communications systems to mitigate the risk of denial of space-based communications and PNT information.

Summary – developing networked command and control

Section 3 – Developing adaptable command and control

Key components of a command and control framework

4.13. Defence should establish a framework to guide their C2 approach. It must drive a dynamic and cyclical process, continuously tuned by changes to the operating environment and the degree of integration required with partners. Key components of an effective framework should include the following.

a. A clear sense-making capability, underpinned by a common digital foundation that provides coherent understanding to all partners. Use of artificial intelligence should be incorporated to assist analysing large data sets.

b. Diagnosis (sense-making) of information at the appropriate levels (command nodes to global headquarters) with the intent of maximising situational awareness. Collaboration with the C2 enterprise may be necessary to reach into pools of information, understanding and awareness beyond Defence. Use of artificial intelligence should be incorporated to enhance understanding and support decision-making. Outputs from the sense-making and diagnosis functions must inform a characterisation of the operational environment and determine the necessary degree of integration with partners. The framework should clearly establish the C2 approach that will be most effective both in terms of interaction with partners and the way activities should be prosecuted.

c. Informed by the C2 approach, Defence's C2 capability should allocate and control resources to activities that will create effects (or amplify the effects of partner organisations). This is not a binary step and may require a complex mix of activities and C2 approaches, supported by dynamic communication across an integrated force. Use of artificial intelligence should be incorporated to support operational planning and human-in-the-loop decision-making.

d. A feedback loop that can monitor the impact of effects and integrate lessons learned to adjust the C2 approach or the planned effects as necessary. Constant tuning of the cyclical process should be driven by updated situational awareness, diagnosis and refining activities informed by the most effective C2 approach.

Tuning the command and control approach

4.14. Defence should adopt NATO's recommended approaches for the required degree of integration with partners; this is detailed in Chapter 1, Table 1.1. David Snowdon's Cynefin framework has led to the following recommended approaches for differing levels of complexity in the operating environment.[37]

a. **For clear situations: sense–categorise–respond.** The decision-maker should respond when they have collected enough data and have sufficient expertise to apply standardised responses (developed as best practices).

b. **For complicated situations: sense–analyse–respond.** Initially it is not obvious what is happening. The decision-maker should aim to establish sufficient understanding to be able to devise appropriate responses. Frequent redesign of ways of thinking, planning and acting may be required.

c. **For complex situations: probe–sense–respond.** The environment is characterised by surprising and unpredictable change, ambiguity and non-linearity. As the system responds to probes, desirable results are amplified and undesirable outcomes are dampened. An iterative approach is needed, taking steps to influence the potentially favourable trends and relationships. There is no acknowledged best practice; where possible, iterations should be 'safe to fail',[38] founded in innovation, learning and adaptation. This is at odds to the approach for clear and complicated situations in that pursuing a level of confidence in initial decisions and choice of actions is not sensible due to high levels of uncertainty.

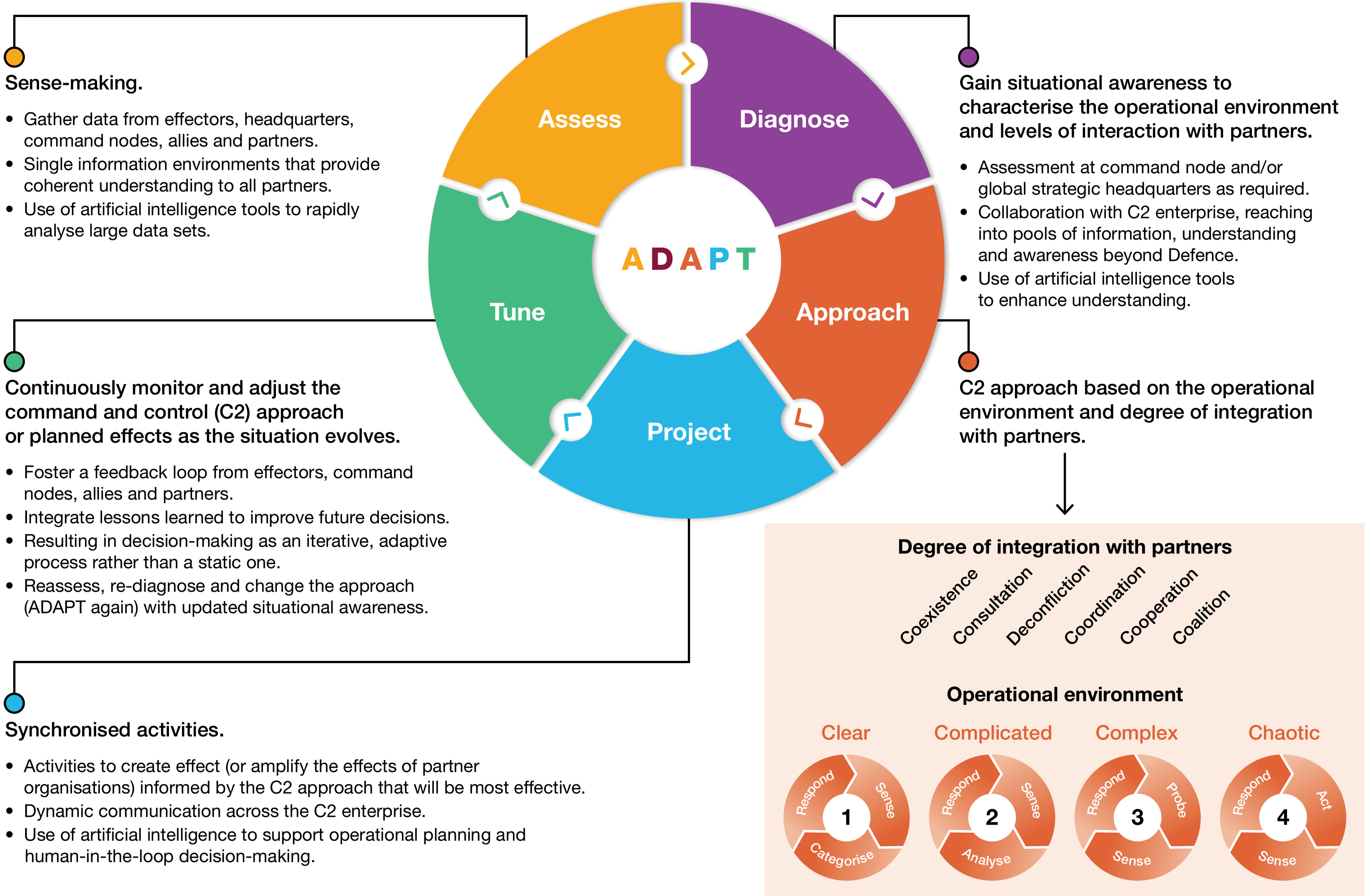
d. **For chaotic situations: act–sense–respond.** The environment is inherently unstable, variables are decoupled negating any clear feedback loops, and the outcome of actions are unknowable. There is little point in deliberating, particularly as delaying a decision, or failing to decide at all, may produce negative outcomes. Novel practice is likely to be a hybrid combination of best/good/emergent practice.

[37] The Cynefin framework is a conceptual framework used to aid decision-making.
[38] 'Safe to fail' does not mean totally 'safe', but 'safe within the organisational tolerance for uncertainty and failure'. This is of particular relevance in the context of military operations.

Proposed framework to guide the command and control approach

4.15. Existing C2 frameworks embody the cycle of observation, orientation, decision and action (OODA). This leads to a C2 approach broadly suited to clear and complicated situations. Responses are generally developed through plans that assume predictable cause and effect, and decision-makers default to established good practice. In a chaotic situation where there is no obvious relationship between actions taken and what may happen, the response becomes more instinctive. For example, under some warfighting conditions, there is little time to generate a sophisticated approach, leading to decisive actions that address the most pressing issues and sense the outputs.

4.16. An updated framework is necessary to meet the demands of an integrated force and the operating environment. This concept proposes an example framework based on assess, diagnose, approach, project and tune (ADAPT) functions. This places greater emphasis on how activities should be prosecuted and the feedback loops that are important for mitigating complexity via ‘probe–sense–respond’. The model has been designed around adaptability but also incorporates the other required C2 attributes – integrated, networked and artificial intelligence-enabled. The ADAPT model, shown in Figure 4.1, is proposed as a starting point; further work is required to refine a framework to guide the C2 approach. Once an effective framework has been established, it must be underpinned through education and training.



Sense-making.

- Gather data from effectors, headquarters, command nodes, allies and partners.
- Single information environments that provide coherent understanding to all partners.
- Use of artificial intelligence tools to rapidly analyse large data sets.

Gain situational awareness to characterise the operational environment and levels of interaction with partners.

- Assessment at command node and/or global strategic headquarters as required.
- Collaboration with C2 enterprise, reaching into pools of information, understanding and awareness beyond Defence.
- Use of artificial intelligence tools to enhance understanding.

C2 approach based on the operational environment and degree of integration with partners.

Continuously monitor and adjust the command and control (C2) approach or planned effects as the situation evolves.

- Foster a feedback loop from effectors, command nodes, allies and partners.
- Integrate lessons learned to improve future decisions.
- Resulting in decision-making as an iterative, adaptive process rather than a static one.
- Reassess, re-diagnose and change the approach (ADAPT again) with updated situational awareness.

Synchronised activities.

- Activities to create effect (or amplify the effects of partner organisations) informed by the C2 approach that will be most effective.
- Dynamic communication across the C2 enterprise.
- Use of artificial intelligence to support operational planning and human-in-the-loop decision-making.

Figure 4.1 – Proposed ‘adapt’ command and control operating model

People who are adaptable and can work amidst complexity

4.17. Defence should develop intuitive and experienced people who are proficient in a range of approaches to commanding and controlling. People will continue to need intellectual agility, personal robustness and operational experience, but Defence should encourage greater innovation and less constricted thinking. There is synergy with this concept's proposals for 'new ways of operating' (see paragraph 4.3) to develop the necessary people requirements though specialist C2 skills and professional training. Training in challenging situations where no 'right answer' exists will forge the ability of C2 staff to handle uncertainty and comprehend complex situations rather than conforming to a process. Training should encompass the abilities and approaches of partner organisations and the technologies and information tools embedded in C2 systems.

4.18. New styles of leadership should be developed to encourage a culture of adaptation. Greater emphasis should be placed on new ideas and collaboration, both essential to effective performance in a complex operating environment. Defence should move away from behaviours that are inward-looking and only support the continuous feeding of information to a commander, creating single points of failure and risking cognitive overload through excessive decision-making demands. Leaders should increasingly enable, empower and catalyse their staff rather than directing. Just as a joint commander today understands the abilities, effects and limitations of the military system, in the future they should study and build experience of the critical new tools of their C2 trade, which includes critical relationships with partners across government, NATO and non-military entities. Defence should ensure future leaders are equipped with the attributes and skills to shape the focus and activities of the diverse range of organisations across the C2 enterprise.

	Enabling functions	Concept proposals for Defence
Command and control must be adaptable	A framework to guide the right C2 approach depending on complexity of the environment and the degree of integration with partners	• Adopt NATO's recommended approaches for the required degree of integration with partners. • The assess, diagnose, approach, project and tune (ADAPT) framework is proposed as an example to guide the C2 approach and embed the feedback loops necessary to mitigate complexity. • Once an effective framework has been established, it must be underpinned through education and training.
	People who are adaptable and can work amidst complexity	• Encourage greater innovation and less constricted thinking. • Develop the necessary people requirements through specialist C2 skills and professional training. • Training needs to prepare people for challenging situations where no 'right answer' exists, and to understand the abilities and approaches of partner organisations as well as the technologies and information tools embedded in C2 systems. • Develop new styles of leadership to encourage a culture of adaptation. • Ensure future leaders are equipped with the attributes and skills to shape the focus and activities of the diverse range of organisations across the C2 enterprise.

Summary – developing adaptable command and control

Section 4 – Developing artificial intelligence-enabled command and control

Artificial intelligence tools that support human decision-making

4.19. Artificial intelligence and machine learning provide new opportunities to enhance our C2 capability, such as enhanced sense-making, faster decision-making, critiquing and stimulating alternative views, or spotting flaws in planning assumptions and logic. With big data[39] being a by-product of both an expanded engagement space and a proliferation of sensors, the ability to make better sense of complexity in the operating environment and discover the insights potentially embedded in such large data sets will surpass human cognitive capabilities. Artificial intelligence, supported by machine learning approaches, such as deep learning and neural networks, can help C2 staff rapidly analyse vast amounts of information and extract valuable insights. Whilst the complexity in the environment cannot be wholly addressed by using such technology, it provides an opportunity to reduce the scale of the challenge, as long as it is designed to work effectively with new ways of thinking about, and operating in, complexity. A primary challenge is determining how to team these technologies effectively with humans so that our overall C2 capability is enhanced. Three examples of teaming artificial intelligence technology with humans to enhance C2 capability are proposed. They have been developed from research suggesting that such artificial intelligence elements could be plausibly created.[40] This is clearly not an exhaustive list; other applications for the use of artificial intelligence technologies will be developed alongside the technology and/or to address specific issues. The challenge is to provide C2 staff with the tools required to understand and assess comprehensively, and decide effectively, in the operating environment. The three examples are described below.

a. **Enhanced understanding.** The use of artificial intelligence and machine learning can help enhance our understanding of stakeholders,

[39] Big data refers to extremely large data sets that are complex and difficult to process using traditional data processing tools. Big data is a by-product of technological change that results in a greater volume of data being generated, at greater speeds and across an increasing number of sources.

[40] As reported in the 'Machine Speed Command and Control Project', undertaken by the Defence Science and Technology Laboratory to demonstrate artificial intelligence transformative potential within operational-level C2.

their perceptions, intentions and likely behaviours in operational settings. The technologies are effective at analysing complex data gathered from cultural factors, observed behaviours, relationships with other stakeholders and in the context of a specific issue within an environment or a system. Artificial intelligence 'agents' could provide a visualisation of stakeholders relevant to a critical issue and a well-informed assessment of how they might respond. Currently such assessments are very subjective and based on limited (by human cognition) awareness and understanding.

b. **Operational design.** The use of artificial intelligence and machine learning to help generate decisive conditions for attaining an operational end state. Working within defined parameters, these technologies would fuse mission aims with processes, planning assumptions and intelligence data (capabilities, centres of gravity and operating environment). Artificial intelligence agents could output descriptions and representations of potential decisive conditions that could help attain an operational end state. Current non-artificial intelligence-based mission planning places significant demands on human resources and cannot match machine speed nor the number of planning factors considered.

c. **Argumentation.** Embedding artificial intelligence and machine learning into C2 systems to track decisions and actions, and provide a record of rationale and logic flow. Given that much activity during planning at the operational level is dependent on conversations, development of effective speech to text capabilities will be key. Once this capability is available, argumentation engines have the potential to detect inconsistencies in manual (human-based) reasoning, provide representations of hypothesis and help create visualisations of decision trees. They could also be used to provide real time feedback to ongoing conversations in the form of charts and dialogue interjections. Their outputs could highlight legislation, policy and regulation relevant to a hypothesis whilst also providing quick access to potentially relevant information.

4.20. To support human-machine teaming, new processes must be developed that fuse machine outputs effectively with human planning and decision-making. These must support accurate and timely inputs to artificial intelligence agents and ensure outputs can be tailored to the users' needs. It will be possible for some C2 activities to be replaced through the use of algorithmic-based approaches. Aligned with this, artificial intelligence, especially when machine learning-based, can similarly be used to largely replace human effort with that of the machine. Defence should review the potential for algorithm-based approaches and artificial intelligence to automate activities that will reduce the workload of C2 staff. However, the overarching aim is to establish an architecture where human cognition is enhanced by artificial intelligence agents whilst ensuring a person maintains overall control and accountability.

Legal and policy frameworks

4.21. The legal and policy frameworks covering the use of automation, artificial intelligence, machine learning and human-machine teaming are developing rapidly. The driving force is mostly commercial adopters; for example, Amazon who have now received Federal Aviation Authority to operate drones beyond visual line of sight. Defence must be proactive in monitoring and, where appropriate, shaping ongoing work to create new rules for emerging technology. It will be important to steer the development of international agreements so that they disincentivise potential adversaries from weaponising readily available technologies in an unethical manner. Defence must also identify and leverage synergies with commercial technologies that underpin approvals for using artificial intelligence or automation (such as Amazon's onboard detect-and-avoid system). Sole use of autonomous systems for military decision-making is an unlikely (and unwanted) legal outcome. Work to develop legal and policy frameworks should remain focused on the opportunities available from human-machine teaming.

	Enabling functions	Concept proposals for Defence
Command and control must be artificial intelligence-enabled	Artificial intelligence tools that support human decision-making	• Provide C2 staff with the tools required to 'understand and assess' fully, and 'decide effectively' in the operating environment. Three examples proposed are described below. o **Enhanced understanding.** The use of artificial intelligence and machine learning can help enhance our understanding of stakeholders, their perceptions, intentions and likely behaviours in operational settings. o **Operational design.** The use of artificial intelligence and machine learning to generate decisive conditions for attaining an operational end state. o **Argumentation.** Embedding artificial intelligence and machine learning into C2 systems to automatically track decisions and actions, and provide a record of rationale and logic flow. Their outputs could highlight legislation, policy and regulation relevant to a hypothesis whilst also enabling quick access to relevant information. • New processes must be developed that fuse machine outputs effectively with human planning and decision-making, with the overarching aim of enhancing human cognition. • Review the potential for algorithm-based approaches and artificial intelligence to automate activities that will reduce the workload of C2 staff. • Establish an architecture where human cognition is enhanced by artificial intelligence agents whilst ensuring a person maintains overall control and accountability.
	Legal and policy frameworks	• Be proactive in monitoring and, where appropriate, shaping ongoing work to create new rules for emerging technology. • Identify and leverage synergies with commercial technologies that underpin approvals for using artificial intelligence or automation.

Summary – developing artificial intelligence-enabled command and control

Section 5 – Developing resilient command and control

Assessing required command and control resilience

4.22. To determine the C2 resilience necessary, processes must be developed to assess potential threats against the tolerance to risk for a given task. Table 4.1 provides a list of potential threats related to C2 vulnerabilities that should be assessed as a minimum. This process should be embedded into central planning processes, with the aim of delivering conditions-based C2 resilience for all scenarios.

Command and control vulnerabilities	Examples of potential threats
People	• Adversaries will target communication and information systems used for decision-making and delegating authority, aiming to isolate people and create uncertainty.
Infrastructure	• Adversaries will employ advanced electronic surveillance methods to search for command posts, making them vulnerable to lethal attack.
Information	• Adversaries will seek to access confidential information via our communication and information systems. • Adversaries will seek to compromise information integrity (for example, by spoofing global positioning systems). • Adversaries will seek to limit information availability. Denial of service attacks can be levied by electromagnetic, cyber or lethal assets.

Table 4.1 – Potential threats to command and control components

Mitigating threats

4.23. The trend towards larger deployed headquarters must be reversed. Instead, Defence should aspire to smaller, more mobile and/or dispersed headquarters whilst placing greater emphasis on force protection and survivability. As a minimum, camouflage, hardening, security and deception should be reviewed for the specific purposes of protecting deployed C2 nodes.

Resilience must also be considered for larger, more permanent and static headquarters, including those based in the UK homeland. Defence should establish plans to rapidly disperse fixed strategic and operational headquarters to counter threats such as long-range lethal strike, terrorist attacks, proxy warfare, and cyber and electromagnetic activities. These plans should be tested through regular exercises and enhanced through lesson-based opportunities for improvement.

4.24. Defence should establish a network of redundancies and reversionary modes in C2 systems to minimise vulnerability and overload. Where possible, technical systems should support users in identifying threat activity and degradation. C2 organisations and their supporting systems should establish a variety of ways of operating and ensure alternatives are available to avoid single points of failure for communications and data sharing.

4.25. The need (and ability) to transmit ever increasing volumes of data comes with a dependency on space-based assets and fixed ground networks. The vulnerabilities of these systems are acknowledged. Defence should develop C2 operating modes that are not dependent on mass data transfer or ones that can operate on intermittent (and thus limited) data transfer. Transition to alternative, more resilient operating modes should be practiced regularly through exercises to provide assurance that both the human and machine components of C2 can function effectively with limited access to information and degraded communications.

	Enabling functions	Concept proposals for Defence
Command and control must be resilient	Assessing required C2 resilience	• Develop processes to assess potential threats against the tolerance to risk for a given task and embed into central planning process with the aim of delivering conditions-based C2 resilience for all scenarios.
	Mitigating threats	• Aspire to smaller, more mobile and/or dispersed headquarters whilst placing greater emphasis on force protection and survivability. • Establish plans to rapidly disperse fixed strategic and operational headquarters, including those based in the UK homeland. • Defence should establish a network of redundancies and reversionary modes in C2 systems to minimise vulnerability and overload. • C2 organisations and their supporting systems should establish a variety of ways of operating and ensure alternatives are available to avoid single points of failure for communications and data sharing. • Develop C2 operating modes that are not dependent on mass data transfer or can operate on intermittent (and thus limited) data transfer.

Summary – developing resilient command and control

Chapter 5

Further work

5.1. Adopting the concept proposals detailed in Chapter 4 will help develop a command and control (C2) capability that will support an integrated force to enhance operational effectiveness and achieve competitive advantage. It will also fulfil the purpose of this concept, which is to inform C2 developments, promote alignment of C2 capabilities within Defence and avoid disjointed solutions.

5.2. As noted in the scope of this concept, further work is required to develop the ideas alongside other C2 projects within Defence. Post publication, the aim is to widen engagement on C2, understand ongoing C2 development activities and cohere ideas. A concept implementation plan will be developed through engagement with the community of interest. The plan will support the implementation of the ideas proposed in this concept and then refine them via a wider review.

5.3. Further work is also required to develop some of the themes in this concept and to conceptualise C2 beyond 2030. This will include a supplementary paper to provide greater detail on research and academic thinking that supports this joint capability concept note and ‘future C2’. Other potential subjects for further work are detailed at Table 5.1 (noting the list is subject to change and there is no commitment to any of these proposals at this stage).

© Vasin Lee / Shutterstock.com

Topic	Brief description of the question/challenge
Conceptualise C2 for specific Defence tasks	This work is needed to assess the C2 requirements for key Defence functions, such as targeting, kill webs and integrated air defence. It would identify further developments to C2 (new developments and ones that enhance the proposals in this concept).
Developing the C2 approach in complex environments	How can we exploit both the latest knowledge from academia and the practical experience from organisations facing similar challenges to develop the approach to C2 in complex environments?
Review C2 requirements for multi-domain operations	What are feasible ways of working collaboratively with North Atlantic Treaty Organization Allies and what are the implications for developing C2?
Review C2 requirements for integrating with partners across government and non-military entities	What are feasible ways of working collaboratively with multiple and diverse partners and what are the implications for developing C2?
Examine feasibility of emergent teaming as a new C2 organising approach	Does dynamic organising, based on emergent teaming, offer potential to support C2 for an integrated force? If so, what are the options and how might they be explored, tested, validated and enabled?
Explore new leadership challenges associated with multi-domain, multi-partner C2 enterprises	What should leadership be like, and how should it be practiced, to be effective in the new broader C2 enterprise and multi-domain operations?
Transitioning C2	How can we implement substantial positive change in C2 that is aligned with the aspirations set out in this joint capability concept note?
Designing for emergence	How to design, shape and influence the components of C2 capability so that it reinforces the desired adaptability to respond to changing operational environments.

Table 5.1 – Potential subjects for further work

Lexicon

Acronyms and abbreviations

5G	fifth generation
ADAPT	assess, diagnose, approach, project and tune
AJP	Allied joint publication
C2	command and control
IMD	intelligence mission data
JCCN	joint capability concept note
JCN	joint concept note
JDP	joint doctrine publication
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
OODA	observation, orientation, decision and action
PESTLE-M	political, economic, social, technological, legal, environmental and military
PNT	positioning, navigation and timing

Notes

Corporate member of
Plain English Campaign
Committed to clearer
communication
235

Published by the Ministry of Defence