Ministry of Defence

The North Atlantic Treaty Organization's concept of multi-domain operations has been adopted by the UK.
As a result, Joint Concept Note 1/20, Multi-Domain Integration has been archived.

Joint Concept Note 1/20

Multi-Domain Integration

Joint Concept Note 1/20

Multi-Domain Integration

Joint Concept Note (JCN) 1/20, dated November 2020, is promulgated as directed by the Chiefs of Staff

Director Development, Concepts and Doctrine Centre

Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing strategic trends, joint concepts and doctrine. 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. Please contact us via:

Email: DCDC-DocEds@mod.gov.uk Telephone: 01793 31 4216/4220

Copyright

Distribution

All DCDC publications, including a biannual DCDC Publications Disk, can be demanded from the LCSLS Headquarters and Operations Centre.
LCSLS Help Desk: 01869 256197 Military Network: 94240 2197

Our publications are available to view and download on defnet (RLI) at:
https://modgovuk.sharepoint.com/sites/defnet/JFC/Pages/dcdc.aspx

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

Foreword

The Information Age has been upon us for some time but we, in UK Defence, remain configured for joint operations more suited to an era of industrial warfare. Our adversaries have developed counter strategies from studying the Western way of warfare. They engage in a continuous struggle using cyber and information combined with all other instruments of statecraft – 'political warfare' – with the goal of winning without fighting. This has stretched our understanding of the definition of warfare well beyond the narrow boundaries within which our traditional approach can hope to succeed.

Our response is to pursue integration – as joint is no longer enough. This is not simply a case of making Defence a little more connected by incorporating activity in the space and the cyber and electromagnetic domains – it is far more significant. To better compete with our adversaries in this era of persistent competition we must be able to operate and war fight in a way that generates advantage through being better integrated across three levels of warfare and all five operational domains: maritime, land, air, space, and cyber and electromagnetic. This multi-domain integration (MDI) will change the way we operate and war fight, and the way we develop our capability. Effective integration of the domains will achieve a multi-domain effect that adds up to far more than simply the sum of the parts. This integrated force must also be fused across government and interoperable with principal allies.

Integrating by instinct and by design will allow us to draw on as many effective capabilities as possible, including non-military, to apply combinations the adversary doesn't expect or cannot guard against. We must inculcate an instinctive inclination to survey all the domains and intervene where we choose in pursuance of our given objectives.

There is no fixed route to a known MDI destination, so this concept provides a headmark to allow us to explore and develop our MDI ambition. In so doing, we will have to take risk, accept some failure and place emphasis on experimentation, training and operations to stimulate

innovation in all lines of development. We will adopt an iterative approach, moving quickly where possible, and learning by doing.

VCDS

Preface

Purpose

1. The principal purpose of Joint Concept Note (JCN) 1/20, *Multi-Domain Integration* is to provide the UK interpretation of multi-domain integration (MDI). It is an exploratory concept that offers an ambitious vision for maintaining advantage in an era of persistent competition. However, it is not possible with current means and the journey towards realising the vision, which we have already started, needs to be tested. This JCN therefore informs the Defence Experimentation Pathway and should undergo formal review within 12 months of being published. This allows the evidence base to be considered and an iterative conceptual approach towards MDI to be developed.

Context

2. This concept is founded on the *Integrated Operating Concept 2025*. It focuses on how to integrate across the domains and levels of warfare and provides a vision for the development of an integrated force out to 2030 and beyond. It does so in the context of integration with partners across government, the private sector and allies. Being integrated across all five domains – maritime, land, air, space, and cyber and electromagnetic – and at every level of warfare will change the way we fight and the way we develop capability. We are moving beyond 'joint' to an era when modern manoeuvre in any domain will be enabled by effects from all domains. This integrated force must also be integrated nationally and with our key allies and partners.

Aim

3. This concept has four specific aims. These are to:

- define the UK interpretation for applying MDI beyond the current force to deliver advantage over our adversaries out to 2030 and beyond;

- outline how Defence can achieve integration across the domains and levels of warfare in the context of integration with allies, partners across government and the private sector;

- present the policy question of our level of ambition for MDI; and

- provide a catalyst for Defence experimentation across concept, capability and warfare development.

Structure

4. JCN 1/20 is divided into four chapters and one annex.

a. **Chapter 1 – Responding to the challenge.** Chapter 1 examines the problem presented by our adversaries and proposes a response constructed around MDI.

b. **Chapter 2 – Domains and environments.** Chapter 2 re-conceptualises our understanding of the domains and environments in the context of MDI.

c. **Chapter 3 – The core tenets.** Chapter 3 introduces, expands and explains the four core tenets of MDI: information advantage, strategically postured, configured for the environments and creating and exploiting synergy.

d. **Chapter 4 – Force development implications.** Chapter 4 considers the implications of developing MDI through the prism of the joint functions, offering insights to how command and control, intelligence, fires, manoeuvre, outreach, information, support and resilience interplay in achieving MDI. It examines risks including the balance between ambition and vulnerabilities.

e. **Annex A.** Annex A suggests how specialisations within Defence can evolve to meet the orchestration element of MDI.

Assumptions

5. This JCN is based on the following assumptions.

a. MDI applies across the operate and war fight spectrum of the *Integrated Operating Concept 2025*.

b. Russia is our primary adversary and pacing threat. Albeit in an era of persistent competition we face an array of state and non-state threats.

c. The UK will be allied by design and the North Atlantic Treaty Organization (NATO) remains central to the pursuit of our strategic ends.

d. Partners across government are amenable to integrating in the way proposed. This is a critical assumption without which MDI will not be achievable.

e. Interoperability with the United States is achievable.

f. Experimentation and testing of the ideas in this concept are essential. We must iterate our way forward through evidence and judgement.

Audience

6. This JCN seeks to inform a wide audience. It is primarily orientated towards developing the idea of integration within Defence but acknowledges it relies on the will of the Whole Force,[1] partners across government, private sector and multinational elements. It is therefore intended to be circulated widely but will need to be complemented by a bespoke primer for non-Defence readers.

1 The use of the term Whole Force in this publication refers to regular and reserve military personnel, civil servants and industrial elements that are part of the Defence-wide military capability.

Linkages

7. JCN 1/20 is underpinned by a number of publications and key documents that provide key linkages, greater detail and broader context to this publication. These include:

- Joint Doctrine Publication 0-01, *UK Defence Doctrine*, 6th Edition;[2]
- Joint Doctrine Note X/21, *Integrated Action*;[3]
- *Integrated Operating Concept 2025*;
- JCN 1/17, *Future Force Concept*;
- JCN 2/17, *Future of Command and Control*;
- JCN 1/18, *Human-Machine Teaming*;
- JCN 2/18, *Information Advantage*;
- JCN X/21, *Future Electromagnetic Activities*;[4]
- *Global Strategic Trends – The Future Starts Today*; and
- *Five Eyes Future Operating Environment 2040*.

2 Joint Doctrine Publication 0-01, *UK Defence Doctrine*, 6th Edition is due to publish in 2021.
3 Joint Doctrine Note X/21, *Integrated Action* is due to publish in 2021.
4 Joint Concept Note X/21, *Future Electromagnetic Activities* is due to publish in 2021.

Contents

Chapter 1

Chapter 1 examines the problem presented by our adversaries and proposes a response constructed around MDI.

> But we cannot rest on our laurels. We must **do more to adapt**. We will be judged by **how we respond** to the opportunities ahead.
>
> Prime Minister Boris Johnson
> Launching the Integrated Review
> February 2020

Chapter 1

Responding to the challenge

Multi-domain integration is the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare.

1.1. This chapter describes the threat we face from adversaries and the challenges and opportunities afforded by technological advancement. It considers how our allies are answering these challenges and concludes by proposing that multi-domain integration (MDI) is part of the UK response to being 'integrated for advantage'.

Section 1 – The threat

1.2. **Adversary threat in general.** The UK faces threats from resurgent and developing powers, state and non-state actors, and violent extremism. A strategy of 'political warfare' is being used by our pacing threat (Russia), which is designed to undermine our cohesion, erode economic, political and social resilience, and challenge our strategic position in key regions of the world. The strategy does not distinguish between peace and war; for them the landscape is characterised by a continuous struggle involving all the instruments of statecraft. Their goal is to achieve their objectives below what we call war. Our deterrence, in combination with allies, is not symmetrical with this way and is only partly effective against it.

1.3. **Adversary systems thinking.** The Western way of war in recent decades has been observed and studied by our main adversaries. They have concluded there is a need to counter advanced opponents by exploiting vulnerabilities in information and communications systems. Russia, China, Iran and the Democratic People's Republic of Korea (DPRK) all emphasise superiority in information as critical to success. They use it to deceive, confuse, disrupt, divide, influence and ultimately

defeat an adversary with superior conventional forces. Systems thinking[5] is very prominent in adversary designs. It aims to exploit vulnerabilities in the interdependent systems of their opponents to minimise their technical advantage; in effect, to attack our cohesion.

1.4. **Adversary multi-domain capability.** Neither Russian, Chinese, Iranian nor the DPRK doctrine contains explicit multi-domain references. But, their absence in written theory does not mean an absence of multi-domain thinking and practice. It is possible to infer a multi-domain practice, particularly with Russia and China, from these nations' actions and force structures. Russian and Chinese military thinking acknowledges the value of non-military measures for creating a desired effect in support of military plans. In the Russian case, this is reflected in departments and agencies falling within the defence establishment, including organisations responsible for humanitarian aid and exploiting broader civilian business activity overseas. So, while our principal adversaries do not have direct multi-domain equivalent concepts, they are already interoperating military and non-military capabilities and operating with freedom across the domains both home and away.

The National Defense Management Center of the Russian Federation coordinates the activities of all ministries in the interests of ensuring the defence of, and security of, the state

© ppl / Shutterstock.com

5 Russia employs an approach, known as 'new-type war', that posits the adversary as a system with key sub-systems or nodes, and looks to create strategic effects by simultaneously targeting key military, supporting or decision-making functions. China's theory of victory is centred on systems confrontation and systems attack. This is characterised by the use of integrated kinetic and non-kinetic operations while degrading the adversary's communication and information systems, ultimately eroding their will to fight.

Russian multi-sphere operations

In August 2020, Russia conducted an exercise in its Central Military District that gave insight into its version of MDI. The exercise was a test of command and control in forming flexible force groupings to repel a global strike from an adversary through a multi-sphere operation (mnogosfernoy operatsii), as reported in an article in the Voyenno Promyshlennyy Kuryer (Military Industrial Courier) on 25 August 2020. The exercise involved motorised, armoured, air, unmanned aerial vehicle, air defence, missile, chemical, biological, radiological and nuclear (CBRN) and electronic warfare force elements working in support of each other in a defensive action, particularly testing command and control arrangements. According to the Russian journal, electronic warfare penetrated deep into enemy air defence systems and physical targets including enemy command and control systems. This exercise underlines that Russia can use an effective range of capabilities across multiple domains at the tactical level, noting that such a capability will be employed as part of a wider spectrum of non-military measures.

'Russian Armed Forces Test Multi-Domain Operations'[5]
Roger McDermott

1.5. **Sub-threshold challenge.** Sophisticated operations that target systems can be combined with more conventional military operations such as proxies, coercion, offensive cyber and lawfare. The result is a way in war that leads to objectives being achieved without the need to escalate above the threshold of armed conflict. Additionally, they are executed in such a way that would disrupt our systems in the early stages of any conflict; thereby turning 'shaping' operations into 'decisive' ones. The experience gained in exploiting cyber, electromagnetic and information technologies in recent conflicts has provided Russia and China with these obvious start points, as well as a head start for any potential future conflict with the UK.

6 McDermott, R, 'Russian Armed Forces Test Multi-Domain Operations', *Eurasia Daily Monitor,* 9 September 2020.

1.6. **Differing problem sets.** In developing a multi-domain approach, there is a need to consider the geostrategic differences in relation to our adversaries. Russia is a land power and is weighted in that domain. In competition and armed conflict with Russia, the large continental land mass affects the MDI requirement as does the North Atlantic Treaty Organization's (NATO) considerable geostrategic land depth to Russia's west. In contrast, a confrontation with China is likely to be centred on the air and maritime domains, emphasised by new capabilities on the island chains and the relative lack of Western strategic depth. Thus, there are choices about our multi-domain composition depending on who we expect to compete alongside and against.

Section 2 – Technological developments

1.7. **New technological possibilities.** The pace of technological advancement has been, and remains, a driver for change. New technologies that combine processing power, connectivity, automation, quantum computing, machine learning and artificial intelligence will allow not just a new generation of weapons systems but new ways in war. It will allow the processing and analysis of large amounts of data, together with the generation of a near complete picture of the environment and activity within each domain, at all levels of warfare. It will become harder to hide significant military signatures anywhere on the globe. A mix of manned, unmanned and autonomous systems will bring a further change in lethality and agility whilst hypersonics, layered systems of ballistic and long-range missiles and counter-space capabilities will continue to extend the competitive space.

1.8. **Precision effects.** The passing of the Industrial Age of warfare has brought a shift of emphasis in which static concentrations of fielded forces are more vulnerable in light of the increased range and accuracy of modern weapons and sensors. The domains of space, and cyber and electromagnetic, although mostly unseen, are already part of the competitive battlespace; more of the contest is virtual and involves information. Well-connected, and continually evolving, systems and networks will therefore be the key enablers in delivering precision, timing and especially targeted audience effect.

1.9. **Blurred boundaries.** The range and speed of these new munitions and non-munitions 'fires' combined with improvements in detection through visual, electromagnetic, acoustic and other signatures means the traditional boundaries between land, maritime and air forces have become blurred or non-existent. For example, it might be possible in some cases to achieve sea denial of a maritime environment through land-based long-range systems; the same could apply in reverse. In such scenarios, single Services may be primarily focused on creating integrated effects in other domains.

1.10. **Time compression.** The expanded battlespace amplifies the importance of timing because geography is less limiting. Whereas troops in close contact battles will typically have the same immediate time horizons as before, there is likely to be less time at the higher levels than there used to be. This will require re-evaluation of those traditional rhythms of military activity used for planning and executing operations; particularly when integrated with our partners across government and other actors. There is a requirement to be more dynamic, pre-emptive and, where necessary, selectively ambiguous.

Section 3 – Our allies

1.11. **United States.** The United States (US) Army published a multi-domain operations concept in December 2018.[7] It identified that its adversaries have developed lethal and non-lethal capabilities that have expanded the battlespace in time and physical space, particularly through enhanced anti-access and area denial (A2AD) systems. The US Army designed a response to contest adversary activity more effectively sub-threshold and to be better placed to cross into, and back from, armed conflict. Whilst these challenges are fully recognised within the context of the US Army, UK MDI is not a copy of the US Army concept. Taking account of the differences in scale and geostrategic ambition, this joint concept note (JCN) is closer to the US Joint Staff global integration idea which focuses on trans-regional, all domain, multifunctional integration.

7 United States Army Training and Doctrine Command Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*.

1.12. **North Atlantic Treaty Organization.** A NATO-led multi-domain concept is currently being developed, but the *NATO Warfighting Capstone Concept* recognises the same condition of persistent competition as the UK and also identifies the same main threats, which are global in nature. NATO's 'shape, contest, fight' framework reflects the need to contest on a daily basis and seeks to refocus towards a multi-domain approach.

Section 4 – Regaining advantage

1.13. The UK must respond to the actions of our adversaries and the new possibilities afforded by technology. More military formations, platforms and long-range systems than our adversaries cannot realistically be acquired. Instead, the UK should increase the range of capabilities that can be brought to bear beyond maritime, land and air force deployments, including non-military capabilities, and synchronise their employment for best overall impact.

1.14. **Relationship with the *Integrated Operating Concept 2025* and integrated action.** The *Integrated Operating Concept 2025* (IOpC 25) introduces the central idea of being integrated for advantage. This advantage comes from being integrated across government, integrated with allies and integrated across the domains and levels of warfare as illustrated in Figure 1.1. Integrated action is the newest tenet of UK capstone doctrine and addresses this integration challenge to ensure the military instrument delivers its contribution to national objectives. MDI, the focus of this JCN, will amplify and help to optimise integrated action. MDI and the integrated force developed must also be integrated nationally and with allies and partners.

Figure 1.1 – Integrated for advantage

1.15. **Fusion across government.** Everything Defence does should be in support of the overall national objectives and be integrated within the fusion doctrine framework of National Security Strategy Implementation Groups. Orchestration of military strategic effects (OMSE) describes how Defence delivers its outputs in support of these national objectives as either a supporting or supported actor to other departments of government. This JCN recognises these relationships and the need to work as a system with the instruments of national power; equally it recognises that Defence will not have full freedom of action across the domains. For example, offensive cyber is not under the exclusive control of Defence and activities in space will have immediate consequences for other departments. This adds layers to military judgement and mission command because the drivers for, and consequences of, MDI are extensive.

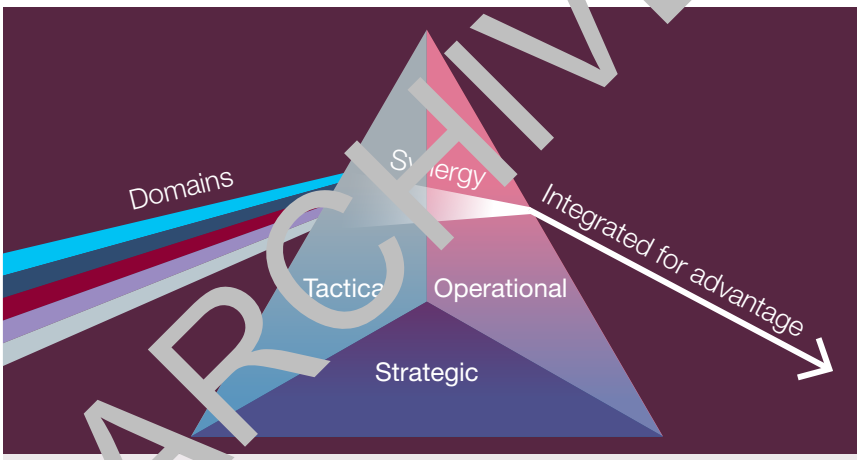
1.16. **Past experience.** The idea of integrating military with non-military capabilities is not new. The difference with MDI is that the integration applies in a domain context in which partners across government either wholly or partly control domain capabilities. In pursuing MDI beyond Defence, cultural differences, trust, information sharing, and organisational inertia should be anticipated. For a start, the idea of operational domains will be new to most people outside Defence. We will need to build institutional familiarity.

1.17. **Integrating across the levels of warfare.** As MDI must consider partners across government it means that MDI automatically spans the levels of warfare. Integrating across the levels however, does not mean trying to delete the levels, as each contributes to the control of capabilities at its disposal and manages the various time horizons. They also protect other levels of warfare from being overwhelmed and allow appropriate tempos to be determined. This means integration is about synchronising as much of the timing and tempo cycles as possible. For example, we will need to orchestrate strategically tasked space and offensive cyber assets working at the speed of light with physical tactical manoeuvre.

1.18. **Dependencies and deficiencies.** In considering how MDI can be achieved it is important to identify where we are now. The current system is already capable of a certain degree of MDI and programmes are underway such as the Information Advantage Change Campaign and the MDI Change Programme. Equally, Defence should identify deficiencies that are and will become critical to delivering MDI, examples being: seabed to space situational awareness, target audience analysis and an agile global support system. It is also necessary for Defence to address the deficiencies and dependencies beyond Defence, as these are part of the overall system. For example, in the space domain it will require Defence to consider how it interacts with the private sector over the control of space assets.

Defence will need to consider its dependencies with the private sector across the domains

1.19. **A response through multi-domain integration.** Our response to the threats, challenges and opportunities we face is to pursue integration; joint is no longer enough. MDI is more than being good at joint or simply adding space, and cyber and electromagnetic considerations. MDI is about designing and configuring the Whole Force for dynamic and continuous integration of all global capabilities together, inside and outside the theatre, munitions and non-munitions, above and below the threshold of armed conflict. The greatest effect will be from drawing in as many capabilities as possible to apply combinations the adversary does not expect or cannot guard against. Forcing the enemy to defend all domains all the time from all directions will impose multiple dilemmas and open up vulnerabilities. It is not just an offensive concept; the ideas and designs are as applicable in defence and in engaging for influence.



A representation of multi-domain integration

Key points

- Our principal adversaries are already operating in all the domains all the time. They will use the full spectrum of capabilities to undermine cohesion, erode economic, political and social resilience, and challenge our strategic position in key regions of the world.
- The potential of new technologies and the competitive arenas of the space, and cyber and electromagnetic domains are blurring the traditional boundaries between military forces, compressing time at the higher levels of command.
- The UK needs to increase the range of capabilities that can be brought to bear beyond maritime, land and air.
- This MDI concept proposes how to integrate the domains and levels of warfare but also recognises the vital importance of being integrated nationally and with allies and partners.
- MDI is about more than actions in one domain supporting another. It is about the synergy of capabilities and activities in and from multiple domains and levels of warfare.

Notes


ARCHIVED

Chapter 2

Chapter 2 re-conceptualises our understanding of the domains and environments in the context of MDI.

> I have a vision of UK Defence, where we're able to **join the dots** between space, air, surface and sub-surface, so that the sum of the parts means much more than the value of the individual parts, and where we can do this **in real time** at the time and place of our choosing.
>
> Ben Wallace
> Secretary of State for Defence
> July 2020

Chapter 2

Understanding domains and environments

Domains

2.1. To understand how multi-domain integration (MDI) can deliver advantage, there is first a need to consider what constitutes an operational domain.[8] This provides the basis for understanding how effects can be created by combining capabilities across the domains and significantly, how Defence can focus its activity alongside other actors to achieve objectives in the practical arenas – the environments.

2.2. **Relationship between the domains.** The operational domains are useful as a mental framework for planning. In particular, the use of domains serves to emphasise the importance of thinking laterally about the full range of capabilities that could be at one's disposal. While allies and adversaries generally recognise maritime, land, air and space, only the UK combines cyber and electromagnetic into one, as illustrated in Figure 2.1. Cyber and electromagnetic activities overlap and are inextricably linked, while cyberspace and the electromagnetic environment are where activities happen.

We must think laterally about capabilities available across the domains

© sdecoret / Shutterstock.com

8 Operational domains are defined as: discrete spheres of military activity within which operations are undertaken to achieve objectives in support of the mission. Joint Doctrine Publication 0-01.1, *UK Terminology Supplement to NATOTerm.*

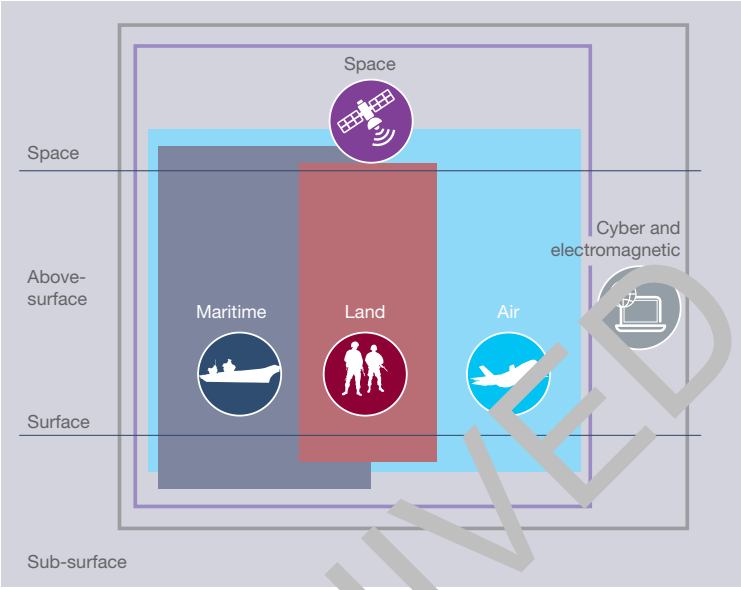


Figure 2.1 – Illustration of domains as described in UK doctrine

2.3. **Unequal domains.** The five operational domains are not equivalent or equal. There is a significant difference when considering the relationship of the space and the cyber and electromagnetic domains. Space is a constant in relation to the air, land and maritime domains because it, as well as being a domain in which discrete activity is also possible. The UK is reliant on space for critical services such as position, navigation and timing, and satellite communications. Therefore, activities in space, especially destructive actions, are almost certainly of strategic significance and involve high stakes in terms of deterrence. The cyber and electromagnetic domain is ubiquitous and pervades all other domains; in all cases some degree of freedom of action in the cyber and electromagnetic domain is indispensable. The space and the cyber and electromagnetic domains underpin MDI with its emphasis on systems and networks and links to information activities; they are critical enablers and effecters, yet they are the least understood domains in UK Defence.

2.4. **Moving on from domain seams.** The three traditional domains of maritime, land and air broadly map across to the single Services. However, boundaries are ambiguous and not clearly delineated. For example, army attack helicopters in the littoral operate in the maritime, land and air domains simultaneously; in the space domain, a ground station connects with satellites via the medium of the electromagnetic spectrum while rockets ascend through the air, but all are part of the space domain. Most of the domains interplay in the majority of real-world situations. Therefore, seams, inculcated into military thinking as vulnerable fissures, are less relevant because the domains overlap; for example, all are present in a coastal environment. Multi-domain thinking transcends seams; the most likely 'seams' to worry about in MDO are those among the instruments of national power, among allies and with the private sector.

2.5. **Using the domains.** The aim in MDO is not to use as many domains as possible when planning for effect; rather it is to create, find and exploit unprotected vulnerabilities by extending the range of activities and capabilities that can be brought to bear across the domains. Doing this presents too many combinations for the adversary to guard against. Multi-domain action is a way of doing this. For example, a naval surface combatant expects to defend itself from hostile aircraft or cruise missiles fired from the coast but will be less familiar with the threat from long-range land-based fires in combination with disruption to satellite navigation systems.

Environments

2.6. When it comes to executing military operations, activity actually takes place in environments. Environments provide the settings, or surroundings, for military activities and they exist prior to, during and after military activity. Each is unique and therefore has an influence on how different headquarters and formations conduct their activities. For example, operating in the Persian Gulf could include: force elements at sea in the restricted waters of the Strait; the island of Bahrain; air assets in Qatar; the sea lines of communication via Suez; the Mediterranean island of Cyprus; Gibraltar; and the UK home base. Each of these physical

places has different environmental characteristics and weather, different localised audiences, actors, adversaries and enemies (A3E) and particular ways of conveying information.

2.7. The detailed practical business of MDI therefore comes down to orchestrating activity in these environments. Advantage is most likely to be gained where an activity or capability is effected unexpectedly from the adversary's perspective and exploits a vulnerability. Activities across the domains and levels of warfare, integrated across government with allies and private sector elements is a way of creating these unexpected situations. This creates a direct physical, virtual or cognitive effect on A3E, or overwhelms the adversary by creating dilemmas, which weakens will and cohesion, thereby altering perceptions, beliefs and behaviours. This could be because it was effective in exploiting the specific conditions and vulnerabilities in the operating environment and/or because it comes from a domain that the adversary was not prepared for: MDI is manoeuvrist. Environments are central to the idea of MDI because it is where the domains interplay, where activity actually occurs and where outcomes are sought. Further explanation of the environments is covered in Chapter 3.

Each environment has different ways of conveying information, different audiences and different physical characteristics[9]

9 Image credits from left to right: iStock.com / peshkov, iStock.com / Hydromet and iStock.com / Alicia_Garcia.

Key points

- The 'traditional' domains of maritime, land and air broadly map across to the single Services, but boundaries are ambiguous and are not clearly delineated.
- The five operational domains are not equal: space is global and encompasses the air, land and maritime domains while the cyber and electromagnetic domain permeates and pervades all the others.
- The aim in MDI is not to use as many domains as possible; rather it is to create and find opportunities for exploitation, through extending the range of activities and capabilities that can be brought to bear.
- When it comes to the practical execution of activities and the realisation of effects, it is environments that should be the focus of integration and not domains.


ARCHIVED
$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$
$\int_0^{} 2x + 4\,dx = 3x^3 + x^2 + 4x + C \Big]_0^{} = 102$
$e^{x+iy} = e^x(\cos y + i \sin y)$

Chapter 3

Chapter 3 introduces, expands and explains the four core tenets of MDI: information advantage, strategically postured, configured for the environments, and creating and exploiting synergy.

> We have to move beyond 'jointery' – **integration is now needed at every level** – not just at the operational level where the term 'joint' applies.
>
> General Sir Nick Carter
> Chief of the Defence Staff
> December 2019

Chapter 3

The core tenets

Core tenets – an overview

3.1. This chapter explains the core tenets of multi-domain integration (MDI), as summarised below. The MDI model is shown in Figure 3.1.

a. **Information advantage.** Enabling and effecting orchestration through comprehensive and persistent sensing and understanding of environments and audiences, which must be common across government and with allies.

b. **Strategically postured.** The global, domain-centric arrangement of capabilities.

c. **Configured for the environments.** Readiness for multi-domain activity in operating areas and environments to influence the behaviour of selected audiences.

d. **Creating and exploiting synergy.** Generating, timing and exploiting windows of opportunity for relative advantage by creating synergy.

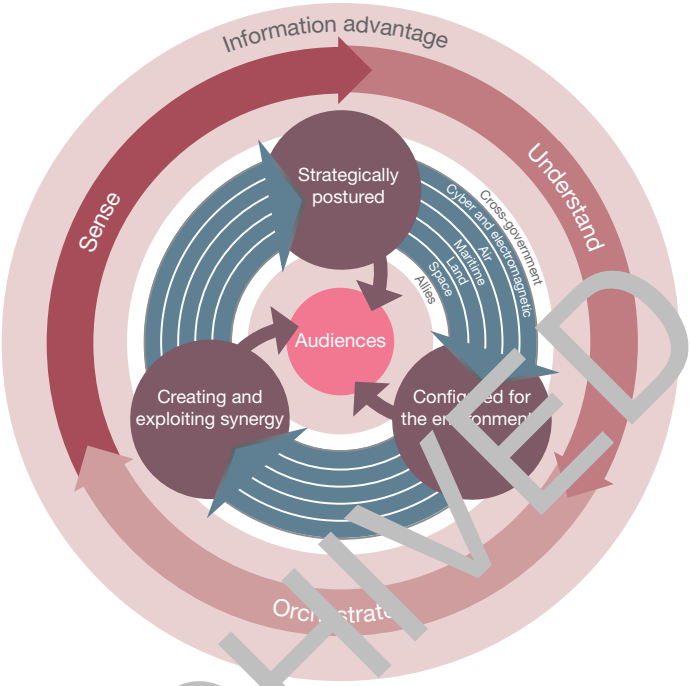


Figure 3.1 – The multi-domain integration model

Section 1 - Tenet 1: information advantage

Enabling and effecting orchestration through comprehensive and persistent sensing and understanding of environments and audiences, which must be common across government and with allies.

3.2. In an era of persistent competition, information advantage will anchor all our activities, from the tactical to the strategic. MDI involves a contest for information advantage. The side that gains the upper hand, both above and below the threshold of armed conflict, is the one that takes the most timely, well-targeted decisions and actions over time. Knowing what to do and when rests on the ability to sense and understand the whole set of influences and opportunities at play. The ability to then orchestrate the right

blend of actions among the multiplicity of levers at one's disposal into an integrated overall effort is what realises desirable outcomes. To be able to do this continuously better than the adversary requires sustained information advantage relative to the adversary.

Sense, understand and orchestrate

3.3. The *Integrated Operating Concept 2025* (IOpC 25) introduced the imperative to sense, understand and thereafter orchestrate effects. This is the driving force of MDI; it is analogous to an engine in which sense and understand are the fuel mix and orchestrate is the motor. All three are needed; they must be matched and in balance and of appropriate power for the purpose. The more powerful the engine is, the more windows of opportunity can be exploited across the continuum of competition. If sense and understand are inadequate in comparison to orchestrate, there is a likelihood of misdirected activity that could be counterproductive.

3.4. Sense, understand and orchestrate is not a new framework for the observe, orient, decide and act (OODA) loop. It is less transactional, applies across all the levels of warfare, should be more conducive to non-military elements and is the way we will work out what to do, when, with whom and to what aim. These three related functions have always been necessary, so now are they specified along with a need for balance between them. Additionally, MDI places a much-inflated demand upon them because of the challenge of integrating across the levels of warfare, domains and with other actors.

3.5. In MDI the sense, understand and orchestrate functions are enabled and expressed through a command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) system that connects everything together and allows the system to function cohesively. Advantage in MDI is achieved through being better at sensing and understanding than the adversary, enabled through the means of a C4ISTAR system. This C4ISTAR system can be understood in the following way.

a. The first two Cs in C4ISTAR are **command and control**. Command and control is orchestration, which covers integrating, planning and executing; it thrives on decision advantage.

b. The second two Cs are **communications and computers**. This enables a single information environment[10] connecting the orchestrators with the understanding. It must therefore connect the force elements of our own force; along with those of our allies and partners across government. The single information environment is likely to include a 'digital backbone' and cloud-based capabilities.

c. The final part – ISTAR is **intelligence, surveillance, target acquisition and reconnaissance**. It is the sense which is likely to be an overabundance of data and understand, which will apply processing, exploitation and dissemination (PED) capacity, to convert it into insight and foresight. This is shared among orchestrators via the single information environment.

How will the quantity of sensed data be managed?

10 Joint Concept Note (JCN) 1/17, *Future Force Concept* used the 2017 Defence Information Strategy description of the single information environment. This was 'a logical construct where assured information can pass unhindered from point of origin to point of need. The single information environment will incorporate a single intelligence environment.'

Sense

3.6. Sensing is the essential precursor to understand but needs to be considered more broadly in MDI than just military surveillance systems; it needs to be part of an enterprise approach involving partners across government, allies and the private sector. Sensing provides the raw material for the PED loop through the surveillance and reconnaissance tasks of detection, classification, recognition, tracking and identification to support target acquisition and generate understanding. MDI requires a comprehensive blending of physical sensing with cyber and electromagnetic signatures. MDI particularly requires the ability to sense behaviour among audiences, actors, adversaries and enemies (A3E) for opportunities to exploit and to inform our measures of effectiveness. Audience sensing will need to track social media and other sources in the information environment. Much of this will be open-source information; the trick will be to sift it, interpret it and visualise it in a timely fashion through the C4ISTAR system to those that need it.

3.7. It will be necessary to link the sensors directly to effecters in some situations and to actively probe and stimulate responses. Where the situation is bounded, fast moving and does not require too much integration, the emphasis is likely to be on high tempo through automation and autonomy. A collective and well-resourced machine-readable intelligence mission data system is therefore critical. In more complex situations with higher integration demands or where the need for reliable situational awareness is higher, the requirement will be for more deliberate understanding through PED activity coalesced with sensing from, and in support of, the other instruments of national power.

Understand

3.8. Understanding is the perception and interpretation of a situation to provide the context, insight and foresight required for effective decision-making. It involves developing knowledge to a level that enables us to know why something has happened or is happening (insight) and be able to identify and anticipate what may happen (foresight). Understanding must focus on the A3E relevant to the integrated force as

a whole and must be persistent. The A3E set will need to be understood in the context of the specific operating environments and the global information environment. Commanders who understand these interplays will make better-informed decisions and increase their chances of achieving the intended behaviour changes, or at least know if they are not. A richer audience analysis capability is needed than is currently possessed.[11]

3.9. Common understanding is the ability to comprehend perceptions of groups other than our own and to establish an accepted and relevant baseline for communication, interpretation and action. This common understanding will need to be achieved among the allies and non-military elements, especially through the orchestration of military strategic effects (OMSE) process, whilst assessing aims and risks as broadly as possible. These groups will have differing interpretations of events and views to one another but sharing and fusion will be needed if integration is to be achieved, and the product made available at the right classifications.

3.10. Understanding our own capabilities is as important as understanding the adversary's. To be able to identify where we may possess a domain advantage or disadvantage (a domain mismatch) and foresee windows of opportunity, it will be necessary to understand future and potential capabilities among our own and allied force elements. How we reconfigure the force or augment it with additional capacity by domain will have an impact on this. Traditional comparisons of strengths will therefore have a domain dimension to identify the potential for mismatch. Understanding the 'newer' domains is of particular importance in this respect: for example, the UK must develop a means to achieve sufficient space domain awareness.

11 The Information Advantage Change Campaign includes an insight, evaluation and measurement accelerator project to understand audiences and the impact of our information activities on them.

Orchestrate

3.11. Orchestration is the planning and execution of activities, achieved through integration, that is necessary to influence the behaviour of A3E. It is based on the sensing and understanding of our own, allied and adversary situations and must proceed on the evidence of the actual effects of the activity being executed rather than an assumption of successful intended effects. Orchestration must be resilient and able to continue functioning when the environment becomes so contested and degraded that a clear picture of audience influence is difficult to achieve. In this case judgement will have to apply, but the idea of persistent audience understanding remains valid. The more that is understood and orchestrated when operating, the greater the chance of success if we are required to war fight.

Information systems requirement

3.12. **Vision of the multi-domain integration single information environment.** Federating UK military and non-military information is essential for a fusion approach – it is the linking 'glue'. There must be timely access to shared situational awareness and decision-making in a form that is readily understood at every required level of warfare from the home base to the operating environments, through a user-defined operating picture. Mission and targeting data must be discoverable and available globally in near time and without risk. While a digital backbone is a good visualisation of a bearer system permitting connections into the integrated multi-domain force, this joint concept note (JCN) does not attempt to describe its technical form but the effect is a single information environment. As well as connecting across government the UK single information environment must be capable of integrating into an Alliance framework.[12]

3.13. **C4ISTAR system.** The information exchange requirement associated with MDI is unprecedented. The mass of data derived from myriad sensors will necessitate artificial intelligence and machine learning to detect patterns where previously there was only noise. It must be

12 The North Atlantic Treaty Organization (NATO) is currently developing a common Federated Mission Network.

secure, yet with broad and flexible access, have minimal data latency and bandwidth, be amenable to network management and conform to information technology and data standards. The more extensive the system, the greater its potential to integrate, but the greater the risk of a security breach. A C4ISTAR system as described will require technical leaps and major investment,[13] but it is fundamental to enable MDI – it is the key requirement.

Section 2 – Tenet 2: strategically postured

The global, domain-centric arrangement of capabilities.

3.14. This tenet proposes direction for one of the four foundational principles outlined in the IOpC 25 – an agile and adaptable posture. Successful MDI is founded on having the right capabilities in the right places to be able to converge with others across the domains. This starts with setting the strategic stage through multi-domain posturing.[14] Posture includes policy decisions and is here that fundamental choices on how Defence is conducted need to be taken with a multi-domain mindset. The equipment that we purchase; how we select and train our personnel; and deciding the tasks Defence is expected to fulfil should be decisions made with this mindset. Due to the intra-governmental dependencies associated with MDI, these decisions cannot be divorced from other government departments with whom Defence must be integrated. These decisions should be constantly informed and reviewed through our sensing and understanding, with the ability to enact changes when they are required.

13 JCN 2/17, *Future of Command and Control* discusses the interdependencies between: people, technical, processes and structural aspects which interact in a command and control system.

14 Multi-domain posture is the strategic calibration and distribution of multi-domain capabilities through force management, apportionment, readiness capacity, permissions and authorities.

3.15. **Domain balance.** At the grand strategic level, the UK could decide to seek an overall domain balance[15] in its force structure; alternatively it could deliberately design in an imbalance or a selective domain(s) bias. This would be a complex calculation based upon our potential adversaries with a weighting given to our pacing threat, anticipated Defence contribution to National Security Objectives and expected participation from allies and partners. For example, it could be that the circumstances of our expected operating environments mean that a suitable domain capability can be employed from other domains, for example, denying an adversary space capability through action in the land domain against its ground segment.

3.16. **Burden-sharing arrangements.** The UK already burden-shares with Five Eyes partners in strategic intelligence, surveillance, reconnaissance and intelligence analysis,[16] but could apply the idea of burden-sharing by domain in a systematic way. For example, the UK could agree to weight the air, cyber and electromagnetic domains in an allied arrangement, which could be coalition or North Atlantic Treaty Organization (NATO)-based. This would allow allies to specialise in the domains they value most and are best at, or to preserve options for independent operations if they prefer. This is a major policy question dealt with later in the JCN, but posturing should start with consideration of domain balance.

The UK could burden-share with allies by domain

15 Domain balance is our own relative strength across the domains incorporating the complementary provision of domain capabilities between own, partners across government, allies and partners.

16 This is conducted through the Strategic Effects Force Allocation Board (SEFAB).

3.17. **Support.** Support considerations are integral to the multi-domain posture; they impact decisions about force structure, overall domain balance and domain-centric burden-sharing. The requirement to take a global perspective when dealing with global challenges, violent extremist organisations, and employing capabilities in domains that have global reach (for example, space and offensive cyber), drives the support aspect of strategic posturing. Depending upon the force structure, domain balance and burden-sharing decisions, support arrangements in strategic posturing could focus on: forward basing; pre-positioning; power projection from the home base; afloat/on-wheels stocks; the forward production of items and equipment; increased self-sustainment capabilities – or permutations of them all. The point is that the ability to do MDI is reliant on good strategic posturing and a ready and sustainable integrated force.

3.18. **Strategic effects management process.** Force employment at the strategic level is part of the strategic effects management process (SEMP), but a more domain-centric approach could be adopted. This kind of strategy could include calibrating selected domains to dislocate the pacing threat's domain laydown. This could be achieved by holding domain capability at responsive states to exploit anticipated gaps at moments of vulnerability and enabled through the support posture described above. The SEMP could apportion by domain or monitor domain weighting across the global set-up, including the homeland, as part of overall allied multi-domain arrangements. The SEMP and Joint Commitments Strategic Steering Group (JCSSG) could expend a proportion of overall UK domain capabilities to satisfy campaign requirements, but also consider upcoming strategic windows with strategic A3E in their sights. This is strategic multi-domain posturing: a deliberate activity, which must naturally support the wider UK's international posture by integrating the domain-related capabilities they and private sector industry can bring to bear.

Strategic posturing in the Far East

China's Maritime Silk Road Initiative can be seen as a form of domain-centric strategic posturing. The idea is enacted through a 'string of pearls' in which China develops relationships and access arrangements in geostrategically important ports dominating the sea lanes between China's Hainan island through the Bay of Bengal to the Arabian Sea, the Middle East region and beyond. Initially a maritime domain affair, as China builds its aircraft carrier and naval power projection capabilities, the maritime road will strategically complement the land-based Belt and Road Initiative and prepare the wider region of the Indian Ocean for Chinese multi-domain activities.

Section 3 – Tenet 3: configured for the environments

Readiness for multi-domain activity in operating areas and environments to influence the behaviour of selected audiences.

3.19. This tenet will predominantly be driven by the operational level and centred on the doctrine of integrated action. However, the operational and strategic level must be in harmony to ensure consistency in desired strategic effects and to manage those capabilities that may be controlled at the strategic level, particularly within the space and cyber and electromagnetic domains. To ensure this harmony is generated necessitates an expansion on the idea of environments introduced in Chapter 2.

3.20. **Operating environments.** Operating environments represent the composite of local conditions and circumstances in which military and non-military capabilities must be orchestrated to achieve influence. Operating environments are the surroundings or settings for military operations, and they will be specific to that portion of the battlespace, depending on the relationship with the sub-environments within them. It is the combination of these sub-environments that we need to sense and understand, trying to identify and create points of potential advantage

in the interplay between them. These sub-environments are described below and illustrated in Figure 3.2.

a. **Human sub-environment.** The system of individuals, groups, organisations and their beliefs, values, interests, aims and interactions. It should be possible to categorise people into A3E to plan the cognitive influences required upon each.

b. **Physical sub-environment.** The surface, sub-surface, above surface and space where physical activities take place, where the A3E live, where objects and infrastructure exist, and where weather and atmospheric conditions affect operations.

c. **Information sub-environment.** The data, information, media plus the information systems, cyberspace and electromagnetic spectrum that convey information and influence A3E.

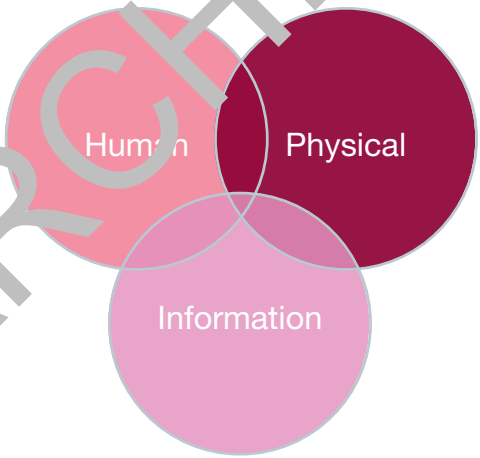


Figure 3.2 – The sub-environments

3.21. **Levels of warfare in operating environments.** With their focus on audiences, all levels of warfare are present, or at least latent, in operating environments in two respects. First, control of some capabilities is held at certain levels, for example, strategic communication, so there needs to be channels available to intervene with them at lower levels in an integrated fashion at the right moment. Secondly, activities at lower levels create effects at higher levels, intentional or otherwise, for example, allegations of human rights abuses on the ground. Operating environments are therefore not synonymous with the operational level of warfare. Figure 3.3 illustrates the interplay of the three levels of warfare and how activity will involve at least one of the three levels: it may be a combination of human, physical and information factors that necessitates consideration at the strategic level, potentially involving another government department, or operational or tactical. Although not illustrated, a sub-environment combination could have implications across all levels of warfare.

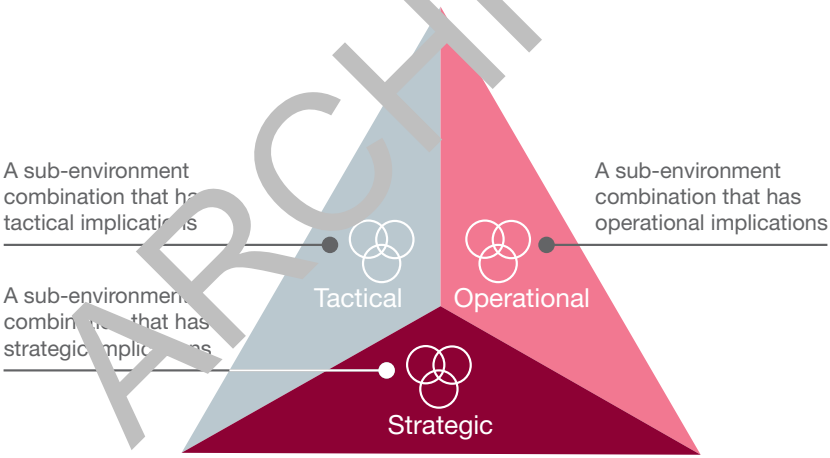


Figure 3.3 – The operating environment

The kidnapping of the Chibok female student[s] by Bo[ko] Ha[ra]m in 2014 is an example of an event within an [op]erati[ng] envi[ron]ment having a strategic im[pac]

© BBC

Multi-domain operating areas – a new spatial framework

3.22. The strategic context, the continuation of competition and the influence of the space and cyber and electromagnetic domains means that geographically bounded operating areas are less suitable.[17] There could be exploitable domain-centric synergies between geographically separate operating areas. It is these factors that give rise to a need for a new spatial framework – a multi-domain operating area. This new framework sees the contest in its broadest possible scope that may be global or regional and is likely to contain several operating environments, linked by national and alliance strategic aims, or by adversary interest.

3.23. The operating area is global when we, or our adversaries, can manoeuvre in a geographically unconstrained domain, such as space or where the effects unfold in an unconstrained way as it does in the information environment. Where adversaries, such as some insurgent groups or less developed militaries, are mostly limited to the traditional domains of maritime, land and air, the operating area could be reduced in scope, so perhaps regional rather than global. The relationship between the MDI operating area and the operating environments is depicted in Figure 3.4.

17 An example is the space domain, where critical infrastructure located on the ground may be geographically separate to where an operation is taking place; thus requiring reconsideration of how it can be protected or effected.

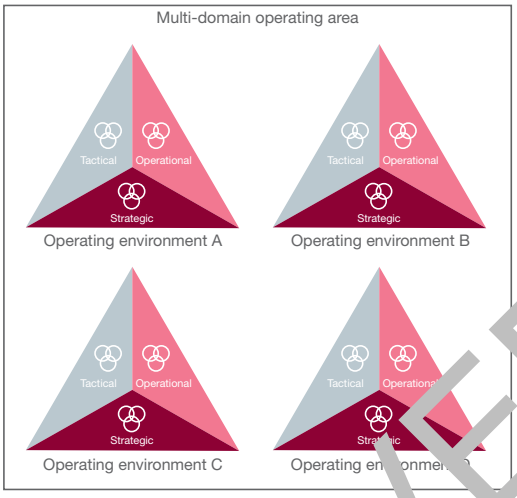


Figure 3.4 – A multi-domain operating area

3.24. Introducing regional operating areas and global operating areas (Figure 3.5) helps to establish the need to integrate across the levels of warfare, understand the interplay between the various actors and to consider situations and potential influences as broadly as possible, as opposed to only having joint operations areas with their narrower connection to the operational level. This creates the space for maximum use of the domains in a way that might outmatch an adversary.

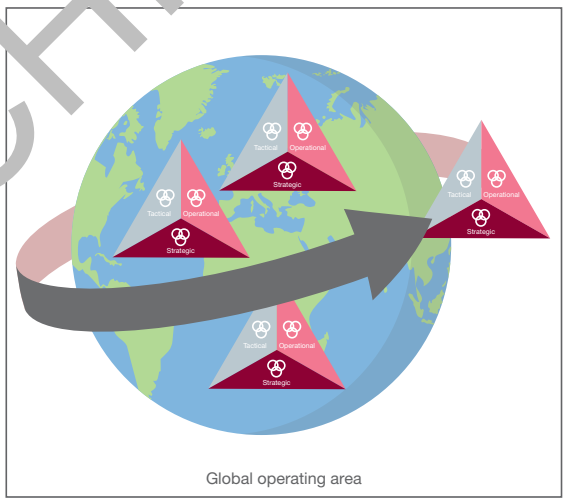


Figure 3.5 – A global operating area

3.25. **Global information environment.** In addition to the localised information sub-environment, there is always a global information environment to consider. The global nature of the information environment means that an activity on one side of the globe can quickly yield effects on the other, commonly at the strategic level. This environment includes social media in cyberspace, international print, opinion formers and broadcast media with whom we have no direct channels. It may also include global A3E who are affected by second and third order effects, such as the allies of the adversary.

Configuring for the environments

3.26. At the operational level, Defence seeks to achieve strategic objectives in accordance with the OMSE process. In MDP, this is enabled through multi-domain configuration.[18] Configuration is an operational-level task, which fashions the force elements allocated from strategic posturing and focuses on the relevant A3E. It integrates them with other capabilities such as in-theatre partners, other UK government or non-military elements to prepare and plan activities specific to operating areas and environments.

3.27. The aim is to ensure military capabilities are arranged, readied and optimised to be brought together for synergy to exploit windows of opportunity within the environments. This will be a continuous process of dynamically managing the operational and tactical laydown of military force elements to not only operate sub-threshold but also be ready to war fight if required. The scope for reconfiguring dynamically will be enabled by the strategic posturing described in Section 2, particularly the support arrangements.

3.28. When planning the configuration of the force, the operational level should also consider the best domain balance in operating environments. This especially includes the responsiveness of domain capabilities that are relatively light in theatre in comparison to the adversary and those which might have high pay-off potential. While it might be useful in some

18 Multi-domain configuration is readiness for cross-domain synergy within operating environments through integrating and synchronising joint functions, allies and partners across government.

circumstances to designate a supported domain such as cyber and electromagnetic, it will be more normal to think in terms of complementary action and convergence of domains and to consider economy, concentration and surging of domain activity.

3.29. The tactical level will be as domain-agnostic as possible, employing fires and actions from any domain to create effects that exploit windows of opportunity. Domains will be balanced or biased according to operational plans. However, there could be options for tactical concentration, supporting/supported relationships, employing domain-based reserves or surges to achieve domain-overmatch and synergy. Examples of enablers and capabilities at the tactical level include:

- fires and other effecters capable of reaching across domains;
- commanders willing and capable of operating across domains; and
- a support system capable of sustaining at the desired tempo and scale of physical action.

3.30. **Configured for outcomes across the levels of warfare.** MDI is likely to gain advantage in the immediate operating environments where effects are created, especially advantages of an operational or tactical nature. They might also have a significant or principal effect in the global information environment. They could also have a domain-centric effect by unsettling an adversary's domain balance in another, or multiple other, operating environments, which might be geographically separated, and perhaps amplified by an ally's similar action somewhere else. This could be a way of perpetrating a strategic offset action.

Section 4 – Tenet 4: creating and exploiting synergy

Generating, timing and exploiting windows of opportunity for relative advantage through the creation of synergy.

Synergy

3.31. Synergy is achieved through the interaction of two or more agents to create a combined effect greater than the sum of their separate parts. It is what sense, understand and orchestrate should be trying to create and exploit; it is therefore a core tenet of MDI. MDI envisages complementary synergies that multiply effects and thereby enables Defence to fulfil its objective in an agile, assertive and adaptable way. The prize of synergy encourages Defence to understand where to focus to achieve an advantageous cumulative effect.

Cross-domain synergy

3.32. MDI specifically seeks advantage through cross-domain synergy.[19] Cross-domain means imparting an effect from one domain into another. Cross-domain synergy is therefore a product of MDI, where advantage is achieved in a single domain or combination of domains through cross-domain manoeuvre,[20] it is a specific product of integrating the domains. Cross-domain synergy can be achieved at all levels of warfare from strategic to tactical. Action at the strategic level will create the conditions for cross-domain synergy by augmenting operating areas with domain capabilities either directly, through reachback or through synchronising strategic activity with lower levels.

19 Cross-domain synergy is advantage in a single domain or combination of domains, created and exploited by the use of cross-domain manoeuvre.
20 Cross-domain manoeuvre is the complementary employment of capabilities in one or more domains in support of another to achieve cross-domain synergy.

3.33. Cross-domain synergy exploits vulnerabilities across the levels of warfare. A strategic raid could be a single or multi-domain action with the purpose of affecting an adversary's global multi-domain calculus. The intended effect could be to threaten domain overmatch in a region, thereby imposing a dilemma on the adversary of whether to react in such a way that affects its domain balance. This would be a strategic-level exploitation of a window of opportunity,[21] which might subsequently open an operational-level window somewhere else.

3.34. At the operational and tactical levels, advantage is most likely to be gained where an action comes from a domain that the adversary was not prepared for, by virtue of being cross-domain, and because it is effective in exploiting the specific conditions and circumstances in an operating environment. Good MDI will involve orchestrating manoeuvrist combinations from the full range of capabilities available to generate cross-domain synergy against these windows of opportunity. Cross-domain manoeuvre is the way to achieve cross-domain synergy. A design to converge multiple domains into a focused effort will almost certainly require synchronised cross-domain manoeuvre.

Windows of opportunity

3.35. Windows of opportunity will be created or sensed within the combination of human, physical and information sub-environments. They should directly or indirectly target vulnerable parts of the adversarial system. This is represented in Figure 3.6. For example, in a technology-savvy, densely populated island city state, where everyone has immediate Internet access, information will spread quickly so an effective window of opportunity might be an action in cyberspace. Alternatively, the upcoming signing of a trade agreement with a state that is sympathetic to our adversary opens an opportunity in the global information environment, which can be linked to an engagement activity in a related operating environment due to local audience sentiment there.

21 A window of opportunity in the context of MDI is a moment of relative advantage identified across the environments for cross-domain synergy.

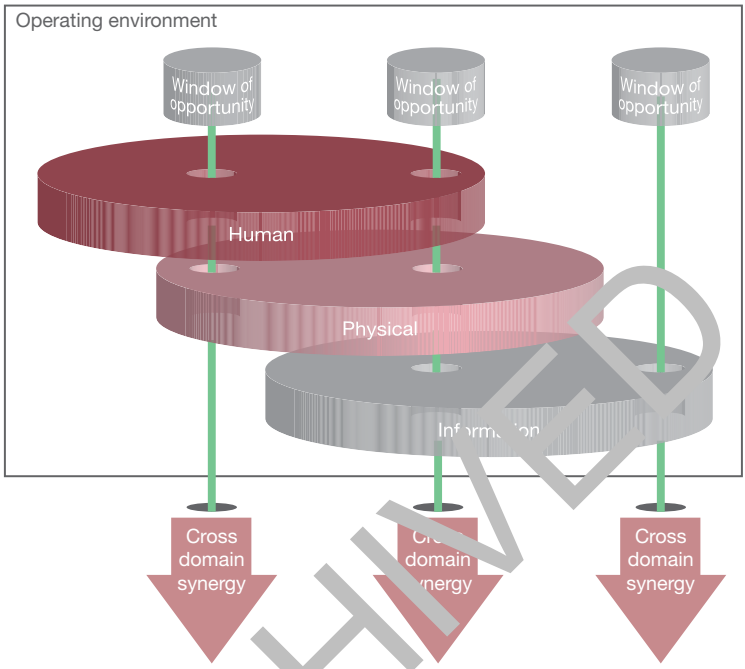


Figure 3.6 – Windows of opportunity

3.36. A window of opportunity may also be generated through a domain mismatch. These can occur in the following ways:

- foreseeing an impending stress, stretch or gap in an adversary domain or domain balance, for example, intelligence of a snap exercise drawing maritime assets to one place;
- enabled through augmentation of domain capabilities from higher (dynamic strategic apportionment) or through allies, for example, the allocation of remotely piloted air systems capable of strike and intelligence, surveillance and reconnaissance;
- by applying other levers of national power which deliver or enable domain impact, for example, increase in stabilisation funding improves attitudes towards UK forces,

- enabled through pre-planned surging and economising of in-theatre domain activity, for example, attaining high aircraft availability through an engineering maintenance surge;
- developed through the use of deception; and
- brought about through cross-domain manoeuvre, synchronisation across domains and converging the domains.

Integrating levels in windows of opportunity

3.37. In MDI, windows of opportunity may be fleeting or extended and will exist at different levels. Some actions within an operating environment will seek tactical or operational objectives but will resound at the strategic level or will be specifically intended to affect global audiences. Alternatively, operating environments might offer a locus for a strategic intervention for other instruments of national power or allies seeking opportunities in tactical settings. Figure 3.7 illustrates this relationship and shows how a window of opportunity within a combination of sub-environments, indicated by the green dot, may have tactical or strategic relevance.

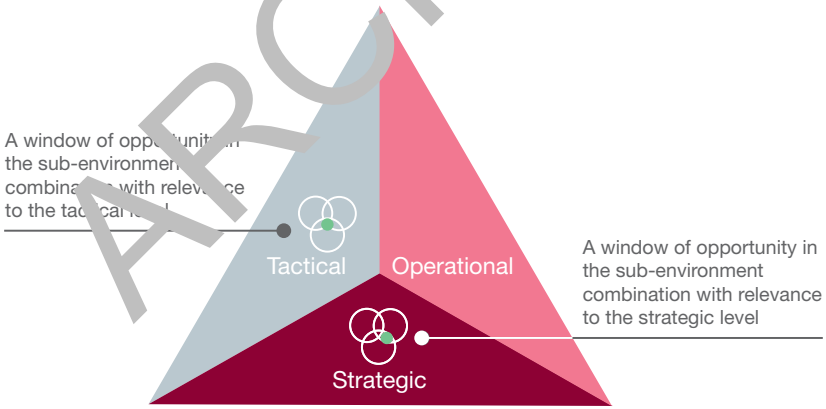


Figure 3.7 – Windows of opportunity across the levels of warfare

3.38. Figure 3.8 illustrates the key terms introduced in this section. In this instance cross-domain manoeuvre between the land, space and cyber and electromagnetic domain results in cross-domain synergy in a window of opportunity with both strategic and tactical relevance.

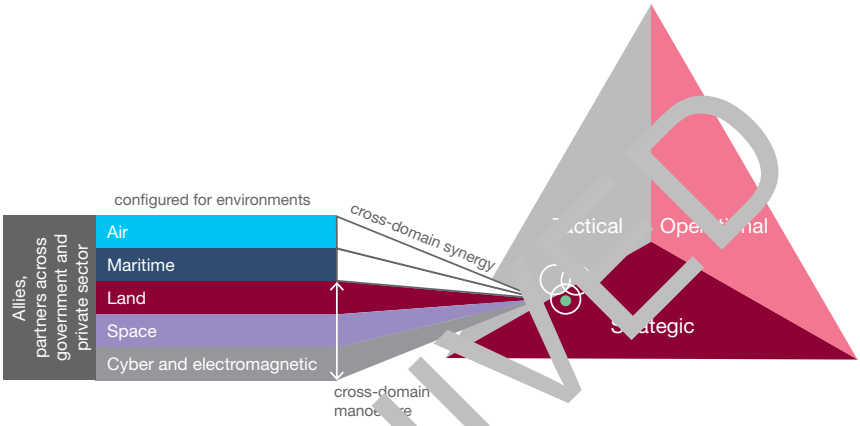


Figure 3.8 – Cross-domain manoeuvre and synergy to exploit the window of opportunity

3.39. **Operational art.** Operational art[22] will be in the planning, creation and exploitation of windows of opportunity. The best effect and tempo will flow from a sequence of windows or a near simultaneous array of windows that seek to disrupt an adversary across an operating area. Windows must be foreseen and identified, which is enabled by the force having configured and planned for it with other instruments of national power as part of a coherent system. The idea is close to full spectrum targeting (FSpecT), seeing windows as targets and arrays of them as target systems.

3.40. **Maximising cross-domain synergy.** It is easier to visualise MDI in situations when we have the initiative and are able to foresee or engineer windows of opportunity and to plan advantageous sequences. However, MDI applies equally in defensive or reactionary scenarios where an

22 Operational art is defined as: the employment of forces to attain strategic and/or operational objectives through the design, organization, integration and conduct of strategies, campaigns, major operations and battles. NATOTerm.

adversary is denied an outcome. Reactive and fast-moving situations will make significant demands on our C4ISTAR systems; cross-domain synergy in these circumstances arising from rapid cross-domain manoeuvre may be the key to regaining the initiative. The ability to seize fleeting opportunities will come when commanders in 'other' domains have the instinctive awareness and enterprise to manoeuvre across domains or command in another domain, thereby generating cross-domain synergy in novel or unexpected combinations. Cross-domain synergy is proportionate to what can be integrated, as shown in Figure 3.9.

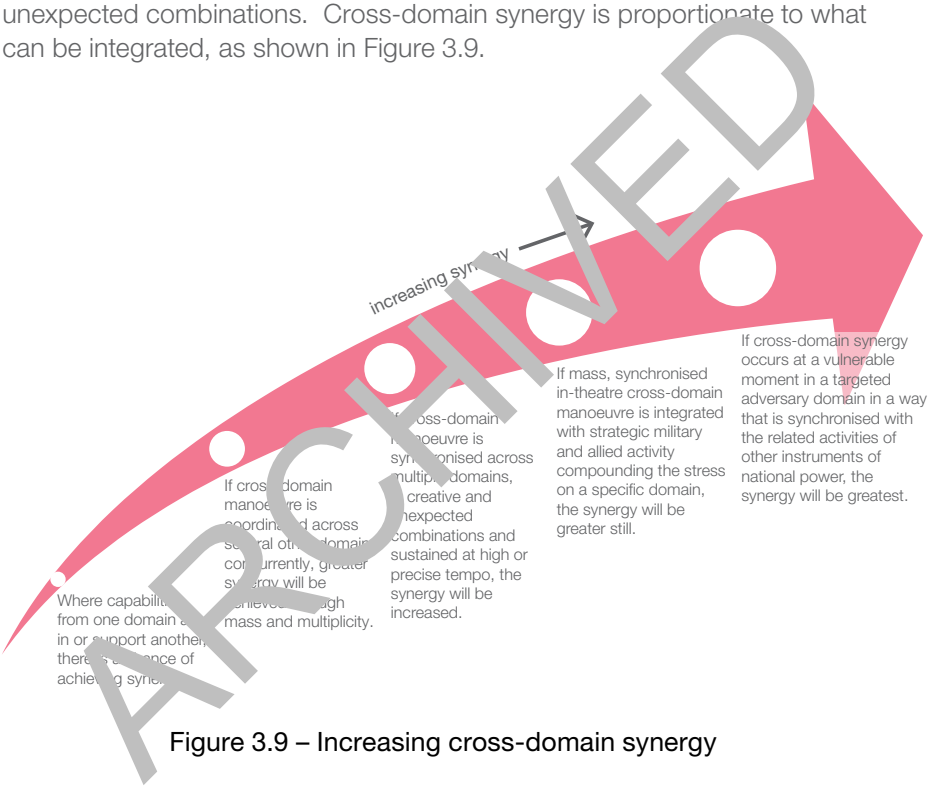


Figure 3.9 – Increasing cross-domain synergy

3.41. **Timing.** Timing is a key challenge for MDI because integrating the domains and levels of warfare in time will be at least as important, if not more so, than integrating in geography/space. Time is a form of 'depth' in the MDI battlespace because the higher levels of command and partners across government will probably be looking further ahead for windows of opportunity. Inserting and synchronising windows in the longer term with those in the near term for synergistic effect will be the aim. The compression of time, especially at the higher levels of command, reinforces

the challenge of the timing factor. The strategic level will have to be close enough to events to be capable of seeing and seizing the moments for synchronisation without overriding the other levels. Understanding the integration demand in time, particularly across government, is both an art and science and will be the key challenge for senior commanders. Important aspects of timing are outlined below.

a. **Synchronisation.** Synchronisation is about integrating events in time to establish favourable rhythms that complement each other. Synchronisation covers not just the coordination of activities that Defence may undertake with partners across government, but the different tempos of these spheres of activity over time. For example, synchronisation might revolve around a strategic window of opportunity in the form of a diplomatic or planned government strategic communication intervention. This could temporarily drive the tempo of all other activities across the levels of warfare until that particular point in time, or perhaps subsequent to it.

b. **Simultaneity.** Simultaneity concerns multi-domain activities happening at the same time for shock or to overload an adversary with multiple dilemmas.

c. **Regeneration.** Regeneration is a timing factor, particularly with military activity at the lower levels of command. Multi-domain capability will vary over time as platforms need to be repositioned, reset for maintenance or resupplied after intense use. The aim should be to configure the force over time to exploit windows of opportunity consistent with available multi-domain capabilities.

d. **Tempo.** Tempo is defined as: the rate of military action relative to the enemy.[23] A high tempo relative to the enemy is generally thought likely to maintain the initiative by trapping the adversary in the early parts of the OODA loop, struggling to 'act' and being inundated with dilemmas. In high-intensity combat at the tactical level, this is highly applicable and may increase chances of success. However, it is a fallacy to think in terms of a single adversary OODA loop; instead there are multiple OODA loops in play at any time both

23 NATOTerm.

within the levels of warfare and especially between them. This is an important consideration: identifying the most pertinent loops in respect of the constellation of A3E and then integrating the different tempos to deliver the most advantage, as shown in Figure 3.10.

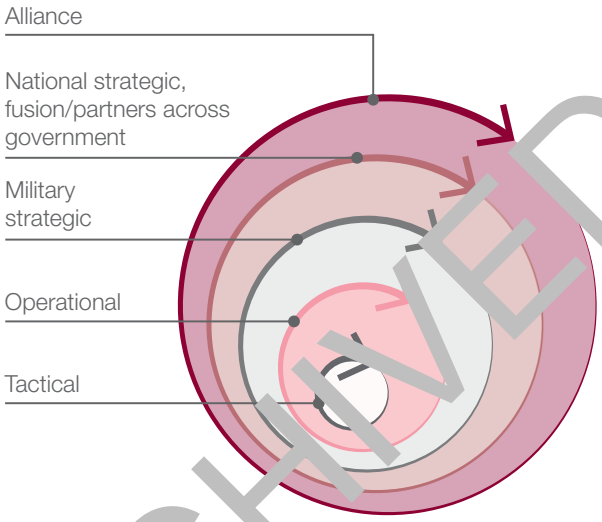


Figure 3.10 – Multiple OODA loops

3.42. **Audience focus.** Aspiring for the highest tempo possible is not always required and could be counterproductive. Going too fast may result in a situation where the effects we seek have not yet played out on the target audience and proceeding further at the fastest rate denies the A3E the cognitive room to change their behaviour in the way we desire. This may be true at the higher levels of command, particularly where other allies or instruments of national power are involved, or where audience-influence 'soak time' is crucial and requires sensing and measuring, or where a cornered enemy's few remaining options include weapons of mass effect. A smarter approach in which tempo adapts to match the actual effects being created on A3E, evidenced by measures of effectiveness, should be sought. This emphasis on playing the audience rather than the rate of military activity places a high demand on the sense, understand and orchestrate functions as audience perception and loyalty can take a long time to change.

Key points

Tenet 1: information advantage. This tenet is about enabling and effecting orchestration through comprehensive and persistent sensing and understanding of environments and audiences, which must be common across government and with allies.

- In MDI, the sense, understand, orchestrate functions are enabled and expressed through a C4ISTAR system.

Tenet 2: strategically postured. The global, domain-centric arrangement of capabilities.

- Successful MDI is only possible if the right capabilities are in the right places to integrate with others. This comes through setting the strategic stage: posturing.

- Posturing should make use of domain balance arrangements.

Tenet 3: configured for the environments. Readiness for multi-domain activity in operating areas and environments to influence the behaviour of selected audiences.

- The operational level will help to integrate multi-domain capabilities that may be controlled at the strategic level, such as space and offensive cyber, with the tactical.

- Operating environments represent the composite of local conditions and circumstances, including the physical surroundings and the A3E they host.

Tenet 4: creating and exploiting synergy. Generating, timing and exploiting windows of opportunity for relative advantage through the creation of synergy.

- Tempo in MDI should be calibrated to be optimal rather than as high as possible.
- Cross-domain synergy will be most exploitable in windows of opportunity. They are identified or engineered within the combination of human, physical and information sub-environments according to relative domain strengths.
- Planning should identify sequences of windows of opportunity, timed for most advantageous effect.


ARCHIVED

Chapter 4

Chapter 4 considers the implications of developing multi-domain integration through the prism of the joint functions, offering insights on how command and control, intelligence, fires, information, manoeuvre, outreach, support and resilience interplay in achieving multi-domain integration. It examines risks including the balance between ambition and vulnerabilities.

> … we must inculcate an instinctive inclination to survey **all the domains**, intervene and command as necessary in pursuance of the overall **multi-domain force objective**.

General Sir Patrick Sanders
Commander Strategic Command
July 2020

Chapter 4

Force development implications

The joint functions

4.1. The joint functions are related capabilities and activities that assist commanders to integrate, synchronise and direct joint operations. They are normally used as a planning checklist in tactical and joint headquarters; however, this multi-domain integration (MDI) concept proposes a more fundamental adoption of these functions. As they have no boundaries, they are applicable to MDI and can be extrapolated to the strategic level – becoming integrating functions. Headquarters structures organised in this way facilitate an understanding of the full range of multi-domain capabilities that are available. As well as being recast as 'integrating functions', force protection is cast as resilience and sustainment as support. The integrating functions are used below to explore force development implications and represent the priorities for experimentation. They are shown in Figure 4.1.

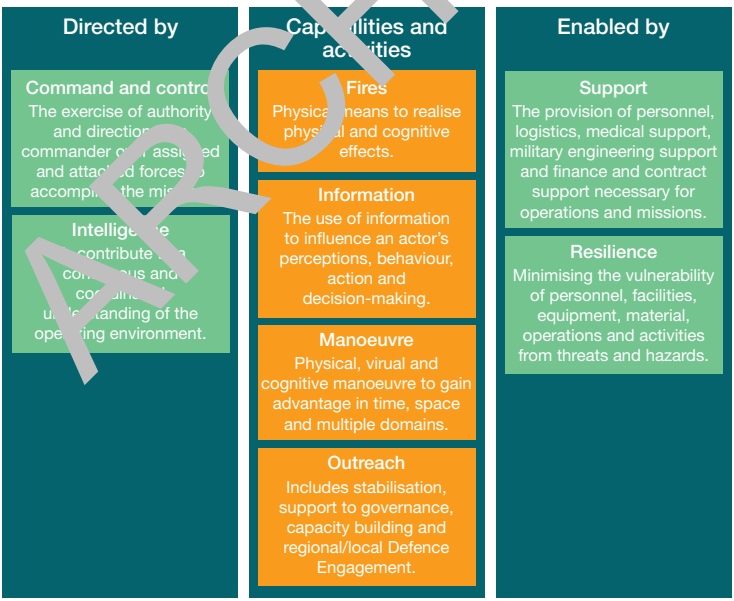


Figure 4.1 – The integrating functions

Section 1 – Command and control

4.2. **Interdependencies.** A command and control system is a socio-technical enterprise owing to the complex interactions between people, structures, technology and processes, as illustrated in Figure 4.2.[24] MDI will necessitate significant advances in each of these individual areas as they are fundamental to successfully realising the conceptual vision; it is therefore necessary to consider each in turn.

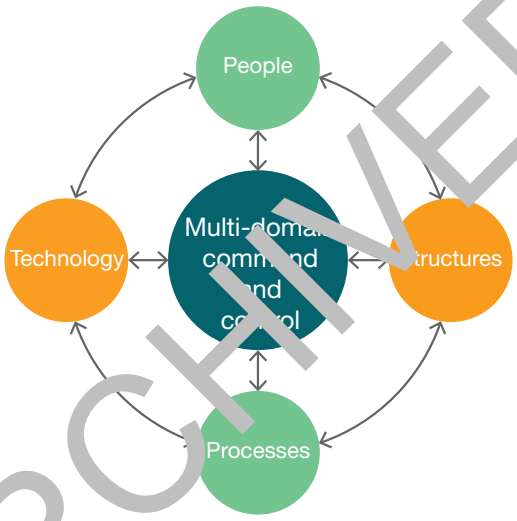


Figure 4.2 – Multi-domain command and control

People

4.3. **Cultural challenge.** The current generation of Defence personnel has brought a trajectory of incremental gains in jointery, but this concept envisages a reframing. This reframing brings a need for a much deeper multi-domain competence than is currently present across Defence. Where there is awareness and some understanding of activity in other domains today, there will need to be an ability to visualise, stimulate and act across other domains; where necessary, an ability to command in them too. There needs to be an early and substantial improvement in

24 Joint Concept Note (JCN) 2/17, *Future of Command and Control*.

understanding of the cyber and electromagnetic and space domains and how to integrate them. The educational foundation for this must be developed. This presents a much-increased demand on professional military education and is at least as important as any other capability requirement described.

4.4. **People management.** The traditional models for recruiting, managing and retaining personnel are already being challenged by the Information Age. MDI will amplify this need for change. The necessity for integration across the domains, and hence those skill sets that enable this, will require Defence to be able to recruit those with the right skills or the potential to have the right skills, at speed. Lateral entry mechanisms are one such means for this, as are joint career management structures that serve to improve retention through greater recognition of talent and expertise.

4.5. **A wider outlook.** MDI will require Defence personnel to be as familiar working across government and with the private sector as they are across domains. An understanding of other governmental departments and a culture that allows successful relationships to be developed is necessary to ensure a genuinely enduring contribution to fusion doctrine. In the private sector, particularly so in the space and cyber and electromagnetic domain, Defence people have to be equipped and managed, such that retention and individual ambition are balanced. This is likely to be necessary to achieve an integrated force.

Multi-domain integration will require Defence to build greater institutional familiarity with partners across government

Structures

4.6. **Designing pathways.** The scale to which MDI must be practiced if it is to benefit the UK will necessitate fundamental change in command and control structures. The operational art of exploiting windows of opportunity through cross-domain synergy, with all the attendant permissions, authorities and contextualised pictures, may well be a sufficiently demanding function in itself to demand new structures. It may also require us to re-evaluate how our single Services support these structures. United States experimentation in the Doolittle Series of war games found that multi-domain operations centres were needed at global and local levels and mission control teams were needed to control tactical missions.[25] This resulted in a new specialisation in the United States Air Force has developed a new officer career field for planning multi-domain operations within the joint all-domain command and control (JADC2) system. Annex A provides more detail about how new structures and a new specialisation could help to meet the orchestration challenge.

4.7. **Componency.** Existing component command structures may not be suitable for MDI because of their hierarchical lines of command that involve sequential and time-consuming communications channels. Experimentation should be focused in this area to understand the longer-term solution to achieving MDI.

Processes

4.8. **Domain ownership.** Due to the way in which the domains interplay in environments, they cannot be owned. MDI may need a looser sense of ownership between the traditional commands and the domains they most commonly operate in. This will demand new processes. Commanders will need to be able to discern opportunities for advantage across domains and the levels of warfare in a culture that encourages cross-domain manoeuvre and intervention, rather than maybe seeing it as trespassing. Instead of looking at the domain in front of them

25 The Doolittle Series of war games was chartered by the Chief of Staff of the United States Air Force to explore multi-domain warfighting concepts to improve command and control of air, space, and cyberspace forces in support of dynamic and operationally agile operations.

and seeking support from the others, it will be necessary to look across the domains and converge in an agile and assertive way. For example, maritime, land or air forces in a supporting role to electromagnetic activity could be a normal situation. Space domain planning must be integrated in a way that accounts for military, civil and especially commercial linkages, as well as allies.

Technology

4.9. **Humans in command.** Chapter 3 outlines the ambitious command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) systems that will be needed for MDI, but the vision is not one of machines in command. The machine will bring advantages of automation and augmentation by artificial intelligence for bounded less-complex data-centric tasks. They will allow analysis that covers descriptive, diagnostic, predictive and ultimately prescriptive capabilities. However, as well as conveying data, the system will need to connect the right people at the right moments for decision-making, delegation of authorities, and legal/ethical assurance. These interventions and inputs of guile, judgement, emotional intelligence and understanding of subtle complexities will remain the basis for military success – and means the human input will endure.

4.10. **Commanding with machines.** Commanders will nevertheless have to be comfortable with having options generated by machines and understand why they offer the solutions they do or make the 'mistakes' they make. Robotics, intelligent and autonomous systems will need to be complemented with carefully calibrated levels of appropriate human control according to the complexity of the task. To command effectively within a multi-domain system, the human operator must be involved.

Section 2 – Intelligence

4.11. **Outcome based.** In an outcome-based approach, commanders and staff extrapolate from the orchestration of military strategic effects (OMSE) process what effects need to be imparted on audiences, actors, adversaries and enemies (A3E) to achieve the desired outcome. Intelligence then needs to develop an understanding of the conditions, predispositions, biases and behaviour of the audiences that need to be influenced. In MDI, sensing and understanding the A3E is the full mix for orchestration; therefore, consistent with the findings of the OMSE project,[26] a much greater capacity for human factors analysis, audience analysis and understanding non-munitions based targeting is needed than is currently possessed. This capacity will likely be drawn from open-source as well as intelligence agency sources and must be capable of being sustained over time to understand the effects that are actually being realised upon A3E, compared to the effects intended and hoped for.

4.12. **Identifying windows of opportunity.** Identifying windows of opportunity for cross-domain synergy will be a form of intelligence support to targeting. It will identify domain-centric mismatches with our adversaries and windows of opportunity within the human, physical and information sub-environments. To fully support MDI, intelligence analysis will need to be able to achieve this between related operational environments at a global level.

4.13. **Single intelligence environment.** Intelligence and intelligence mission data will need to be available in a way that is contextualised to the user. Contextualised in this sense means already integrated with allies and across government, at the right classification rather than limited to the lowest classification, capable of permitting further interrogation, probably through a cloud-based system, and tailored to the user. It will also need to be integrated across the levels of warfare to be able to realise windows of opportunity at all levels. The single intelligence environment must be a subset of the single information environment to enable unified decision support and operations support.

26 *Orchestration of Military Strategic Effects Review Report,* 12 December 2019.

Section 3 – Fires, information, manoeuvre and outreach

4.14. The capabilities and activities of fires, information, manoeuvre and outreach should be orchestrated to achieve A3E influence in support of the desired outcome. These functions represent the primary military effecters, but in MDI they are integrated with allies, across government and with private sector elements; they are also to be capable of operating cross-domain. These effecters can be extended beyond the operational level as described below.

a. **Fires.** Fires to be munitions and non-munitions effecters employed within and across operating environments. They include cyber, electronic attack, space and those from other instruments of national power.

b. **Information.** Information to include actions designed to affect information systems, as well as those activities directly seeking a direct cognitive influence. As a recognised instrument of national power which all government departments have a role in, it is both a challenge and an opportunity for integration both in terms of the narrative and maintaining intra-governmental situational awareness. The existence of a persistent competitive global information environment in addition to any operationally localised A3E is a reality that demands this function to be seen as a daily item of MDI.

Information activities represent both a challenge and an opportunity for integration across domains and across government

c. **Manoeuvre.** Manoeuvre is possible through other instruments of national power, strategic-level global offset actions, space activities, regional and global domain-related burden-sharing arrangements. Strategic domain manoeuvre includes efforts to unbalance adversary domain balance by engineering regional and global overmatches and stresses.

d. **Outreach.** Outreach includes civil-military interactions and assumes that Defence activity will be part of a broader cross-governmental approach. It includes stabilisation, support to governance, Defence-level and military capacity building engagement activity plus an audience-focussed approach towards alliances, host nation activity, diplomacy, global organisations and institutions. It is essential to ensuring that the right outcomes are achieved and, in the event of armed conflict, in ensuring that a state of normal, if not more favourable, competition is achieved afterwards. Outreach is a form of information effecter due to its influence effect.

Section 4 – Resilience

4.15. Previously labelled as force protection, but in the context of MDI, now recast as resilience. MDI is as much, if not more, about systems and networks as it is about formations and firepower and this colours interpretation of force protection from an MDI perspective. It is about minimising the vulnerability of personnel, facilities, equipment, materiel, operations and activities from threats and hazards. Bearing in mind the intention to integrate with non-military elements, the resilience and protective function needs to consider the private sector.

4.16. **Vulnerabilities.** MDI envisages an advantage in information, technology, automation and autonomy, but in so doing, MDI carries a corresponding and equal vulnerability because systems will sometimes fail or not work as intended. Systems and networks will be limited by degraded or denied electromagnetic environment conditions, be physically damaged, might be prone to being fooled by adversary spoofing, or even unable to cope with our own acts of deception. The

relative importance of electronic force protection is therefore increased. Passive measures, such as hardened and secure systems alongside good, secure data protocols and disciplined procedures will complement active measures such as distributed operations.

4.17. **Understanding machines.** Our systems might make unexpectedly bad decisions based on unrealistic rules and algorithms that were only exposed in the full complexity of real conditions. Adversary augmented intelligence might be equivalent to ours and able to predict it in real time. The consequences for resilience are that humans must be capable of knowing when technology is not functioning as hoped and taking the necessary response.

4.18. **Adapting to threats.** The human-machine systems must be capable of adapting to the threats through alternative modes. The mantra is 'preserve the capacity to act'. This should be made a virtue by planning and assuming a level of working technology below the maximum, and below that enjoyed in exercises and synthetic environments. This will provide a more sustainable condition with headroom to press harder if it works well and when it matters most.

4.19. **Command and control modes.** As well as having sufficient information systems capabilities to equip the force, reactive adjustments to current or future contests will demand dynamic approaches to command, control, communications and computers resilience. Joint Concept Note 2/17 *Future of Command and Control* describes adaptive and agile headquarters responding to changes in network connectivity and performance and learning in real time – this is the vision. MDI should exploit diverse and fluctuating command and control styles according to the specific cyber and electromagnetic conditions prevalent within the environments. An ability to pre-select or reactively adopt different styles should be developed: at one end, a decentralised/automated style where complexity and the need for situational awareness is lower; at the other end a centralised/tight style where complexity and the need for situational awareness is higher; and alternative/reversionary styles where forced. These variations could equally be used as part of deliberate security/deception plans.

4.20. **Decentralised and automated command and control.** MDI will be most effective where the C4ISTAR systems and networks are augmented by artificial intelligence and autonomy to support decision-making. This most highly automated, decentralised style will require higher levels of assured communication and information systems resilience and security because it will be handing over a part of the job to machines, albeit with 'human-in-the-loop' oversight. Augmentation by machines is high risk, high reward. The high risks are that an adversary is able to penetrate our systems and either observe or disrupt them; or the adversary has equal artificial intelligence systems using similar programmes and is therefore capable of predicting what others do; or that the situation is either too complex and changeable to allow automation to proceed at high speed according to algorithms.

4.21. **Centralised and tight command and control.** Scenarios involving emotional, legal, ethical and complex informational dilemmas, particularly where judgements of timing are involved and the human factor is most pronounced, are likely to tilt the calculation in favour of tighter command and control. The adage 'if you don't understand the problem, neither will artificial intelligence' should apply. Sub-threshold scenarios of escalatory tensions where the effect of messaging is not yet understood, or de-escalatory stand-off situations may make artificial intelligence relatively risky.

4.22. **Alternative and reversionary.** Where the cyber and electromagnetic domain is highly contested or denied, or for other reasons such as planned deception, alternative or reversionary modes must still be a practiced option. These modes will be 'decentralised', but not in the same respect as the decentralised and automated mode which gives more rein to automation in straightforward situations.

Exploiting windows of opportunity demands agile support systems

Section 5 – Support

4.23. Support encompasses logistics support[27] and engineering support[28] and equipment support.[29] In the same way that sense and understand needs to be matched to desired orchestration capacity, supporting capacity must also be commensurate. Exploiting cross-domain synergy in windows of opportunity at varying tempos using cross-domain manoeuvre across geographically non-contiguous operating environments demands equivalent competitive and enduring support advantage[30] as it does information advantage. This will require a paradigm shift in platform and equipment availability; developing superior, assured, environmentally sustainable and cost-effective logistic services; exploiting data and technology; and a culture of interoperability.

27 Logistics support is the activity to sustain forces by providing materiel; moving personnel and materiel; and providing logistics support services.
28 Engineering support ensures that performance and safety margins are known and managed.
29 Equipment support, a significant subset of engineering support, is the management of the material state of the equipment through maintenance, repair, replacement and control of components crucial to its performance.
30 Support advantage is described by Defence Support as battle-winning effect through the superior provision of support functions compared to that of the enemy.

4.24. In MDI, there should be broader interpretations of support, in terms of how it is enabled to account for the assumption of working as a Whole Force and for specific domain considerations. For example, the space domain provides essential enabling services including positioning, navigation and timing without which the integrated multi-domain force will be severely hampered in achieving its aims. The maintenance of enabling space-based services is critical not just for MDI, but also for other instruments of national power.

4.25. This concept envisages domain balance and domain burden-sharing arrangements with allies. In consequence, the need for full interoperability with allies, including modularisation and standardisation of items and spares, commonality of processes, procedures and standards is clear. This should recognise and embrace UK Defence's dependencies on industry and contractors (such as non-organic elements of the balanced Whole Force) as key contributors to the MDI support solution.

4.26. The support advantages coming from cross-domain synergy and from integrating with other flow from foresight. That is exhibited in preparedness, and the ability to react at the speed of relevance through a blend of options including pre-positioning and technology exploitation,[31] and is underpinned by agile supporting systems (posturing and configuration). An operational/tactical multi-domain sustainment system will involve domain capabilities conducting cross-domain activity and manoeuvre to support other domains, not just for UK force elements but for allies and partners as well. An operational system capable of reacting and manoeuvring across environments according to the multi-domain demands of the moment will need a Defence support intelligence capability. Such a dynamic system will need to have depth, redundancy and conduct contingent and predictive activities that will service both peacetime and warfighting activity and be force multiplying when it matters.

31 Such as the forward production of equipment via additive manufacture, deception and increased self-sustainment capabilities.

The ability to react at the speed of relevance will depend on technology exploitation that delivers support solutions across environments

4.27. Resilience will be required to operate in degraded environments. Cyber and electromagnetic threats will be a major challenge as considerable aspects of the support enterprise will be information-led, technology-enabled, predictive, integrated and interoperable and involve private sector partnerships both at home and in overseas operating areas. The dilemma will be setting a balance between seeking maximised automation and efficiency on one side and security and resilience on the other.

Section 6 - Risks

4.28. **Balancing ambition and vulnerability.** This concept describes an optimal, or optimistic vision for very high and hitherto unachieved levels of integration and capability. However, MDI is not a binary condition that exists or not. It is a spectrum, at one end omniscience with the ability to integrate every friendly entity seamlessly according to the plan with faultless targeted effect; in the middle is a workable ability to cooperate and support each other in a joint fashion; and at the lower end is single Service-centric, possibly deconflicted action.

4.29. **Building collective multi-domain integration.** Real world situations involve adversarial action where relative advantage will apply. The ability to work at lesser, partial and degraded levels of MDI must be regarded as the norm; the core tenets of the *Five Eyes Command and Control Concept Note* offer a potential framework for developing this ability.[32] The likely trajectory is of MDI growth over time, unevenly matched with allies, aiming to integrate the best out of partial, developing and degraded capabilities. Somewhat counter-intuitively, while the greatest level of MDI potential is through all our allies and partners designing in and nurturing a collective multi-domain capability, a degree of variegation rather than a one-size-fits-all system might be helpful for resilience. Experimentation is vital to understanding this way forward.

4.30. **Inherent risks of complex systems.** In looking to exploit information technology, ambition and vulnerability are two sides of the same coin. The higher the ambition and the more complex the overall system, the higher the risk. Noting Chinese and Russian emphasis on systems thinking, the more integrated our system is, the more it becomes a target for systems attack. In a complex system, there is simply more to go wrong, more scope for security breaches and greater potential for unexpected outputs. With more allies, partners and departments, there is more scope for mistakes, leaks, breaches, differences of understanding, intention and goals.

4.31. **Advantage paradox.** Apart from these risks, there is also a paradox that the greater the capability of our information technology in relation to the adversary, the greater our potential advantage to act quickly and decisively. If the adversary perceives this risk, there is a more urgent incentive to either find ways to counter our advantage, or to strike first. As described in Chapter 1, identifying the Western advantage in precision weapons and ways of war is what has driven the advancement of Chinese and Russian capabilities to the need for another offset. To guard against this, the ideal is to have capable, resilient information systems, and to be good at sensing and understanding adversary perceptions.

32 The core tenets are: trust, resilience, agile, decision advantage, collaborative and interoperable. *FVEY Command and Control Concept Note: a FVEY Command and Control Response Network v1.0,* 31 May 2019.

Key points

- MDI envisages an agile command and control capability, augmented by autonomy and automation.
- MDI requires efficient levels of processes, permissions and information exchange capacities to orchestrate cross-domain thinking and manoeuvre. The C4ISTAR system envisaged will require technical, procedural, cultural and educational leaps.
- An ability and cultural inclination to survey the domains, intervene and command as necessary as part of the overall multi-domain force objective will be a force multiplier.
- Component command structures may not be the ultimate solution for dynamic MDI.
- Understanding A3E is a first, foremost and sustained task. A greater capacity for human factors analysis, audience and systems analysis is needed than is currently possessed.
- The functions of fires, information, manoeuvre and outreach are suited to domain thinking and should be integrated and synchronised across the levels of warfare.
- In MDI, the function of force protection should be interpreted as resilience and sustainment should be broadened to support.
- The higher the ambition and the more complex the overall system, the higher the risk.
- The greatest level of national capability will come through investing in highly technical information technology matched by required changes to military culture, education and training.

Notes

Annex A

Multi-domain integration – specialisation

A.1. The level of orchestration needed in multi-domain integration (MDI) demands a review of how integration is functionally delivered. One such option is a coordinating function capable of taking a hub and spoke form. This model would support integration across the domains and levels of warfare through command and control migration around the command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance (C4ISTAR) network to coordinate the integration needs of the moment. The main hub, or hubs, would support planning, particularly linking with allies and partners across government, while spokes would support 'forward' parts and be able to collapse and deploy somewhere else in the network almost instantaneously to support higher integration demands. Hubs would have maximum connectivity, including through high capacity cloud-based systems and support principal operational and tactical command and control nodes. Hubs would continuously deploy and redeploy an architecture of spoke teams, also with enhanced connectivity.

A.2. Headquarters would be reinforced with hubs and spokes according to the dynamic integration needs of the situation. Standing headquarters would have an appropriately scaled set of multi-domain operator specialists covering the diverse demands of the domains: they would either be the hubs themselves or connect to hubs. Headquarters will identify opportunities and potential vulnerabilities in the domains and be capable of cross-domain manoeuvre and controlling battlespace across domains. Major integration episodes will incur dynamic reinforcement of MDI spokes.

Multi-domain designers and coordinators

A.3. A specialisation of multi-domain designers and coordinators could provide the expertise to integrate systems and networks. Multi-domain designers would integrate capabilities through planning full spectrum targeting (FSpecT), identifying windows and designing pathways, with a specialisation of coordinators for managing execution. This specialist function would augment or replace traditional J3/5 and J3 respectively. Hubs and spoke teams would have expertise in both multi-domain design and coordination. The spoke teams would augment existing command and control with additional designer and coordinator capacity. The designers and coordinators would not necessarily need to be together in a forward-based tent, compartment or hangar, but they would need to be able to gain near real time command intent and decision-making, and connect with higher levels of command.

A.4. The designers would have expertise in planning FSpecT through access to sensing and understanding; would be connected to audience analysis systems; and would help to plan the convergence of capabilities for cross-domain synergy. They could act as brokers between force elements effectively leading capability, with multi-domain coordinators looking to 'buy' actions and effects.

A.5. Multi-domain coordinators would be skilled in connecting systems and networks. They would apply the right levels of authority, delegation and calibrate automation and autonomy levels according to command and control complexity and resilience conditions to facilitate timely command interventions. They would ensure connection of the right sensors to the best effecters under control of the best command and control node with the requisite authorities and permissions. They could act as the 'human-in-the-loop' where artificial intelligence and automation is used and connect with command intent. This would be the J3 operations function of today. The issue of authorities and permissions is crucial, as this way of war will necessitate the ability to task any effecter agnostic of the domain from which it came.

Lexicon

Section 1 – Acronyms and abbreviations

A2AD	anti-access and area denial
A3E	audiences, actors, adversaries and enemies
C4ISTAR	command, control, communications, computers, intelligence, surveillance, target acquisition and reconnaissance
CBRN	chemical, biological, radiological and nuclear
DPRK	Democratic People's Republic of Korea
FSpecT	full spectrum targeting
FVEY	Five Eyes
IOpC 25	Integrated Operating Concept 2025
JADC2	joint all-domain command and control
JCN	joint concept note
JCSSG	Joint Commitments Strategic Steering Group
JEF	Joint Expeditionary Force
MDI	multi-domain integration
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
OMSE	orchestration of military strategic effects
OODA	observe, orient, decide and act
PED	processing, exploitation and dissemination
SEFAB	Strategic Effects Force Allocation Board
SEMP	strategic effects management process

UK	United Kingdom
US	United States
VCDS	Vice Chief of the Defence Staff

Section 2 – Terms and definitions

This section is divided into three parts. First, we list working definitions that are yet to be endorsed. We then list endorsed terms and definitions followed by other useful terms and descriptions used in this publication.

Working definitions

multi-domain integration
The posturing of military capabilities in concert with other instruments of national power, allies and partners configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare. (JCN 1/20)

information advantage
The credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems. (JCN 2/18)

Endorsed definitions

operational art
The employment of forces to attain strategic and/or operational objectives through the design, organization, integration and conduct of strategies, campaigns, major operations and battles. (NATOTerm)

operational domains
Discrete spheres of military activity within which operations are undertaken to achieve objectives in support of the mission.
Note: The operational domains are maritime, land, air, space, and cyber and electromagnetic. (JDP 0-01.1)

tempo
The rate of military action relative to the enemy. (NATOTerm)

Other useful terms and descriptions

cross-domain
Imparting an effect from one domain into another.

cross-domain manoeuvre
The complementary employment of capabilities in one or more domains in support of another to achieve cross-domain synergy.

cross-domain synergy
Advantage in a single or combination of domains created and exploited by the use of cross-domain manoeuvre and fires.

domain balance
Our own relative strength across the domains incorporating the complementary provision of domain capabilities between own, partners across government, allies and partners.

environments
Environments provide the setting for military activities. The environment exists prior to, during and after military activity. They will be specific to operations and headquarters, except for the information environment, within which all operations will be conducted.[33]

multi-domain configuration
Readiness for cross-domain synergy within operating environments through integrating and synchronising joint functions and other allies and partners across government.

33 This description differs from the endorsed definition where environments are defined as: the surroundings in which an organization operates, including air, water, land, natural resources, flora, fauna, humans, and their interrelations. NATOTerm.

multi-domain operating area
A multi-domain operating area describes a higher-level battlespace; this may be global, regional or joint and is likely to contain several operating environments, linked by the aims of military and non-military activity.

multi-domain posturing
The strategic calibration and distribution of multi-domain capabilities through force management, apportionment, readiness capacity, permissions and authorities.

operating environment
Operating environments represent the composite of local conditions and circumstances in which military and non-military capabilities must be orchestrated to achieve influence.

window of opportunity
A moment of relative advantage identified across the environments for cross-domain synergy.

Designed by the Development, Concepts and Doctrine Centre

Published by the Ministry of Defence
This publication is also available at www.gov.uk/mod/dcdc