Ministry
of Defence

ARCHIVED

Joint Concept Note 1/17

Future Force Concept

Development, Concepts and Doctrine Centre

ARCHIVED

Joint Concept Note 1/17

Future Force Concept

Joint Concept Note (JCN) 1/17, dated July 2017, is promulgated as directed by the Chiefs of Staff

Director Concepts and Doctrine

ARCHIVED

Conditions of release

1. This information is Crown copyright. The Ministry of Defence (MOD) exclusively owns the intellectual property rights for this publication. You are not to forward, reprint, copy, distribute, reproduce, store in a retrieval system, or transmit its information outside the MOD without VCDS' permission.

2. This information may be subject to privately owned rights.

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 send them to:

The Development, Concepts and Doctrine Centre
Ministry of Defence Shrivenham
SWINDON
Wiltshire
SN6 8RF

Telephone:	01793 31 4216/4217/4220
Military network:	96161 4216/4217/4220
E-mail:	DCDC-DocEds@mod.gov.uk

All images, or otherwise stated are: © Crown copyright/MOD 2017.

ARCHIVED

Distribution

The distribution of Joint Concept Note (JCN) 1/17 is managed by the Forms and Publications Section, LCSLS Headquarters and Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. All of our other publications, including a regularly updated DCDC Publications Disk, can also be demanded from the LCSLS Operations Centre.

LCSLS Help Desk:	01869 256197
Military Network:	94240 2197

Our publications are available to view and download on the Defence Intranet (RLI) at: http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/DCDC and on the Internet at: www.gov.uk/mod/dcdc

Foreword

1. Joint Concept Note 1/17, *Future Force Concept* provides the principal Defence-level guidance and coherence for all future force development in the strategic headquarters and in all commands. This publication represents a step-change in our approach, from separate environmental to an increasingly integrated, joint concept. This change will provide a clearer vector for the design and development of the future force and balance of investment decisions.

2. At the heart of the *Future Force Concept* is the idea that we need to enhance joint action, and therefore our influence and effect on intended audiences, through exploiting information better, being more integrated as a force – across five operating domains that are underpinned by the information environment – and more adaptable to changing circumstances. These are the three central themes of enhancing joint action; a framework for orchestrating activities that will provide Defence's contribution to an increasingly full spectrum approach alongside allies and partners, particularly NATO.

3. Ideas, in the form of concepts, matter in Defence because they bring coherence to the development of a future force across all of the Defence lines of development. So this first joint *Future Force Concept* is an important step forward. But it is by no means the whole. It is the interaction between future concept, future force development and today's force experimentation, training and our lessons learned, which will increasingly flag up the choices we need to make to insert new capability at the tempo required, within resources.

4. The *Future Force Concept* must be read and understood by those involved in policy and strategy formulation, by military capability and acquisition staff, by operational commanders and staffs as they consider the future operating environment, and by the staff and students at the Joint Services Command and Staff College and single-Service warfare centres.

ARCHIVED

Vice Chief of the Defence Staff

Philip Jones

Chief of Naval Staff/
First Sea Lord

Nick Carter.

Chief of the
General Staff

Chief of the
Air Staff

Chris Deverell

Commander Joint
Forces Command

> “Success against complex and diverse threats that exploit pervasive information requires us to do things differently.”

Joint Concept Note 1/17, *Future Force Concept*

Preface

ARCHIVED

Purpose

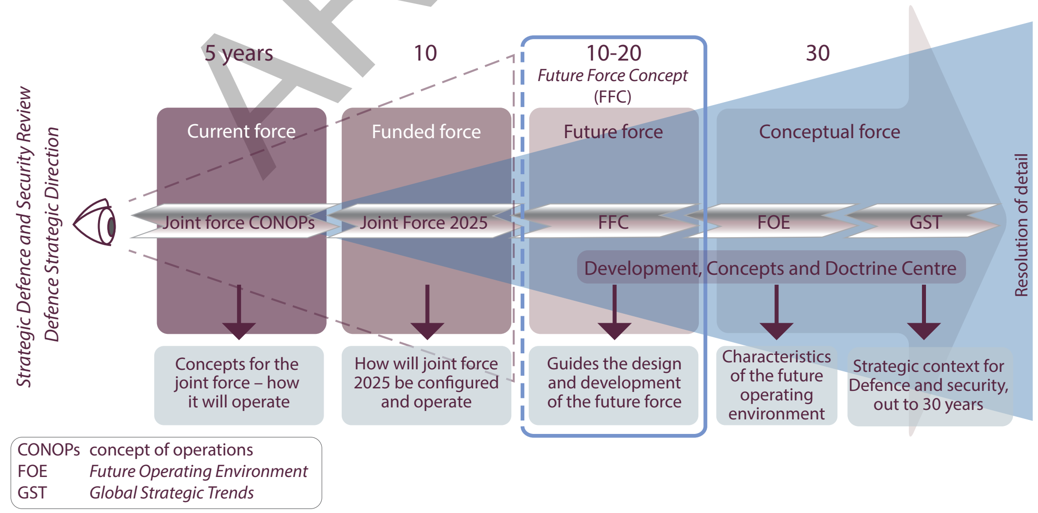
1. Joint Concept Note (JCN) 1/17, *Future Force Concept* combines the separate environmental operating concepts into a single publication. Its purpose is to guide coherent future force development in the strategic headquarters and in all commands, beyond current policy and resource horizons. As the authoritative high-level analytical concept, it supports balance of investment decision-making to shape the design and development of the future force out to 2035.

Context

2. Success against complex and diverse threats that exploit pervasive information requires us to do things differently. At the heart of this concept is the idea that we can enhance joint action, and therefore our influence, through exploiting information, being more integrated as a force and more adaptable to changing circumstances. Integrating information and physical activity across all domains – cyber, space, maritime, land and air – within a full spectrum and multinational approach will be the prerequisite to future success.

Provenance

3. The *Future Force Concept* is evidence-based, policy and resource aware and promotes a joint mindset and common purpose. It has been informed by: operational lessons; training and experimentation conducted by NATO, international partners, Joint Forces Command, the Royal Navy, British Army and Royal Air Force; as well as the views from a broad academic and industry network. It forms part of a continuum of conceptual thinking and headmarks from today out to 30 years, as indicated at Figure 1.


5 years
10
10-20
Future Force Concept
(FFC)
30
Strategic Defence and Security Review
Defence Strategic Direction
Current force
Funded force
Future force
Conceptual force
Joint force CONOPs
Joint Force 2025
FFC
FOE
GST
Development, Concepts and Doctrine Centre
Resolution of detail
Concepts for the joint force – how it will operate
How will joint force 2025 be configured and operate
Guides the design and development of the future force
Characteristics of the future operating environment
Strategic context for Defence and security, out to 30 years

CONOPs	concept of operations
FOE	*Future Operating Environment*
GST	*Global Strategic Trends*

Figure 1 – The Future Force Concept; guiding coherent future force development

Audience

4. The *Future Force Concept* must be read and understood by those involved in policy and strategy formulation, by military capability and acquisition staff, by operational commanders and staffs as they consider the future operating environment, and by the staff and students at the Joint Services Command and Staff College and single-Service warfare centres.

Structure

5. The *Future Force Concept* is divided into 4 parts.

a. **Part 1 – The strategic context and operating environment out to 2035.** Part 1 describes the key aspects of the contemporary and future strategic context and operating environment informed primarily, but not exclusively, by the Development, Concepts and Doctrine Centre's Strategic Trends Programme.

b. **Part 2 – Enhancing joint action.** Part 2 is the heart of the *Future Force Concept* and considers how joint action can be enhanced through exploiting information and being more integrated and adaptable.

c. **Part 3 – Characteristics, challenges and opportunities across domains.** Part 3 considers the five operating domains – cyber, space, maritime, land and air – in greater detail.

d. **Part 4 – Deductions and insights.** Part 4 summarises the principal deductions and insights to guide coherent future force development in the strategic headquarters and in all commands.

Linkages

6. The *Future Force Concept* is linked to the following documents:

- *National Security Strategy and Strategic Defence and Security Review 2015*;
- *Global Strategic Trends – Out to 2045*; and
- *Future Operating Environment 2035*.

ARCHIVED

Contents

ARCHIVED

> “Enhancing joint action through exploiting information, being more integrated as a force and more adaptable to changing circumstances.”

Joint Concept Note 1/17, *Future Force Concept*

Executive summary

Introduction

1. Joint Concept Note (JCN) 1/17, *Future Force Concept* brings together, for the first time, the individual environmental concepts into a single concept to guide coherent force development in the strategic headquarters and in all commands. It is evidence based, resource and policy aware and is the authoritative high-level analytical concept to shape the design and development of the future force out to 2035.

The strategic context and operating environment

2. The *Future Force Concept* foresees a future strategic context and future operating environment characterised by complexity, instability, uncertainty and pervasive information. The distinction between war and peace has blurred and adversaries, both state and non-state, will threaten the stability of the rules-based international order. We will experience persistent and multi-faceted (hybrid) state-on-state and non-state competition, contested access to and control of all domains, and increasing competition for skills. Within this operating context, bringing influence to bear on adversaries, actors and audiences will be more complex and competitive, yet will be ever more central to delivering future strategic, operational and tactical success.

3. We need to do things differently whilst building on our hard-earned strengths to provide credible military options and maintain our freedom of action and political utility. We must also be conceptually pragmatic, recognising the freedoms and constraints of our re-capitalised equipment programme. The future force design must seek to deter adversaries from acting against UK interests and yet the UK will inevitably have insufficient capacity to deter some threats. So we must keep working within a multinational framework to remain effective. Deterrence against the full range of threats to UK interests will require wider partnerships in general and with the NATO Alliance in particular. NATO will remain the cornerstone of our security; the only Alliance that can generate sufficient mass and integrate the conventional and nuclear forces that might credibly deter the most dangerous threats to our security.

ARCHIVED

The *Future Force Concept* – enhancing joint action

4. At the heart of the concept is the idea that we can enhance joint action, and therefore our influence, through exploiting information, being more integrated as a force and more adaptable to changing circumstances. These are the three central ideas behind enhancing joint action; a framework for orchestrating activities that will endure as Defence's contribution to a full spectrum approach alongside allies and partners. Failure to improve all three risks loss of influence.

5. The future force will increasingly need to operate across multiple domains – cyber, space, maritime, land and air. Our primary integration focus should therefore be the joint force, but we would increase options for policy-makers by strengthening our cross-government approach and by improving our interoperability with NATO. Joint action – as a concept – is entirely consistent with NATO and is recognised across Government as Defence's contribution to a full spectrum approach.

6. The *Future Force Concept* recognises five operating domains that are underpinned by the information environment. Although all domains remain equally important, the relative start points for integrating across the domains as a joint force are not. In particular we lag well behind in our ability to exploit the information environment and in the full integration of space and cyber domains.

7. Adapting to changing complex environments, rather than seeking to control them, will be fundamental so the pre-eminent quality of the future force will be the ability to adapt, combined with the agility to do so with relative ease. However, adaptation, or incremental change, is sometimes insufficient and militaries must also be able to innovate to retain their advantage over potential adversaries. Critically, it is organisational learning that underpins adaptation, innovation and agility.

8. Collaborative and qualitative analysis suggests enhancing joint action through exploiting information and being more integrated and adaptable, will be underpinned by six foundational elements. They are:

- agile command and control;
- partnerships;
- people;
- technology;
- training and experimentation (including learning); and
- future force resilience.

Together, these foundational elements represent the building blocks of gaining and maintaining joint force advantage in the future operating environment.

ARCHIVED

Deductions and insights – priorities for future force development

9. Rather than a long 'shopping list' of capabilities, the *Future Force Concept* identifies nine fundamental deductions and insights judged most critical to guide strategic, joint and command force development. They offer the best prospect of making the joint force fit for the challenges of the future operating environment. They are the future force questions that Defence should not ignore.

- How do we rapidly develop and sustain the capabilities and skills to exploit the information environment?

- How can we deliver agile command and control, to offer decisive advantage in response to operational complexity?

- How can we generate future mass effect?

- What must we do to promote and influence conceptual, physical and technical interoperability with partners, on a multilateral basis?

- Maintaining freedom of action within contested domains will require the integration of activity in all domains. How can we develop the understanding and skills to achieve this?

- How will we secure access to the knowledge, skills, experience and talent to operate, innovate and adapt?

- How can we best prepare (training, experimentation and learning) to operate with joint, inter-agency and multinational elements, particularly in complex urban-littoral environments?

- How can we best achieve rapid capability insertion?

- How do we deliver and assure the resilience of the future force for both expeditionary operations and, increasingly, in support of homeland security?

ARCHIVED

Part 1

The strategic context and operating environment out to 2035

The contemporary and future strategic context and operating environment are characterised by complexity, instability, uncertainty and pervasive information.

ARCHIVED

1.1. The increasing information volume, variety and velocity of transmission fuels the complexity of contemporary and future conflict. It rapidly connects new audiences to conflicts and more tightly binds strategy to tactics. Strategy is therefore increasingly sensitive to tactical actions and the opinions of local, regional and global audiences. For military action to be effective, it must therefore be conducted within the context of an effective strategy and a supporting narrative that gives meaning to tactical actions. This is important, because the pervasive nature of information means that success is, and will continue to be, significantly influenced by the extent to which competing narratives[1] influence, or fail to connect with, audiences.

1.2. The distinction between war and peace has blurred and adversaries, both state and non-state, threaten the stability of the rules-based international order that underpins the UK's long-term security. The range, geographic spread and capabilities of potential adversaries make a distinction between home and overseas operations obsolete. Tactical, operational and strategic success will escape a military that continues to embrace only traditional views of conflict. We live in an era of persistent and multi-faceted state-on-state competition. This competition will challenge decision-making using a broad range of tools with both attributable and non-attributable methods to apply pressure below traditional Western military response thresholds. Recognising and responding effectively to hybrid warfare[2] will become increasingly important.

1.3. Though not a panacea, technology will remain an essential element of gaining advantage in the future operating environment and an important driver of military change over the next 20 years. The tempo of technological change will accelerate and human interaction with technology will increase significantly. Combinations of civil and military technologies will allow state and non-state actors to access sophisticated capabilities that were once the preserve of just a few states. The most significant changes are likely to come from the rapid development of information technologies, new sensors and novel weapons,

[1] Narratives are spoken or written accounts of events. Narratives can dominate collective thought, and once ingrained can be very hard to shift. Moreover, narratives can be formed by imagination, myth and stories rather than fact, especially over time.

[2] Hybrid warfare is defined as: a form of warfare combining conventional and unconventional military and non-military actions to achieve a specific goal. (This definition is currently proposed and awaiting NATO agreement).

developments in artificial intelligence, biological and material sciences and a rapid growth of remote and automated systems. Accessing and developing the knowledge, skills and experience to recognise and respond quickly to transformative ideas and technologies, many of which will be driven by the private sector, will be a primary challenge.

1.4. The proliferation of anti-access and area denial capabilities will enable a wider range of potential adversaries to contest our access to, and freedom of movement within, operational areas. Our adversaries will likely deter Western powers by raising the potential cost of action, to exclude our Armed Forces from theatres or to limit their effective employment; either directly or by exploiting vulnerabilities of wider capabilities upon which we depend. In the broadest sense, anti-access may involve political and economic exclusion, which could translate into refusal for basing, staging, transit, port facilities or overflight rights. Under more hostile circumstances, lethal anti-access systems will include more sophisticated longer-range weapons.

1.5. For more advanced actors, offensive space or ground-based anti-satellite systems could disrupt the UK's reliance on space capabilities. Certainly cyberspace will be contested by more people.[3] Offensive and defensive cyber capability will offer specific advantages to competitors, disrupting our networks and systems, while countering our offensive cyber operations. The challenge to information and infrastructure security will be significant, with cyber attacks anticipated to grow in scope, frequency and impact.

1.6. Nuclear states will strive to modernise their capabilities. Weapons of mass effect will be under continued international surveillance, but limited tactical use by states, rogue regimes, or ideologically-driven non-state actors is increasingly possible.

1.7. With increasing population growth and urbanisation, cities will be more connected and physically, culturally and institutionally complex. The city and its hinterland will be an increasingly complex and ambiguous tapestry of actors with shifting allegiances, within which we may be required to operate in different ways, from major conflict to stabilisation and humanitarian operations. Where cities are located on the littoral, the complexities of the urban environment will be amplified.

1.8. National and international human rights legislation is increasingly likely to constrain our freedom of action. 'Lawfare' – the use of law, rather than traditional means, to achieve an operational objective – is likely to be more prominent. We should expect greater domestic and international legal scrutiny of military operations. This may not be the case for our adversaries. We must also consider the moral and legal implications of enhanced automation, particularly for systems supporting targeting and fires, if we are to avoid ceding significant advantage to future adversaries.

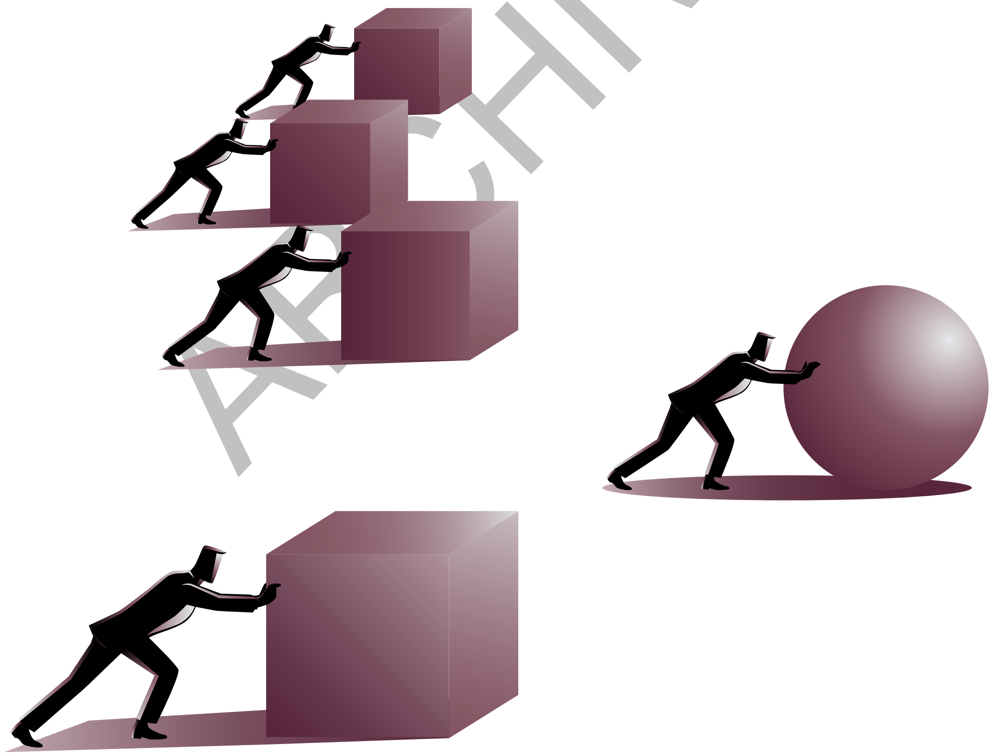
ARCHIVED

[3] Cyberspace is defined as: an operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical,virtual and cognitive domains. Development, Concepts and Doctrine Centre (DCDC), *Cyber Primer*, 2nd Edition.

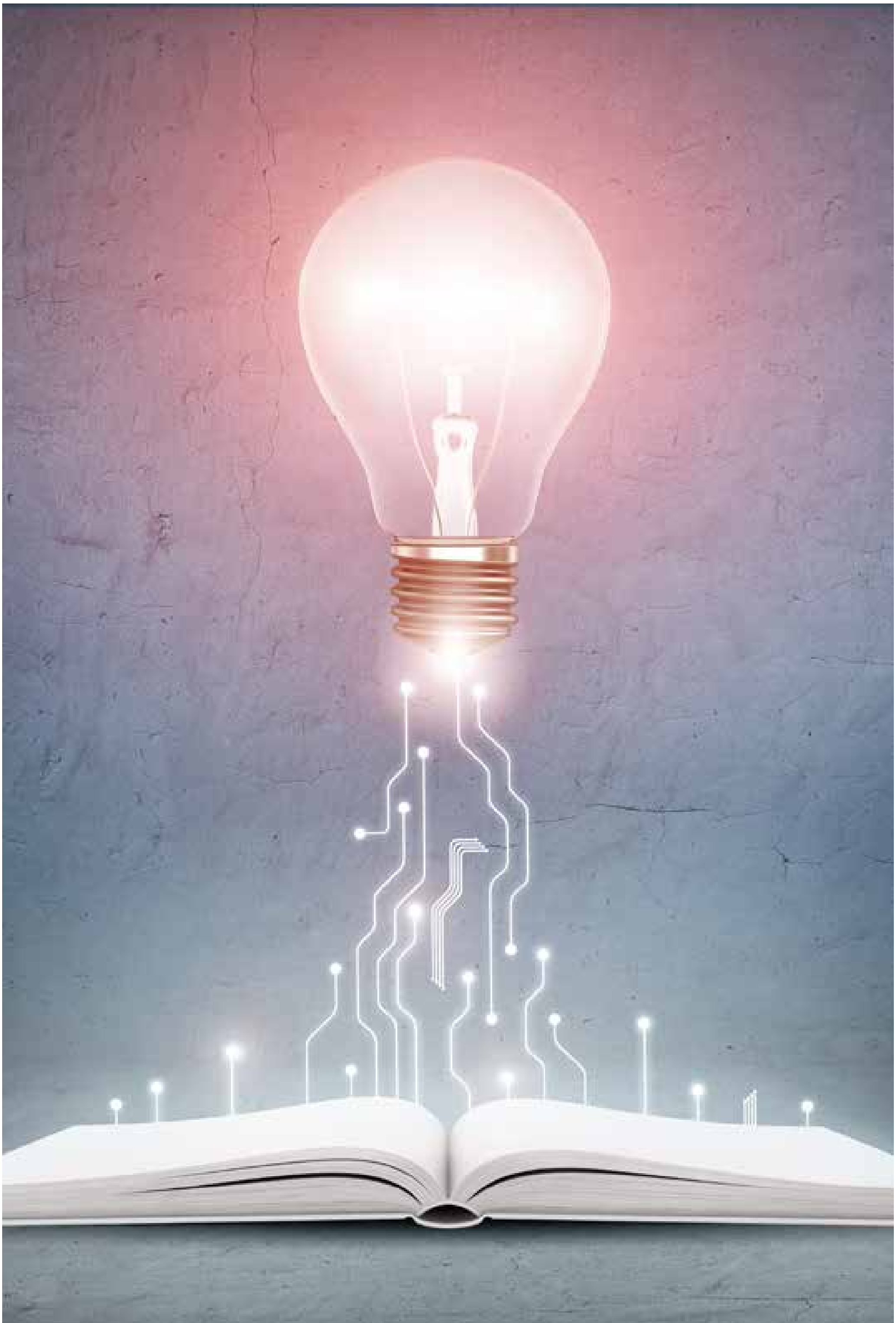
1.9. In this operating environment, bringing influence to bear is more complex and competitive, and yet it is increasingly central to future success. We therefore need to do things differently if we are to provide credible military options to maintain our freedom of action and political utility. A pragmatic response is required recognising that, whilst we are partly constrained by a capitalised equipment programme, there is a strong capability base on which to build. Any changes must guard our hard-won and enviable joint foundation, recognising that it is rooted in the unique strengths and professional competence of each Service, in a combat ethos and pragmatic fighting culture enshrined in the manoeuvrist approach and mission command, and in a robust education and training system.

1.10. The future force design must seek to deter adversaries acting against UK interests. Prevention is easier from a position of strength and it demands the credibility of a robust force confident to fight and adapt in contact when deterrence fails, which it sometimes will. Short of total war, pragmatism will limit UK Defence spending to a capable force, but with less mass than we might desire. This will inevitably have insufficient capacity to deter some threats and so the UK must keep working within a multinational framework for deterrence to remain effective. The framework within which deterrence will continue to function against the full range of threats to UK interests is one of wider partnerships in general and the NATO Alliance in particular.

ARCHIVED



Accessing and developing the knowledge, skills and experience to recognise and respond quickly to transformative ideas and technologies



Part 2

Enhancing joint action

Joint action is defined as: the deliberate use and orchestration of military capabilities and activities to affect an actor's will, understanding and capability, and the cohesion between them to achieve influence.[4]

2.1. Exploiting information, being more integrated as a force, and being more adaptable to changing circumstances are the three central ideas at the heart of enhancing joint action;[4] a framework for orchestrating activities that will endure as Defence's contribution to a full spectrum approach.[5] The component parts of joint action are highlighted below in Figure 2.1.

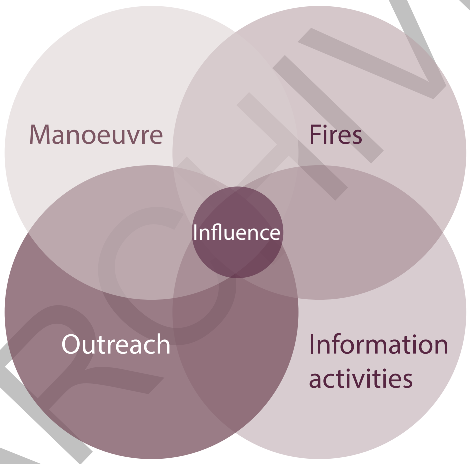


Figure 2.1 – Joint action

2.2. Influence will only be achieved with a clear focus on audiences and effects, and by integrating and synchronising kinetic and non-kinetic activities conducted across the physical and virtual domains to try to achieve those effects.[6] The deterrent threat or coercive use of force are the principal means by which military power influences people or changes the course of events. However, the power of a potent narrative amplified by social

ARCHIVED

[4] Joint Doctrine Publication (JDP) 3-00, *Campaign Execution*, 3rd Edition, Change 1.

[5] A full spectrum approach draws on a range of levers available to a state actor in a coordinated way to achieve (geo)political and strategic objectives. This can include overt and covert activities and the use of political, cultural, diplomatic, economic, military and other levers. The UK applies its levers of national power within the rules-based international order. Her Majesty's Government, *Full Spectrum Approach Primer*, 2017.

[6] Influence is defined as: the capacity to have an effect on the character, or behaviour of someone or something or the effect itself. *Concise Oxford English Dictionary,* 12th Edition, 2011.

media offers significant advantage to adaptable and agile actors. Therefore, we require a better focus on desired behaviours and information effect as the basis of campaign design. Understanding how individuals, groups and organisations interact within the information environment will be vital to shaping perception, identity and behaviour. This can only be achieved by developing an 'unblinking eye' approach to audiences, enabled by insight, evaluation and measurement.   Plans must then be executed through integrating and synchronising information activities, outreach, fires (physical or virtual) and manoeuvre to affect an actor's understanding, capability and will, and the cohesion between them to achieve influence.

2.3.	The future force will increasingly need to integrate information and physical activity across multiple domains – cyber, space, maritime, land and air – as part of a full spectrum approach alongside allies and partners. Our primary integration focus should therefore be the joint force, but we would increase options for policy-makers by strengthening our cross-government approach and by improving our interoperability with NATO. NATO will remain the cornerstone of our security; the only alliance that can generate sufficient mass and integrate the conventional and nuclear forces that might credibly deter the most dangerous threats to our security. Deterrence and collective defence hinges on credible fighting power to unequivocally demonstrate political resolve.

2.4.	Adapting to changing complex environments, rather than seeking to control them, will be fundamental.[7] So the pre-eminent quality of the future force will be the ability to adapt, combined with the agility to do so with relative ease. Both rely on an effective assessment process at the strategic, operational and tactical levels. Adaptability is not solely adjusting to new external conditions or responding to adversaries. It is also about our ability to respond to internal stimuli to change and to seek opportunities for advantage; and to do so time and again. However, adaptation, or incremental change, is sometimes insufficient and we must innovate[8] to retain our advantage over potential adversaries. Innovation questions the routines and systems that underpin core competencies and can involve large-scale changes, requiring a shift in doctrine, structure and technology. The Defence Innovation Initiative, which seeks a broad and systematic approach to innovation and the development of an open ecosystem that capitalises on and builds fertile partnerships with innovators in industry, academia and allies and partners, should be strongly pursued and exploited.

2.5.	Critically, it is organisational learning that underpins innovation, adaptation and agility. We therefore require leaders throughout Defence to engage with and drive cultural and behavioural changes that enable learning, including experience from beyond Defence, supported by appropriate structures, processes, tools, training and education. The relationship between adaptability, innovation and agility is shown at Figure 2.2.

ARCHIVED

[7] Military adaptation involves incremental changes to tactics, techniques, procedures, structures and equipment to improve performance. JDP 04, *Understanding and Decision-making*, 2nd Edition.

[8] Innovation often involves large-scale changes, requiring a mix of doctrinal, structural and technological change. JDP 04, *Understanding and Decision-making*, 2nd Edition.

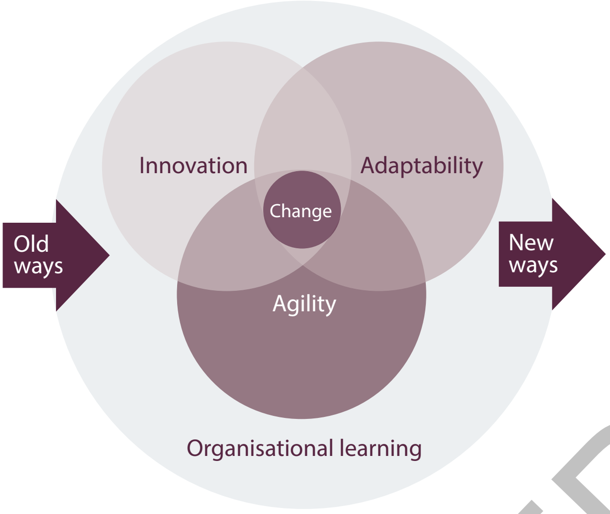


Figure 2.2 – Innovation, adaptability, agility and learning

ARCHIVED

2.6. Collaborative and qualitative analysis suggests enhancing joint action through exploiting information and being more integrated and adaptable, will be underpinned by six foundational elements: agile command and control (C2); partnerships; people; technology; training and experimentation; and future force resilience. Taken together, improving these elements can deliver future joint force advantage. The enhancing joint action model is illustrated below in Figure 2.3.

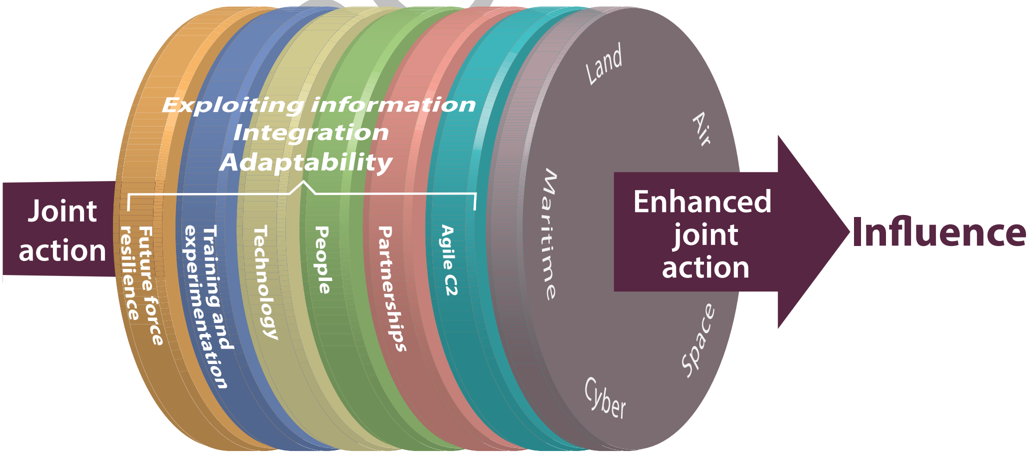


Figure 2.3 – Enhancing joint action: delivering future joint force advantage

Agile command and control

2.7. The equipment programme promises better data collection, but analysis and decision-making is not keeping pace; we do not lead these associated technology frontiers. The pace and growth of information, much open-source and non-military, but still relevant, risks undermining decision-making as diverse threats demand more agile responses.

2.8. Agile C2 is the best response to these problems, which are now almost invariably characterised as complex,[9] with few simple cause and effect relationships. If we can no longer predict, we must instead cope better with unpredicted change. It requires a general shift away from traditional command hierarchies towards flatter C2 networks and greater delegations of authority, albeit still guided by command intent. It will change the way individuals, organisations and systems relate to one another and work.

2.9. There are three important aspects of agile C2: the extent and integration of information networks; increased and improved collaboration; and mission command. The first two require our capability user requirements to become information rather than platform-centric. This requires tough cultural and behavioural change and necessitates a deeper understanding and exploitation of mission command.

2.10. Information must no longer flow in vertical stovepipes, but instead be widely published and available on multiple networks. Exploiting social, mobility, analytics and cloud (SMAC) will be our major network design criteria, enabling us to communicate more effectively, whether in the office or in the field. There will be practical constraints, principally security, physical connectivity and volume of data that can be handled at information choke points. But, central and vertically-oriented information processes must give way to dynamic lateral networks, with processes shaped by user need. Information gatherers will not just feed predetermined processes, but more widely and quickly publish what they see. Much can be automated. Users subscribe to the information services they need. Data analysis and distribution will also be more automated, either centrally, locally or a mixture of both, but dynamically shaped by end users. The single information environment (SIE) will remain valid, but its shape will need to become more adaptable to user need.[10]

2.11. Because some problems will still be solved using traditional C2 hierarchies, those models should in part survive. However, future operational art[11] must be influenced by training and education to choose the right C2 model for any given conflict; one that allows a commander to exploit information and operate across multiple domains to achieve influence. Evolving operational circumstances will demand the continuous assessment and adjustment of C2 at the right pace; we must not become slaves to technology or process

ARCHIVED

[9] Problems consisting of many different and connected parts. Outcomes of actions are particularly uncertain in complex environments. It does not follow that a repeated action will generate the same outcome it did on the first occasion. JDP 04, *Understanding and Decision-making*, 2nd Edition.

[10] A logical construct whereby assured information can pass unhindered from point of origin to point of need. The single information environment (SIE) will incorporate a single intelligence environment. *Defence information strategy*, updated 20 February 2017.

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

at the expense of adapting to, and innovating in, changing context. We must increasingly strive for collaborative C2 and ultimately a model where decision-making can be pushed to the edges of an organisation to exploit the most relevant information at speed and achieve influence in a highly contested information environment.

2.12. Data analytics is the process of examining and interrogating myriad data to derive insights for decision-making. Commanders will still need to make timely and effective decisions and commercially-led data analysis technologies and simulation capabilities offer the potential to provide significant operational decision support. These decision support technologies will increasingly change the way humans interact and integrate with machines and we should consider the moral and legal factors of moving from 'decision support' to 'decision automation'.[12] Failure to integrate data analytical and visualisation tools into our C2 systems is likely to result in overload and decision paralysis.

2.13. Commanders who enable an organisation to think for itself, to develop ideas and coordinate bottom-up are likely to be more successful. Leadership means will often be through social mechanisms that encourage communication and dialogue, develop trust and stimulate interest and creativity. A culture that promotes collaboration, common understanding, a willingness to experiment, to take measured risk and accept setbacks, and to learn and adapt will reap dividends.

IVED

© Colin Anderson/Blend Images/Getty Images

Commercially-led data analysis technologies and simulation capabilities offer the potential to provide significant operational decision support

[12] Information capabilities will increasingly replace human input to support decision-making. Decision automation is where technologies such as 'deep learning' have advanced to the extent that they have the ability to replace human input for decision support and can make decisions on behalf of the human.

2.14. Flatter C2 networks are inherently more resilient than hierarchies, but all systems, command structures and networks will need a degree of redundancy to cope with technological failure and attacks. Survivability within contested domains could be enhanced by smaller, more agile, distributed and dispersed C2 nodes.[13] An ability to conduct protective operations in cyberspace is vital, as is the critical importance of the electromagnetic spectrum,[14] both are considered in greater detail in Part 3. Agile C2 will need correspondingly agile communications and information systems. Future communications and information systems must be simple to deploy, use, maintain and be reconfigurable and interoperable with NATO, primarily, and other partners where practical.

Partnerships

2.15. The range and scale of domestic and international challenges demand multi-faceted responses, with military power increasingly used within a full-spectrum and multinational context. Enhanced joint action demands routine integration of activity in and across all domains, and at increasingly lower tactical levels. Whilst we must be prepared to fight alone, this is less likely. Pragmatism will drive Defence to be more closely integrated with key partners across Government, industry – including beyond Defence – and our principal allies. The typical breadth of inter-agency and multinational engagement increases the complexity of problem solving. But different perspectives, and in some cases greater experience or knowledge, can improve understanding and decision-making, enhance innovation and creativity through diversity of thought and collaboration, and strengthen our capability, capacity and legitimacy.

HIVED

NATO must remain at the heart of UK Defence policy

[13] Distributed command is the ability to leverage cross-governmental, Defence-wide expertise, while deploying forward bespoke functionality. Dispersed command sees the staff and the application of selected tactical functions deployed forward, but not centrally located.

[14] The electromagnetic spectrum is defined as: the entire and orderly distribution of electromagnetic waves according to their frequency or wavelength. Note: The electromagnetic spectrum includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. NATOTerm.

2.16. NATO must remain at the heart of UK Defence policy. We should pursue greater interoperability with allies, in particular the United States, France and Germany, through NATO. This needs leadership commitment and resource prioritisation but offers the potential to influence NATO transformation. Anticipating the need to lead and support coalitions beyond formal alliances, we should also expect to engage with new partners. It will be easier to find the optimum path that supports technical integration with NATO and our closest allies, without closing down options to work with others, if we lead change from within NATO. This will strengthen Alliance cohesion.

2.17. To ensure UK influence on decision-making and campaign design, it will be important to contribute senior officers and experienced staff officers to complex multinational C2 structures, particularly within NATO. We must support NATO's intent to develop a common federated mission network, including developing our own affiliation and integrating our single information environment into the Alliance C2 framework.

2.18. A broader and closer relationship with industry, academia and civil society – an expanded Whole Force approach – would bring mutual advantage and provide better linkage to the security sector's 'total force'. Each partner can benefit from access to critical skills and knowledge, and our ability to innovate and adapt could be strengthened through a more outward looking approach. Such an approach should be sought during training and experimentation as well as on operations.

People

2.19. Our ability to exploit new technologies and approaches will require access to people with appropriate skills, knowledge and experience. In a competitive and changing labour market, securing access to expertise in important sectors such as science, technology, engineering and mathematics – specifically information and communications, intelligence, cyber, space, nuclear, computing and simulation, medical and legal – will require a more collaborative approach with other government departments, multinational partners, industry and academia. We will need to broaden our knowledge, qualifications, skills and experience through greater external opportunity and lateral entry. Exploiting novel contracts and employment models, including portfolio careers and flexible working practices, will become more important if we are to attract a more diverse pool of talent to Defence. An inclusive approach to accessing skills and knowledge will encourage the open-mindedness that underpins adaptation and agility. Complexity and uncertainty also demand intellectual rigour, and the pace of change means that individuals may need to learn new skills many times in their careers. Lifelong education and training will be vital if we are to maximise the potential of our people.

2.20. The versatility of the human mind is a fundamental enabler of our adaptability although man-machine teaming will become increasingly important; we will need to design our people into future systems and capabilities. A range of technologies offer potential to augment human physical and cognitive performance. Prosthetics and neuroprosthetics (mechanical devices directly controlled by the brain), including exoskeletons and

ARCHIVED

telexistence, offer techniques to overcome the physical limitations of the human body.[15] Support to how we visualise information and learn will also be aided through augmented reality systems and real-time language translation capabilities. We must weigh these compelling advantages against our ethical judgements and the law, cognisant that many potential adversaries will be far less constrained. In future, our response to threats may need us to debate current legal boundaries, or potentially cede decisive advantage to adversaries.

Technology

2.21. Technology will remain an essential element of future conflict and a driver of military change over the next 20 years. Maintaining a technological advantage across key capability areas has for many years enabled us to succeed with relatively small professional armed forces. But globalisation and weapon proliferation, combined with constrained resources, mean that this advantage is likely to be significantly eroded. We will have to compete harder, and at greater cost, to gain access and to dominate where we have been largely unchallenged in recent years. We should therefore expect increasing parity in technology availability and accept that exquisite technology is not the key to operational advantage.

2.22. Operational advantage and freedom of action are not absolute and will evolve over the lifetime of a given capability and the context within which that capability is employed. Future capabilities are as likely to be generated by the novel combination of new ideas and existing technologies as by the application of novel science. The levelling effect of technology proliferation may put an increasing premium on mass and the associated resilience to overwhelm sophisticated defences; a different expression of the manoeuvrist approach, involving predominantly new indirect ways and means to apply strength against identified weakness.

2.23. There are three deductions. Firstly, we must recognise that our people are at the heart of our ability to innovate and adapt. Secondly, we should prioritise the means to more deliberately innovate; a culture of continuous experimentation, in every aspect of defence, without fear of failure; a safe to fail, not fail safe approach. History tells us, and it will increasingly be so in the future, that a force that can adapt quicker with what it has will generally prevail. It is not always essential to have the best equipment; we must learn to master what is good enough and to update it and our tactics frequently. Thirdly, we should focus research and development investment in a number of technology areas, which we judge may offer a decisive and/or asymmetric future advantage. In parallel, we should seek to mitigate risk in those areas where we choose not to invest, or to invest less, by leveraging the investments and influence of our allies and partners. Similarly, we should forge stronger links across Government and with commercial expertise, which promises better long-term affordability and reduced exposure to risk.

ARCHIVED

[15] Telexistance is fundamentally a concept named for the general technology that enables a human to have a real-time sensation of being at a place other than where he or she actually exists, and being able to interact with the remote environment, which may be real, virtual or a combination of both. It also refers to an advanced type of teleoperation system that enables an operator at the control to perform remote tasks dexterously with the feeling of existing in a surrogate robot working in a remote environment.

2.24. The most significant technological progress and scope for disruptive impact is likely to be the rapid development of information and communication technologies; an array of sensors and novel weapons; radical developments in biological and material sciences; and the rapid increase of remote and automated systems – cheap, smart systems that can provide resilience, greater persistence, mass and political choice at reduced cost. Real competitive advantage lies in the potential to harness multiple near simultaneous technological breakthroughs in the hands of the same user.

Maintaining a technological advantage across key capability areas has for many years enabled us to succeed with relatively small professional armed forces.

2.25. To exploit the increasing pace of technological change, we must become more institutionally agile in our acquisition system. This requires a culture of collaboration and the necessity to embrace modular approaches, spiral development and open standards and architectures. Small and medium-sized system providers and non-defence companies, rather than major platform builders, will become the primary sources of innovation. The balance is likely to move towards greater reliance on rapid capability insertion in technological areas where the pace of development in the civil sector is high; particularly for cyber, information and communications technology including data analysis, computing, simulation, space and automation.

ARCHIVED

Technology will remain an essential element of future conflict
and a driver of military change over the next 20 years

Training and experimentation

2.26. Our leaders must inspire and reward creativity, encouraging our people to anticipate and thrive on change and so prevail in demanding environments. Battle labs, wargames and simulation offer opportunities to experiment in how we fight; learning as we test new techniques and systems, building a depth of knowledge in training that will inculcate a habitually adaptive mindset across the joint force and with our partners.

2.27. Preparedness will remain a powerful demonstration of capability and intent at the heart of our conventional deterrent posture. Few exercises or training events are widely reported but each can communicate our strength, credibility and reliability to both deter adversaries and reassure partners. Preparation must include familiarity and proficiency in joint, inter-agency and multinational frameworks to improve cultural awareness and interoperability.

2.28. The anticipated complexity of the future battlespace cannot all be reflected in current live exercises and we must better integrate all the elements of joint action in future training. As well as supporting understanding and decision-making, augmented reality systems and synthetic environments offer opportunities to improve the quality and potentially the availability of training opportunities, including live/synthetic blending for collective training and rehearsal, both domestically and with international partners.

2.29. Live, virtual and constructive training offers opportunities to link across domains, particularly information and cyber, in a way that will not be possible through live-only exercises within the constraints of budgets, training estates and legislation.[16] It promises more effective and frequent joint training than we currently conduct, but it will also support testing and experimentation to help integrate remote and automated systems, as well as other new capabilities as they unfold.

2.30. Despite technological opportunities, people and their perceptions will increasingly dominate decision-making and will constitute vital ground. Therefore, the future operating environment will make increasing demands on the judgement, training and resilience of our people, at all levels, and forces will require tailored cultural preparation for success. We must better prepare people to deal with an omnipresent media, rigorous public attention and legal scrutiny. We have to also invest in sufficient training infrastructure, particularly urban, to support a more realistic approach to the way in which we prepare for conflict.

Our leaders must inspire and reward creativity, encouraging our people to anticipate and thrive on change and so prevail in demanding environments.

ARCHIVED

[16] Live, virtual and constructive training simultaneously includes: live training – real people operating real systems; virtual training – real people operating simulated systems (for example, a pilot in an aircraft simulator); and constructive training – simulated people operating simulated systems (for example, a computer programme generating and controlling threats against a crew in a submarine simulator).

2.31. Some training must assure standards; however, we should create unpredictability by embracing training that pits thinking opponents against each other and generates friction, uncertainty and a multitude of other realistic elements. Training for adaptability is about thriving and not just surviving in chaos. We cannot train for the unforeseen, but generating the right mindset for adapting to the unanticipated and unfamiliar is feasible. Training that creates the fundamental building blocks of capability – our core competencies, fighting spirit and moral cohesion – must endure. But adaptability will flow from training that allows us to practise rapidly reorganising or modifying those well-understood building blocks.

2.32. Training and experimentation must be supported by continuous fast learning through leadership that fosters the rapid sharing of sometimes hard lessons. Effective learning is critical to avoid repeating failure but it is not easy, especially if it challenges routines, special interests and cultural norms. The findings of the Iraq Inquiry published in 2016[17] provided a timely reminder of the need, throughout Defence, to build a culture that promotes and encourages challenge and better performance. This will come from collaborative and open command climates where biases, preferences or erroneous assumptions are challenged. We must also place greater emphasis on the role of evidence and critical thinking in our decision-making processes and incorporate these within education and training. Progress will be signalled by a culture in which there is time and space for honest mistakes in the pursuit of learning, and where calculated risk can be taken without fear of failure. Mutual trust and respect are at the heart of this cultural challenge.

HIVED

The pace of change means that individuals may need to learn new skills many times in their careers

[17] *The Report of the Iraq Inquiry Executive Summary*, HMSO, 2016. Commonly referred to as the 'Chilcot Report'.

Future force resilience

2.33. Deterrence and our freedom of action in contested domains demands a resilient future force at both an individual and organisational level. The resilience of our force will not be an ability to rigidly sustain its form, but instead its capacity to endure shocks, adapt and win. Creative thinking, robustness, redundancy and reversionary modes will enable our freedom of action, accepting that it will be impossible to predict, plan or prepare for every contingency. Materiel losses, degradation of systems, casualties and surprises will occur and we should ensure the ability to replace and grow both capacity and capability rapidly. Operational resilience will need much more than physical protection; legality, legitimacy and public support will become increasingly important. Furthermore, hybrid attacks by adversaries against the will and cohesion of the nation, possibly through targeting soft targets in our homeland, is likely to increase. It needs a broader and more coherent view of protection; a whole-of-society resilience and, thus, a full spectrum approach.

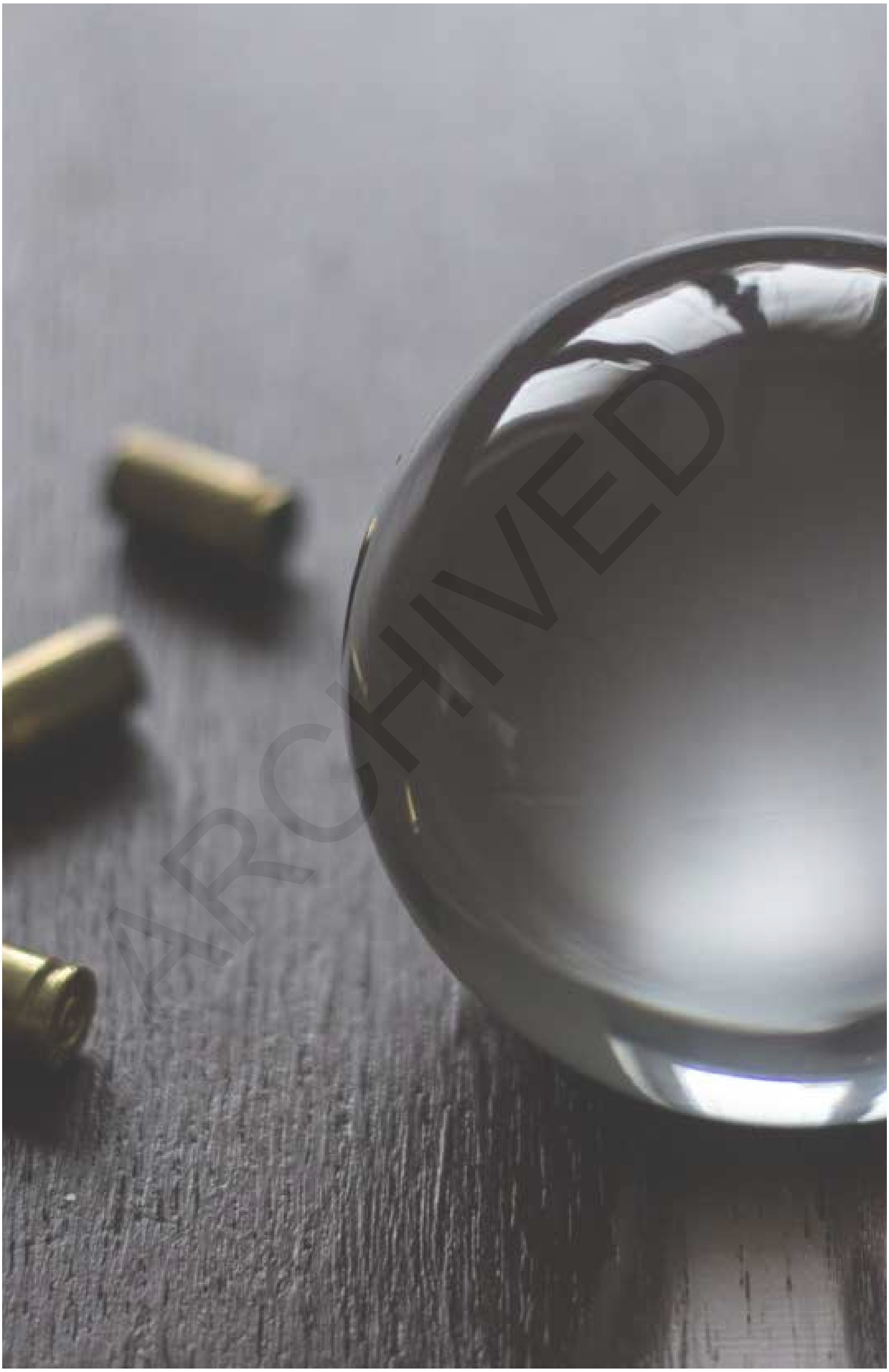
2.34. Working with partners may offset in part our lack of mass, but we should determine the best balance between the quantity and quality of our capabilities; a single exceptionally capable platform can be a single point of failure. Rapid tactical mobility, including the ability to disperse and concentrate at pace, will enhance resilience. Reinvigorated chemical, biological, radiological and nuclear, air and missile defence and counters to multi-spectral sensors are also necessary. Energy-based defences and cyber and electromagnetic activities combined with dispersed operations, camouflage, concealment, deception and the hardening of electromagnetic spectrum dependent systems offer much potential. Given the expansion of military and other activity in space, we should consider the requirement to project power into and through space, both to protect space-based systems from potential adversaries and to guard the benefits inherent in the use of space.

2.35. Ultimately, we can only fight the confrontation or conflict we can sustain; a hollow force is neither credible nor capable. Logistics must therefore be as agile as the forces they support. Through new technology, resources must be capable of being rapidly assigned, distributed and redirected, with the logistic footprint optimised to match both the speed and flexibility of activity and the weight and variety of effects. We need physical and systemic resilience, particularly for munitions, with redundancy and multiple points of supply. And we should increase logistic interoperability and embrace burden sharing with our closest allies, through NATO. The principle of physical sustainment being a national responsibility will need to be tested; moral and political responsibility will endure.

2.36. Technology should enable increased resistance to disease, fatigue and shock, enhanced performance and highly resistant protective materials, as well as more capable bio-sensors for detecting threats. Managing the general health of the future force could be enabled by remote monitoring and application of medicine. Synthetic blood will be more easily stored than traditional transfusion products and may be used in forward medical facilities while casualties undergo robotic surgery supported by reachback telemedicine and advanced bio-manufacturing of useable tissues.

ARCHIVED

ARCHIVED



ARCHIVED

Part 3

Characteristics, challenges and opportunities across domains

Although all domains remain equally important, the relative start points for integrating across the domains as a joint force are not.

3.1. An analysis of an operational environment must consider the four traditional domains – air, land, maritime and space – and the cyber domain. Exploiting the information environment underpins the achievement of influence in and across these domains; this is highlighted below in Figure 3.1. Part 3 considers the principal factors pertinent to each domain. Operations will demand an understanding and integration of all domains and Parts 2 and 3 must be read and considered as a whole given they are entirely interdependent.

ARCHIVED

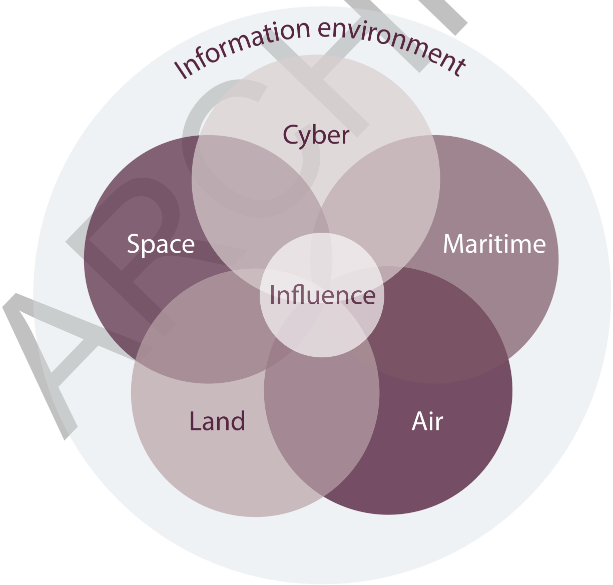


Figure 3.1 – The information environment and the five operating domains: achieving influence as part of a full spectrum approach alongside allies and partners

Section 1 – The cyber domain

Introduction

3.2. Cyber and electromagnetic activities (CEMA) are interdependent and within the cyber domain we must adopt a CEMA approach.[18] Actors will use both electromagnetic activity and cyberspace to contest each domain from the other.[19] Digitisation has led to the convergence of cyber and information activities, heralding an age where CEMA coordination across the joint force will be an imperative for operational success. Freedom to use parts of cyberspace and the electromagnetic environment (EME) flexibly and to deny, degrade or constrain adversary access will offer significant competitive advantage.

3.3. A huge amount of information exists and is transported over the Internet, with close to ubiquitous reach, and potential target system access, in developed states. Much of this information (or the raw data required to produce the information) is available 'open source'. However, some will reside in protected systems or data storage and will require specialist operations to access it.[20] CEMA teams will need to be multi-disciplined, highly trained (not just technically adept) and closely coordinated and deconflicted with other activity across all operational levels.

VED

© iStock.com/chombosan

The potential reach of cyber extends to the whole of modern societal infrastructure

[18] Cyber and electromagnetic activities occur in the electromagnetic environment (EME). The electromagnetic environment is defined as: the totality of electromagnetic phenomena existing at a given location. NATOTerm.
[19] Electromagnetic activities encompass electronic warfare (electronic surveillance, electronic defence and electronic attack) and electromagnetic spectrum management (including radio frequency communications).
[20] Note that even though information may be available as 'open source', exploitation activities require a disciplined, coordinated and managed approach to its collection and exploitation.

3.4. The wider CEMA domain and the characteristics of cyber warfare in particular (including the difficulty in attribution of attacks, the ubiquitous reach of cyber networks and the ability to achieve covert poise) offer an ideal arena and methodology to conduct non-lethal, plausibly deniable and enduring operations. The potential reach of cyber (and the wider CEMA capability) extends to the whole of modern societal infrastructure, ranging from individuals to entire populations. With the overwhelming abundance of information now stored or moved electronically, cyber will play an increasingly major and vital role across all phases of an operation.

CEMA situational awareness

3.5. Cyber terrain constantly fluctuates, in terms of hardware used, software and the configuration of networks. As a consequence CEMA actors need to be adept at understanding and manoeuvring within CEMA and its confluence with the information environment. Real time, or near-real time situational awareness of CEMA will enable the agility for dynamic spectrum management and so enhance joint force resilience. It will also be required to optimise data analytics, which could identify and exploit information.

3.6. Establishing CEMA situational awareness is difficult and therefore both a challenge and an opportunity for everybody. The difficulty of attributing cyber activities is well understood, but as agile use of the EME has become the norm, using spread-spectrum and frequency hopping methods, even identifying actors in the EME is challenging.

3.7. As with standing Defence intelligence activities, we will need to establish cyberspace and EME patterns of behaviour in areas of interest. Standing cyber and EME survey data will enable intelligence, surveillance and reconnaissance (ISR), to help us identify adversary activity and support control of our own use of the EME. Against the ambient background noise of the local EME and routine cyber activity, CEMA situational awareness will also allow us to optimise signature management and develop techniques to hide from or deceive adversary attempts to detect our forces.

ARCHIVED

CEMA integration and control

3.8. The mainstay of CEMA advantage is cyber and electromagnetic battlespace management. Local and time-bounded superiority in cyberspace and the EME will depend on technical and procedural interoperability. Standardised interfaces, protocols and approaches to cyber and electromagnetic battlespace management that allow information exchange across joint forces, allies, Government and industry partners will improve integration and foster adaptability.

3.9. CEMA battlespace execution is likely to require a command and control approach emphasising centralised control but decentralised execution, where execution authority is delegated to the point of best understanding for decision-making. As well as integrating our own offensive actions, we must be able to mitigate the threat from adversaries' cyber or electromagnetic weapons while also preventing fratricide to and from friendly or neutral systems. The volume of digital and electromagnetic data, its complexity and the tempo at which the situation can change will require that some cyber and electromagnetic battlespace management systems will have to be dynamically managed by automation; human response rates will be too slow. Such automation should be domain and function agnostic to minimise coordination issues and maximise responsiveness.

CEMA specialists

3.10. Operations and planning teams must have sufficient expertise to ensure that CEMA is fully integrated into all joint action activities across all domains. This needs cyber specialists, electronic warfare, communications and EME management specialists, plus intelligence analysts.

3.11. Finding the balance between centralised specialist cadres and specialists integrated into generalist headquarters will require continuous refinement. Our Whole Force approach must examine the balance of regular, reserve, civilian and contractor personnel. No single solution will be optimal and we must be flexible to meet the challenge of acquiring expertise. What we must secure is sufficient regular specialists that can respond at very high readiness. These specialists will also support Defence's ability to retain sufficient expertise to act as an intelligent customer where we contract for capability.

ARCHIVED

CEMA education, training and experimentation

3.12. Defence must instil life-long education opportunities for all personnel to ensure that CEMA is well understood by all staff and not just specialists. Education must focus on how military operations can leverage CEMA and essential operational security practices. Training must include the practical applications, advantages and threats of CEMA and not be too focused on the technical details that are the preserve of the specialist cadre.

3.13. Our exercises must be realistic and robustly test our forces' defensive and offensive capabilities. We must be capable of degraded cyberspace and EME operations, adapting quickly to reversionary modes. Realistic training must include security against third parties collecting cyber or EME data on our forces and the challenges of electronic warfare or offensive cyber systems causing fratricide to civil systems. This will drive synthetic cyber and EME training systems.

3.14. Exercising CEMA will provide the vehicle to experiment and drive technical and doctrinal interoperability into the joint force and with our allies and with other government agencies. Increasingly, commercial off-the-shelf solutions will often be the most time and cost effective solutions, leaving military-only systems to be developed for the most critical or sensitive capabilities, typically where security vulnerabilities are at their greatest. The rate of evolution of commercial off-the-shelf technologies will remain high and every exercise will be an opportunity to experiment, supporting 'fail fast' learning approaches and rapid capability integration where advantage is identified.

CEMA resilience

3.15. In addition to emission control, we could exploit tunable metamaterial structures to enable platform surfaces to absorb and/or reflect electromagnetic energy for the desired stealth characteristics. This signature reduction should be complemented with passive or low-power active countermeasures to mask a platform, or to create more attractive false targets. This is pertinent to expeditionary forces that cannot compete with high-power active sensors and countermeasures due to the power limitations of deployable combat platforms.

3.16. Low probability of detection emissions, disguised equipment signatures and non-characteristic patterns of emission or cyber activity could further protect capabilities. This is not purely defensive; effective signature management will force our opponents into active search modes, increasing their own exposure to detection and attack.

3.17. Reversionary modes of operation, including passive sensors and minimising vulnerabilities arising from dependencies on the Global Positioning System (GPS) and other space derived services, would increase resilience; an important component of adaptability. We must also harden some systems against electronic warfare or cyber attack and seek to minimise or eliminate single points of failure. We must better understand the risks of using cloud-based technology; information architecture that underpins decision support, with critical information maintained in readily accessible locations and over trusted communication bearers. This may require a revision of the approach to distributing information across third-party data centres.

CHIVED

We must also harden some systems against electronic warfare or cyber attack and seek to minimise or eliminate single points of failure

3.18. The numerical increase and cost reduction of automated unmanned systems and novel weapons should allow deception using sacrificial platforms. Digital electronics, such as reprogrammable radar systems, will allow waveforms to be adapted more rapidly so that they do not appear in threat libraries. Cognitive electronic warfare technology could respond to new waveforms in real time by classifying the previously unknown signals and then generating jamming signals through machine-learning tools.[21] Our communication systems will also need to use adaptive and machine cognitive techniques to defend against the adversary threat whilst optimising our capabilities in the EME.

3.19. In a permissive environment we should fully exploit reachback and virtual headquarters. In an austere, contested environment we may need to reduce dependency on the EME. We must design reversionary modes that mitigate against degraded or denied EME and then practise and test regularly. Over reliance on technology to underpin command and control is an important potential weakness. If we are more resilient to this threat than our opponent we can create advantage, degrading the EME to a point where we can operate, while they cannot. This is not just technological; mission command will remain an essential reversionary mode for degraded EME operations.

3.20. Cyber lacks the norms and protocols – legal, behavioural and moral – that underpin the rules-based approach in the maritime, land and air domains. It is critical that we develop and understand these norms, nationally and alongside allies, to employ effective cyber capabilities. Whether, and if so how, deterrence can be achieved in the cyber domain remains a matter of debate.

ARCHIVED

Cyber domain – key deductions and insights

The following are considered priority areas for future force development.

- Securing access to specialist cyber skills, both within and external to Defence, whilst developing our own broader cyber awareness to improve security, resilience and better employment of cyber and electromagnetic capabilities.
- Developing cyber and electromagnetic battlespace management to enable agile command and control, information exchange, and joint force integration.
- Building cyber and electromagnetic resilience through adaptive systems, reversionary modes, better understanding of risk, training and education.
- Developing and understanding, nationally and through international partners, acceptable norms and protocols to employ effective cyber capabilities.

[21] Cognitive electronic warfare systems enter into an environment not knowing anything about adversarial systems, they identify and understand them through machine learning and devise countermeasures rapidly if required.

Section 2 – The space domain

3.21. Space has become pivotal in delivering services upon which much of the global economy depends. It enables critical national infrastructure and is recognised as a critical infrastructure itself. From a military perspective, we are currently reliant upon the accurate timing and navigation, communications and ISR provided by space services. This reliance is understood by potential adversaries; several actors are developing means to exploit the vulnerability of space systems and so degrade our space-enabled capabilities. Space, like cyber, lacks and therefore needs the norms and protocols of acceptable behaviour that exist elsewhere; actors' intents are susceptible to misinterpretation. This compounds the difficulty in delivering a deterrent strategy in a domain where future crises are likely to extend. Not only must we deliver security from space, but we must also assure the security of space. This challenge is compounded by high growth in the commercial space sector and the dual use of many space systems.

3.22. Space is becoming more accessible. Small satellites are being developed whose capabilities are increasing as their costs are reducing. The industrialisation of small satellite manufacture which has led to the advent of mega-constellations and the development of reusable launch systems promise to further reduce cost. Technologies will allow rendezvous and proximity operations which can enable on-orbit satellite refuelling, servicing and construction, and debris removal. Other developments include space tourism, asteroid mining and hypersonic transport. The growing trend in commercial leadership, private sector provision of government services and cheaper access will lead to space activity becoming normalised. This will present opportunities and threats.

CHIVED

© Airbus

The proposed OneWeb small satellite constellation of more than 700 communications satellites in low Earth orbit

Space situational awareness

3.23. Space situational awareness encompasses our understanding of the intent of potential adversaries, the domain, and our ability to analyse trends to forecast the future disposition and capabilities of spacecraft, the trajectories of space objects, and space weather. It enables all other space roles and is a requirement for successful space operations. In addition to the anticipated increase in space activity, there are several hundreds of thousands of pieces of space debris orbiting the Earth, which pose a danger to operational spacecraft. Safe operations need improved tracking and characterisation. This is performed by a global network of Earth- and space-based sensors. The United States will increase the number of objects it can track by a factor of ten when its 'Space Fence' becomes operational from 2018.[22] The cost of surveillance and tracking largely prevents it being comprehensively achieved by any individual nation; the UK should develop capabilities in collaboration with key allies to maximise its own and collective space situational awareness.

Space support to operations

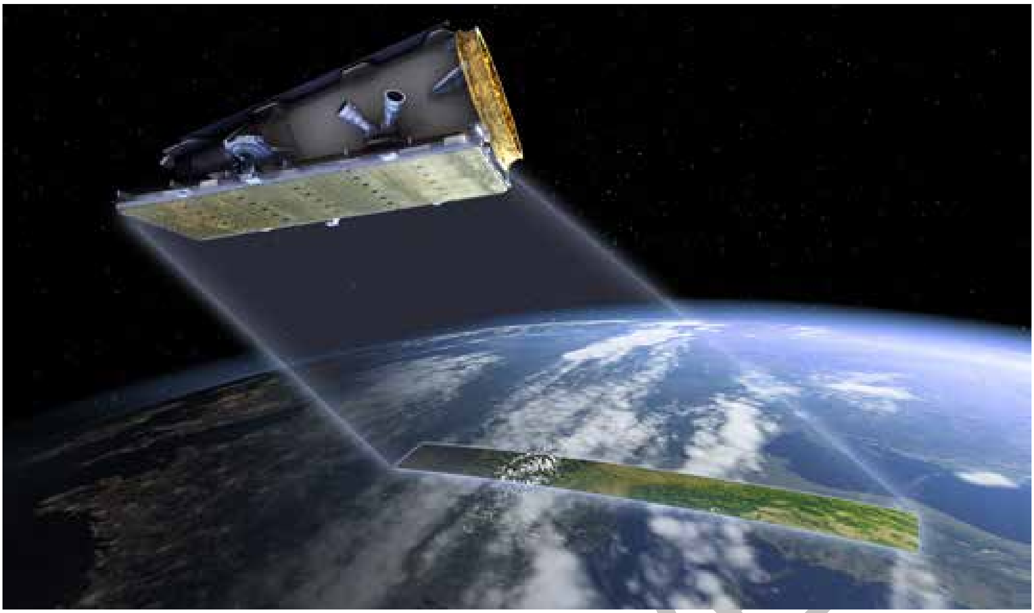
3.24. Space support to operations comprises essential joint force services from, through and to space. These include: ISR; missile warning; environmental monitoring; satellite communications; and position, navigation and timing (PNT). Fundamental to modern warfare, we must improve the resilience of these relatively vulnerable dual use capabilities. ISR capability would benefit from redundancy and a mix of sensors and spacecraft. Low Earth orbit will continue to host the majority of surveillance platforms, however, technology is developing that may permit high-resolution images from higher orbit. High altitude pseudo-satellites that blur the boundary between air and space are likely to provide an effective contribution to an air/space manned/unmanned mix of capabilities. Accurate weather forecasting, a basic requirement for military operations, will continue to rely heavily on space-derived information.

3.25. Satellite communications and space surveillance, including transmission of full motion video, will increasingly be transmitted to aircraft, ships, land platforms and even individual man-portable receivers. Satellites and high altitude pseudo-satellites offer the potential for line of sight communication relay using hard-to-jam free-space lasers. Some resilience can be introduced into position, navigation and timing services by using multiple providers, for example, GPS and Galileo,[23] but resilience must also be designed into equipment from the outset and consider whether an alternative position, navigation and timing source is required.

We must instil greater space awareness across Defence, as well as taking measures to ensure the availability of specialist knowledge.

ARCHIVED

[22] The United States expects to be able to track up to 200,000 objects of five centimetres diameter or greater.
[23] Galileo is Europe's global navigation satellite system that will provide a highly accurate, guaranteed global positioning service under civilian control.



© Surrey Satellite Technology

NovaSAR: a small radar satellite – regardless of daylight or weather conditions, a constellation of three such satellites can image any point on the globe every day

3.26. Those conducting campaign design must understand the accuracy, availability and resilience of these capabilities and factor them into planning from the outset. We must incorporate a space estimate into our processes and synchronise space activity with that conducted in the cyber, maritime, land and air domains. Space, as with cyber, faces challenges in acquiring and maintaining access to expertise in the face of heavy demand and limited supply. We must instil greater space awareness across Defence, as well as taking measures to ensure the availability of specialist knowledge.

ARCHIVE

Space service support

3.27. Space service support includes spacelift, satellite operations and the reconstitution of space capabilities. Commercial developments in affordable reusable launch technologies including space planes, combined with small satellites, offer the potential for a UK launch capability. Military access to this would foster greater flexibility and resilience in providing space services. It would also contribute to the nation's prosperity. UK launches could be conducted from the proposed UK spaceports, but to optimise payloads and orbits other commercial launch sites may also be used. We could exploit the opportunity afforded by the low mass and volume of small satellites to use the residual space on rockets carrying large primary satellites.

3.28. More varied and cheaper launch opportunities will allow the UK and coalition partners to be more responsive to demands for space capabilities. Disposable tactical satellites could maintain low Earth orbit for the duration of an operation, satisfying a previously unfulfilled need for Earth observation or communications above a specific geographic region. Responsive launch could extend to more permanent spacecraft and contribute to space capabilities' reconstitution. Rendezvous and proximity operations could further enhance responsiveness by allowing satellites to be reconfigured, re-roled and technically updated on-orbit. It could also be used to assemble structures that would otherwise be too large to launch from Earth. This may lead to greater capabilities on-orbit; for example, larger mirrors or sensor arrays to enhance Earth observation.

3.29. Suitably qualified and experienced personnel will be essential to aid our understanding of space and develop a wider space domain awareness needed across all components of the joint force. However, shared civil-military space operations centres with security safeguards offer high potential value. Commercial partners might manage the telemetry, tracking and control functions with military practitioners focusing on operations. The UK is in a good position to build intellectual leadership in space capabilities through its unique place as a member of: the Combined Space Operations initiative; NATO; and through its experience on European projects such as Galileo.

Space control

3.30. Space control supports friendly forces' freedom of action in space. It relies on robust space situational awareness. Miniaturisation combined with stealth will likely make it more challenging to understand the purpose of potential adversaries' spacecraft. We should collaborate with allies to develop improved radar, and radar-independent, tracking methods. The latter might include laser and coherent infrared sensors and the deployment of rendezvous and proximity operations-capable sensor satellites to help determine target satellite purpose. Rendezvous and proximity operations, and debris removal technologies present a threat to our space capabilities. They could be used to position adversary spacecraft close enough to disable or destroy friendly capabilities, offering the advantage of a soft kill that need not contribute to space debris. We must be able to command, control and manoeuvre military and civilian spacecraft to respond to on-orbit threats. Mindful of our treaty obligations, the need to protect our space capabilities may require us to exercise offensive, as well as defensive, space control. Such operations can be conducted from all domains – cyber, space, maritime, land and air. The concept of space support to operations, effects from, through, and to space, may need amendment to cover effects in space, including cyber. As with cyber, the lack of norms and protocols inhibits our ability to deliver credible deterrence in space.

Opportunities and threats

3.31. The increasing availability of launch options will allow us to replace malfunctioning or disabled space assets responsively. Commercial, high-resolution surveillance data will augment dedicated military capability. Joint force operations will be supported by commercially available encrypted communications. Costs could be reduced by hosting military payloads – sensors, communications or other equipment – on satellites owned by allies and/or commercial operators. This will provide value for money and contribute to resilience through disaggregation and dispersal. However, some commercial operators may not be comfortable supporting a military enterprise as it may render their spacecraft a

ARCHIVED

target. The targeting of dual use systems can present legal difficulties over the distinction between civil and military purpose, and an associated uncertainty of intent which may give rise to mistrust and increase the possibility of conflict.

3.32. Capabilities will become increasingly available to non-state actors and may increase the likelihood of irresponsible or criminal behaviour in the domain. Space will become increasingly congested, and competition will increase for the most advantageous orbits and use of the electromagnetic spectrum, heightening the risk of collision and electromagnetic interference. Protecting space capabilities and, more critically, the safety of increasing numbers of humans expected in space, will drive greater regulation; more complex launch and on-orbit operational procedures and some form of automated space traffic management, where spacecraft communicate with each other on a machine-to-machine basis. Civil rather than military agencies are likely to govern this. Commercial space services may be available to potential opponents. Adversaries' use of commercial communications networks will complicate our efforts to disrupt command and control; their access to ISR products will mean that by 2035 there will be fewer gaps in surveillance – almost continuous overhead observation will have implications for our own security. Maximising our space situational awareness will become increasingly important. Space systems are digitised and vulnerable to cyber attack. Wide access to cyber capabilities will provide the opportunity for even small belligerent governments, terrorist groups and individuals to instigate high-impact attacks.

ARCHIVED

Space domain – key deductions and insights

The following are considered priority areas for future force development.

- Securing access to specialist space skills, both within and external to Defence, whilst developing our own broader space awareness to improve security and resilience as well as better employment of space capabilities.

- Exploiting commercial capacity and capabilities wherever possible.

- Building resilience in our space-based and space-derived services.

- Developing space situational awareness capabilities with key allies with the ability to perform combined command and control of spacecraft.

- Developing and understanding, nationally and through international partners, acceptable norms and protocols within the space domain to promote order.

Section 3 – The maritime domain

3.33. Maritime forces are configured to exert influence in and from the maritime domain, in the air above and into the littoral. In their contribution to joint action, maritime forces will support land and air forces with cross-domain logistic support, ISR and power projection as part of a full spectrum approach. The maritime domain is similarly subject to actions from all other domains.

3.34. There will be considerable expansion in the global use of the seas and a commensurate increase in the number of maritime-capable actors, above, on and increasingly below the water. We will not always have the advantage but being prepared to fight for joint force freedom of action against an increasing array of adversaries, threats and challenges is at the heart of future maritime force design. States and non-states (particularly large corporations and business) are expected to keep pursuing maritime strategies to garner resources. Prolonged interruption of maritime transportation networks therefore risks undermining a state's prosperity and the welfare of its people, emphasising the importance of the maritime domain beyond its physical bounds. Potentially hostile actors could target areas of strategic importance to the UK, challenging maritime security and freedom of navigation, destabilising the free flow of global traffic. International chokepoints will remain crucial to the free flow of trade and energy security. Protecting transportation links, energy infrastructure and contributing to regional stability will remain vital maritime tasks.

Future implications for the roles of maritime forces

3.35. The strategic context confirms that the roles of maritime forces; war fighting (including the delivery and protection of the continuous at sea deterrent (CASD)), maritime security and Defence Engagement,[24] are likely to endure and be interrelated. Maritime forces require the versatility to conduct them concurrently or consecutively.

War fighting

3.36. The ability to fight underwrites the credibility of maritime security and Defence Engagement and should continue to be the primary role. Future maritime forces should be able to project power at and from the sea through proven methods, including: electronic warfare; direct and indirect fire support; land and surface attack; and air, amphibious and Special Forces operations involving the transfer of combat power from the sea to the land. By 2035 current capabilities could be augmented by: directed energy (laser and microwave) weaponry; directional acoustic weapons; rail guns; hypersonic surface and land attack missiles; and armed remote and automated systems.

3.37. The challenge of establishing time and space-bounded sea control will continue due to the proliferation of advanced weapon and sensor capabilities. This may allow adversaries to oppose access and disrupt maritime operations, particularly in the littoral and at strategic

ARCHIVED

[24] Defence Engagement is defined as: the means by which we use our Defence assets and activities, short of combat operations, to achieve influence. Joint Doctrine Publication (JDP) 04, *Understanding and Decision-making*, 2nd Edition.

chokepoints. Methods will range from, but not be limited to, cyber and information warfare through to the more traditional elements of sea denial (mines, submarines, anti-ship ballistic missiles and swarm attacks). We will thus require the ability to project power at range to counter anti-access threats. Assured force protection capabilities will form an important mitigation to anti-access and area denial (A2AD) risks, including ballistic missile defence.

3.38. Future maritime task group operations will provide political and military options including: deterrence or reassurance prior to a crisis developing; forward presence free from political commitment to intervene; and a scalable range of intervention capabilities and command and control centred on Carrier Enabled Power Projection. The future maritime task group should be capable of delivering a joint, sea-based military force able to operate globally. Future maritime task groups will operate routinely in a multinational context; primarily with NATO. These will range from working alongside strike and amphibious task groups, to fully integrated operations demanding higher levels of interoperability, such as with the United States Navy and United States Marine Corps.

ED

The future maritime task group should be capable of delivering a joint, sea-based military force able to operate globally

3.39. A maritime task group configured for amphibious and land-focused operations should be prepared to conduct and command/direct, at the appropriate level, theatre entry and shaping operations delivering a simultaneous surface and air assault, in support of both concentrated and dispersed operations. The requirement for amphibious forces to secure land points of entry is expected to endure. It could be in coalition with allies, from the waterfront, an inland objective, or a well-found port for follow-on forces. Such operations are likely to exploit air, surface and sub-surface remote and automated systems. Complex threats to the maritime task group will drive the requirement for increased operating ranges for ship to objective manoeuvre connectors. Increasing coastal urbanisation and prevalence of population concentrations around water will require amphibious forces to operate from the sea to estuaries, lakes, rivers and canals.

3.40. Logistic support remains an essential element of maritime task group operations. Defence will require logistic support that is globally responsive, and that exploits joint and multinational capabilities, host-nation support and commercial solutions. It should deliver optimised in-theatre support and sustainment to the maritime task group, using novel technologies and in-place manufacture.

Prolonged interruption of maritime transportation networks therefore risks undermining a state's prosperity and the welfare of its people, emphasising the importance of the maritime domain beyond its physical bounds.

ARCHIVED

3.41. Submarine platforms will likely proliferate, including for commercial use, and developments in their capability are expected to foster increasingly versatile and challenging adversaries. The proliferation of sensor, acoustic database, weapon and processing technologies, coupled with wider understanding of the significance of signature management may mean that emerging platforms will have capabilities similar to our own. Rapidly emerging and highly capable remote and automated systems, nanotechnology and static sensors are likely to be increasingly prevalent in sub-surface operating systems. Unmanned underwater vehicles will provide persistence through renewable energy generation. The majority are expected to operate in the shallows and the contested littoral; however, larger platforms will be capable of operations to the ocean floor. These systems will link with manned platforms using remote command and control nodes to detect, identify and classify potential threats early, at range, and before an adversary can bring offensive weapons to bear. Integrating these systems could provide persistent layered detection, tracking and attack options. The primary detection method is likely to remain acoustic, but non-acoustic and multi-spectral methods will increasingly aid detection, classification and tracking.

3.42. The expected advances in underwater sensing and proliferation of platforms will provide challenges for future underwater operations, but are unlikely to make the oceans transparent to sensors in the period to 2035. The sheer physical volume of the ocean and the challenges of providing persistent wide area search with the required performance, accuracy and coordination mean that underwater vehicles will still rely on stealth to avoid detection. By design and operation underwater vehicles, from continuous at sea deterrence to smaller, bespoke systems, will nonetheless have to work increasingly hard to remain undetected, as maritime and air anti-submarine warfare forces have better capabilities at their disposal. Underwater vehicles may require additional defensive systems and an ability to act offensively if compromised.

Maritime security

3.43. The blurring of UK and overseas threats may lead to increasing challenges in waters that are vulnerable and accessible to actors with maritime capabilities. Future maritime forces are expected to continue playing an important security role in protecting UK national interests, including protecting key maritime infrastructure, our territorial waters, exclusive economic zone and Overseas Territories and international chokepoints. The UK Government is a signatory to multinational treaties and agreements, which promote cooperation in interdicting vessels on the high seas. Future maritime forces can expect to deploy military and law enforcement personnel at range to provide upstream prevention. Integrating military and law enforcement capabilities offers a force multiplier against common threats to national security. With more frequent natural disasters likely to have the most significant impact on littoral areas, maritime forces must be sufficiently adaptable to conduct humanitarian assistance and disaster relief operations as part of a multi-agency response, including providing security, command and control, essential life support, medical and logistical capabilities.

Defence Engagement

3.44. Defence Engagement by maritime forces will strengthen partnerships and provide strategic intelligence. It will support other roles such as maritime security, by encouraging nations to invest in protective security, maritime surveillance and interdiction capabilities, and the legal structures to enable effective policing of their maritime zones. Engagement activity will include exercises with forces of other countries, training and capacity building activities, port visits and a wide range of diplomatic and commercial functions.

ARCHIVED

Future platform design and systems

3.45. Maritime platforms are typically designed with long-life spans, often up to 50 years, which provides a return on investment and a durable capability, but risks obsolescence in a fast-changing world. Procurement needs to be faster, responsive and more agile. Future maritime platform design requires through-life innovation and adaptability to exploit and integrate emerging technologies, in a timely and cost-effective manner, to anticipate and respond to new threats, roles and tasks. Platforms will need to be more agile in employment and our processes sufficiently responsive to refine capabilities swiftly and affordably. Systems should use an open architecture approach and provide sufficient physical space for the addition of new weapons, ISR systems and future additive manufacturing capabilities. We must strike a better balance between sufficient quality and quantity of future combatants to provide better resilience in the face of attrition, including the balance between manned and unmanned systems and platforms.

3.46. Adversaries will use novel weapons against maritime forces and platforms should provide protection, redundancy and resistance to advanced directed energy and chemical, biological, radiological and nuclear weapons, as well as multiple low-tech systems. Survivability could be improved through: markedly increased speed, allied to emerging hull technologies and construction methods; signature and profile reduction; air-cushion or wing-in-ground effect technology; and more varied use of remote and automated systems. This will be especially significant against underwater threats, including intelligent mines and quieter submarines. Maritime platforms of small to medium scale should operate manned, minimally manned or unoccupied, especially for dirty, dull, deep and dangerous missions, capitalising on advances in the automation of fire suppression, flood control and other manpower-intensive tasks. This would allow commanders to assess manning and logistic options, based on threat, intensity and the nature of the task.

3.47. Advanced maritime power generation and energy technology could enable high-power sensors, rail guns and directed energy weapons to be incorporated into maritime platforms. High power lasers have the potential to recharge platforms and sensors, operating at range and in hazardous or hostile areas. Advances in battery, solar power, fuel cell, ultra-capacitors and hybrid power units will find increasing utility in niche roles. Capabilities are expected to benefit both manned and remote and automated systems while potentially reducing logistic burdens.

3.48. Quantum technologies promise a big increase in processing power and speed. This could bring rapid developments, challenges and opportunities for secure communications, signals analysis and precision timing.

IVED

Unmanned systems will transform maritime operations, from ISR, targeting and attack to search and rescue and disaster relief

3.49. Maritime platforms have the ability to exploit future weapon technology. Long-range, silo and carousel launched, precision, loiter, multi-role systems and emerging energy weapons, optimised for a range of targets, point the way ahead for fires projection, fire support and force protection. Maritime-based weapon systems, including rail guns, intelligent projectiles and weaponised remote and automated systems could be linked to next-generation aircraft and networked remote and automated systems for cueing, targeting and attack. This would allow long-range and precision strike of targets in a contested and congested battlespace. By 2035, remote and automated systems are expected to contribute to a much wider range of tasks, including maritime force projection, maritime security, information operations and conventional war fighting. They will be deployable from air, shore, surface and sub-surface vessels, commercial and other marine infrastructure. They could contribute to operations either individually or in networks of systems, controlled remotely or acting independently within pre-defined parameters.

3.50. Maritime ISR functions are expected to be performed within the currently identified optimum electromagnetic bands; this constraint will require strong and resilient networks. Significant development is expected in terms of multi-spectral sensing, sensor fusion and miniaturisation. Sensors are expected to become cheap, widely available and valued by a wider range of actors, presenting maritime forces with an operational security and counter-surveillance challenge.

VED

Maritime domain – key deductions and insights

The following are considered priority areas for future force development.

- Seizing technological opportunities. Identifying, developing and operationalising key technologies, in particular remote and automated systems, that will enhance operational capability.

- Operating effectively in contested and degraded environments, through cross-domain integration, information exploitation, agile command and control, freedom of action and reversionary modes.

- Developing adaptable platforms and systems, including communications, weapons and sensors, to provide capability longevity, through open architecture, configurable through-life to adapt to new technologies and roles.

- Better balancing quality and quantity to provide resilience in the face of attrition, (including the manned and unmanned balance), to meet the challenges of reconstitution for war fighting at scale.

- Adopting novel and responsive logistic support solutions to assure sustainment and resilience.

Section 4 – The land domain

3.51. The land domain cannot be considered in isolation and land forces both support and are supported by actions in and from the cyber, space, maritime and air domains. Effective integration across domains, and within the land domain is vital for effective action. This section considers the implications on each of the functions of land power – fight, engage, secure and support. These are not discrete categories as activities frequently overlap different functions.

Fight

3.52. The core function of land forces is to succeed in combat; this underpins all other functions. New challenges will arise from the broad availability of what were once uniquely Western advantages, for example: long-range precision weapons; massed sensor systems; and long-range reconnaissance capabilities such as unmanned aircraft systems (UAS) and satellite access. In spite of technological advances in detection ranges and firepower, the complexities of terrain, populations and enemy strategies mean that combat will frequently remain a close, personal and visceral affair. The need for a soldier to close with and kill the enemy is an enduring requirement; building and maintaining a combat ethos will therefore remain vital.

3.53. Land forces will need to operate efficiently as dispersed elements to achieve multiple points of presence and to mitigate the threat of massed weapon effects while ready for rapid concentration for decisive effect.[25] Dispersion is enabled by mission command and competence in low-level leadership and tactics. It is also dependent upon robust communications networks and situational awareness. Dispersion will not always be possible; the requirement to protect critical installations or populations will preclude dispersion from physical threats and land forces will still require the resilience to hold ground against the enemy. Dispersed forces are also more difficult to sustain. Effective concentration is dependent upon timely understanding, unity of effort, mobility and assured command and control. Achieving effective concentration in conflict will not simply refer to physical forces, but an ability to integrate activity and effects in and across all domains.

3.54. We must be capable of the reach, sustainment and mobility required to both conduct opposed theatre entry and manoeuvre to the optimum location to achieve influence in contested environments; potentially operating, however undesirable, without assured air support and with limited connectivity. Our forces will seek to avoid detection and deceive opponents through manoeuvre, cyber deception, operational security and emission control. Land forces must be capable of protecting themselves from the plethora of threats that our adversaries may field. This will require counter-remote and automated systems, air defence and long-range attack systems. In conjunction with other partners, land forces must innovate to use layered area and point defences, including ground based air defence, unmanned systems, defensive aid suites, physical resilience, tactical cyber and electronic warfare capabilities.

[25] As an example, the damage sustained by concentrated Ukrainian forces caught by massed rocket artillery strikes has led to significant efforts by Ukrainian forces to disperse and conceal their forces for protection.

ARCHIVED

3.55. Whilst insufficient on its own, air-land integration will be essential. The increase in small UAS in particular will blur the boundaries of what have been traditionally considered distinct air or land activities.[26] This will need dynamic coordination of assets; swarms of small UAS controlled by soldiers must integrate effectively with aircraft and UAS piloted by airmen, sailors, contractors and allies. There is likely to be an increased requirement to project power from the land into the air. Land forces may support air actions with ISR, remote and automated systems, tactical CEMA, fires for suppression of enemy air defence and ground-based air defence systems. Similarly, land forces may be required to enable maritime power by facilitating freedom of manoeuvre in the littoral by securing maritime forces from land-based threats. Land forces will also project power into the maritime domain through ISR, cyber, electromagnetic and lethal effects to support maritime manoeuvre.

3.56. The advantages of human augmentation, described in Part 2, may create profound opportunities in land warfare. In addition, developments in medical and sports sciences will provide benefits for the physical ability to conduct dismounted close combat. Improvements in aptitude testing, especially in low-cost synthetic environment training, will enable improved streaming of personnel. The ability to operate advanced fighting vehicles will require visuospatial aptitudes and the ability to coordinate swarms of unmanned systems will require tactical and battle management skills.

HIVED

© iStock.com/zabelin

Technology will allow augmentation of military skills

[26] As a hypothetical example, the use of micro-unmanned aircraft systems (micro-UAS) like Black Hornet to reconnoitre urban terrain by infantry soldiers would rightly be thought of as a land domain focused concern. The same micro-UAS deployed (without modification) in large numbers in a swarm in the flight path of aircraft would rightly be thought of as an air domain focused concern.

3.57. Enemy capabilities may threaten lines of communication and compel logistic and medical concentrations to be held at distance. This must not limit our ability to project force. Our forces must be capable of functioning in austere conditions with limited support. Fundamental to our ability to tailor support under such constraints will be our ability to improve our use of timely and assured information; anticipating and reducing demand while increasing efficiency and the supply velocity to the point of need.

Our forces must be capable of functioning in austere conditions with limited support.

3.58. Significant commercial investment in logistic technologies will offer opportunities to exploit commercial innovations, including unmanned delivery systems, stock prediction and tracking systems. The use of health and usage monitoring systems (HUMS), and tele-repair will allow rear-based experts to provide assurance and advice to forward elements.[27] Other commercially developed technologies will enable greater flexibility in our sustainment networks, potentially improving our ability to modularise, repair, scavenge or re-use material. Analysis suggests that additive manufacturing could make 70% of the frequently demanded line items for wheeled vehicles and 30% of all deployed items with a 24-hour turnaround in theatre. However, this has its own logistic burden of material and power. The effects of enemy capabilities and distance are also likely to mandate prolonged field care before evacuation. This requirement may also demand novel medical capability solutions to support land manoeuvre, such as far forward or in-transit surgery.

Engage

3.59. While Defence Engagement can be undertaken by any deployable land force element, personnel specialised for arduous capacity building tasks with expertise in training, linguistic and cultural capabilities and optimised for integrating with other nations' forces will be more effective and offer increased opportunity to engage. The ability of such forces, with the resilience to survive in austere conditions and operate at reach could also support planning for theatre entry. As we cannot impose capacity building on partners, to optimise our ability to influence we should identify core competencies and technical specialist capabilities in high demand from allies in regions of interest.

3.60. Our ability to understand new situations is often best supported by access to expertise – generated through investments in engagement – rather than simply our ability to interrogate recorded information from which we attempt to predict. Our human resource systems should enable effective recording and, subsequently, identification of the experiences individuals accrue throughout their careers. Understanding is also perishable; our career models and personnel management should maximise and reinforce training and experiences that generate deeper levels of understanding about regions, groups, cultures and technologies of interest to Defence.

ARCHIVED

[27] Health and usage monitoring systems (HUMS) monitor holdings, usage rates and damage, for example.

Secure

3.61. Only land forces can take and hold ground. While the physical control of ground may offer tactical advantage, it also has powerful psychological and political effects. The decision to deploy land forces can, and will continue to embody a powerful symbol of political will.

3.62. Multi-agency stabilisation operations will require land forces to provide security for other, predominantly civilian, actors. While information activities and cyber tools will offer increasingly compelling and individually-tailored ways to interact remotely with elements of populations, physical interactions between people will remain essential. Technologies such as real time translation will offer significant improvement, but in the near to medium term will not offer the understanding provided by human cultural and linguistic practitioners, especially for the nuances of language and stresses or abnormalities in a subject's speech and behaviour.

Support

3.63. Land forces' support to state and non-state institutions, both at home and overseas is likely to increase. Support will focus on providing military expertise and equipment and self-sufficient self-organising manpower at readiness and scale to respond to disasters. This will demand adaptability, assured and flexible command and control and effective integration and assurance through collaborative training with civil authorities and emergency services.

3.64. The vulnerability of the homeland to threats that are expanding in range and scope can only be mitigated by a genuinely integrated full spectrum approach. The range of threats to the UK increases the likelihood that a military response will be appropriate, and therefore the balance between structuring and equipping for expeditionary operations and the potential increased use of land forces in support of homeland security warrants consideration.

Urban operations

3.65. We will need to exploit the information and data systems being integrated into ever more populated, connected and complex cities. This will improve our understanding and enable targeted dynamic influence activity supported by advances in behavioural sciences. Quantum sensing, other non-invasive sensors and tactical cyber tools may improve our ability to detect and offer greater ISR options. The ability to use simple cyber tools for tactical effect and access to information, and tactical electronic warfare systems will be increasingly important; a platoon able to locate persons of interest or detect sudden movements of populations will gain new capabilities to sense their surroundings.

3.66. Within the urban environment the tasks of armour and air manoeuvre will remain, but how they are delivered will evolve. Combat and armoured engineers teamed with

ARCHIVED

unmanned systems will be key enablers to manoeuvre and counter-mobility in urban terrain. Quad-copter and small jet engine technology developments able to transport individuals may expand the range of systems available to land forces for vertical manoeuvre in constrained urban space.

3.67. Urban terrain is not uniform and will offer different challenges depending on its character. To succeed in urban operations our forces will require access to the different variety of urban terrain types to allow realistic training and experimentation. The use of augmented reality and virtual systems should support training to deal with the challenges representing the scale and complexity of urban operations.

© iStock.com/everlite

Urban terrain is not uniform and will offer different challenges depending on its character

Land domain – key deductions and insights

The following are considered priority areas for future force development.

- Developing interoperability to leverage the power of joint action through our alliances and partnerships.
- Operating effectively in contested and degraded environments, through cross-domain integration, information exploitation, agile command and control, freedom of action and reversionary modes.
- Improving and developing, visible, combined, joint, intra-governmental, inter-agency training and experimentation with a focus on urban-littoral environments.
- Creating flatter, faster, more resilient and agile command and control and battlespace management, enabling new ways of operating, including dispersal and rapid concentration, to enhance survivability.
- Better balancing quality and quantity to provide resilience in the face of attrition and to provide the combat mass (including examining the manned and unmanned balance) required to meet the challenges of future urban operations and reconstitution for war fighting at scale.
- Assuring force projection and sustainment, including adopting novel and responsive logistic support solutions to assure sustainment and resilience.

AR

Section 5 – The air domain

3.68. This section outlines how UK air forces may gain advantage by exploiting developments in automation, stealth, sensors and hypersonics. To outpace adversary decision-making, air forces must also exploit improvements in organisational design and connectivity to provide an agile air command and control capability. As technology advances, the air domain is likely to extend into near space[28] and we should seek to integrate the effects of multiple air platforms or single aircraft conducting one or more of the four air power roles simultaneously across multiple areas of responsibility. Future air command and control must also be more strongly nested within joint and inter-agency command and control networks. Figure 3.2 illustrates the future air power model.

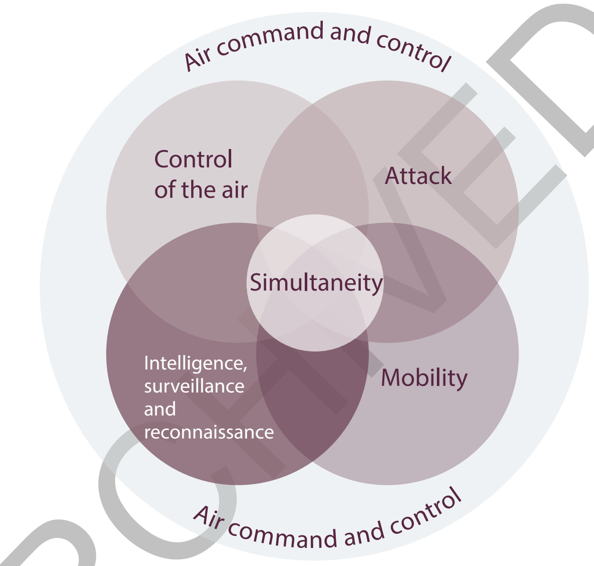


Figure 3.2 – The future air power model

ARCHIVED

Control of the air

3.69. Control of the air at specified times and places will remain an essential requirement to secure freedom of action at acceptable risk for the joint force. Joint forces must be prepared to fight for it, and with terrorist and criminal groups increasingly using UAS, control of the air may also require the participation of the civil authorities. The burgeoning air travel industry and the growing use of commercial and military UAS will make sensing, identifying and engaging future threats increasingly complex.

> Offensive counter-air will become more difficult as more actors gain access to sophisticated air defence capabilities...

[28] Near space is considered to be the volume of atmosphere contained between the altitudes of 100 kilometres, the Karman Line, and 20 kilometres, the current highest practical level for conventional aviation.

3.70. Offensive counter-air will become more difficult as more actors gain access to sophisticated air defence capabilities: passive sensing and low-band radar for detecting low observable aircraft; and advanced surface-to-air missiles and man-portable air defences. The destruction and suppression of enemy air defences will require integrating kinetic and non-kinetic attack from all domains.

3.71. Our defensive counter-air challenges will be compounded as potential adversaries develop hypersonic capabilities, ballistic and cruise missiles, stealth technologies, swarming tactics and large salvo attacks. Defeating these threats will require an integrated and robust layered air and missile defence capability. Sea- and land-based CEMA and fires will need to be synchronised with air systems through a command and control and surveillance network that draws on sensors from all domains. This might allow better allocation of scarce resources and automatic use of the most suitable systems; an efficacy through interdependence. Cheap, capable UAS foreshadow swarming attacks, which adversaries might employ with artificial intelligence to overwhelm existing defensive measures. To respond quickly enough to the complexity and speed of such tactics, we would likely need human-supervised, artificial intelligence control linked to a range of defences including electronic jamming, directed energy weapons, modified counter-rocket/artillery/mortar systems, nets, and/or swarms of our own UAS.

© Airbus

Persistent high altitude pseudo-satellites – the solar powered Zephyr remotely piloted air system flying in the stratosphere

3.72. Despite best efforts to protect air assets, including hardening and the use of camouflage, concealment and deception, attrition in combat is inevitable and we must strike the right balance between capability and mass for resilience. Resilience must extend to continuing control of the air when the EME is denied, for example, using rehearsed distributed command and control.

Intelligence, surveillance and reconnaissance

3.73. Speed and reach enhance air ISR timeliness and height brings a valuable perspective. Technology will allow long endurance air platforms to provide persistent surveillance across the EME. The merging of visible, near infrared, infrared and ultraviolet, radar sensing and signals intelligence could provide higher confidence in collected information and improve situational awareness.

3.74. Unmanned platforms such as high altitude pseudo-satellites and spacecraft offer a persistent wide-area surveillance capability. Equipped with the right sensor mix they can collect information day and night through poor weather. High altitude pseudo-satellites currently offer the advantage of being more readily upgradeable than their true-satellite counterparts and can be re-tasked to different geographic areas more easily. Helium balloons with their capacity for carrying heavy payloads may provide an alternative means of persistent surveillance, communications relay and global navigation satellite system augmentation. Unmanned hybrid air vehicles also offer a persistent capability, which could prove a cost-effective ISR asset in low risk operations.[29]

3.75. All air platforms have potential to be sensors and network nodes, rendering all aircraft ISR assets capable of two or more concurrent roles. To exploit our collection capabilities we must have access to sufficient bandwidth to accommodate the volume of data that will be produced. Whilst we must maintain sufficient focus on data collection, timely information processing and dissemination are equally important.

3.76. Tactical reconnaissance in contested domains may prove challenging. Incremental development of contemporary UAS may be insufficient to meet that challenge. To conduct such missions at a time and place of our choosing will likely need low observable or hypersonic systems.

Attack

3.77. Our capacity to attack from the air with rapid global reach and precision is critical to conventional deterrence and joint action. However, the proliferation of increasingly capable air defence systems is challenging our calculus for what constitutes effective safe stand-off range and our ability to hold adversaries at risk at distance. Advances in camouflage, concealment and deception and the increasing mobility of key adversary systems may challenge our ability to target effectively.

3.78. Geography and operational tempo may prevent basing our aircraft beyond the reach of adversary weapons. To mitigate risk, we could disperse our forces across many airfields and use sea basing or other operating surfaces, including motorways and highways. Hopping from one to another, each austere or well-founded option could provide a temporary operating location. These measures would compound adversary targeting

[29] These aircraft are termed hybrid because in addition to the aerostatic lift derived from the buoyancy of their helium lifting gas, they benefit from aerodynamic lift.

ARCHIVED

difficulties, but some would come with an increased logistic, training, connectivity and force protection challenge. Agile basing may require change to the organisational design and command and control of expeditionary air operations.

3.79. Hypersonic weapons, air or surface launched, offer the ability to reach further and achieve quicker results. They are difficult to intercept, because their speed and flight profile give little warning of their approach. Conventionally armed ballistic missiles also offer the advantages of speed and range; their trajectory, however, is indistinguishable from that of a nuclear ballistic missile and so their use must follow extensive consideration and effective strategic messaging. Mobile targets, and advanced camouflage, concealment and deception may constrain the range of target sets for which they are suitable pending capabilities that can update targeting information during missile flight.

3.80. Modern integrated air defence systems could create regions where many air platforms cannot penetrate and survive. Future generation aircraft may be less constrained by virtue of their low observable design and highly automated sensor functions. They can provide the capability to locally degrade an integrated air defence system, creating airspace in which other less protected systems may operate. To realise this, next generation and legacy types must share and receive information with each other and with networked weapons from all domains. Large aircraft could provide offensive capabilities as arsenal planes; their payloads could comprise hundreds of smart munitions delivered from distance.

ARCHIVED

3.81. The requirement for ever greater precision, distinction and proportionality will continue. Air attack integrated with maritime- and land-based fires can assist with scalable yield weapons and innovative payloads that mix explosives with electronic and cyber effects. In the event of unreliable access to global navigation satellite systems, developments in internal navigation using quantum technologies and other means of accurate timing may offer alternatives to assure precision and synchronisation.

3.82. The persistence and ability of unmanned systems to find, track and engage targets over extended periods and provide a high level of targeting assurance needs secure and resilient satellite communications. The current requirement for human control over the use of lethal force may affect their employability in a denied EME.[30] However, they may use automated modes to navigate the battlespace and evade adversary defences when communication is degraded. When links are re-established through satellite communications or another aircraft using free space optics they promise to offer significant advantage.[31] Low-observable, unmanned combat air vehicles would be able to operate in hostile airspace at higher levels of political risk. Equipped with artificial intelligence they could provide rapid, dynamic analysis of the disposition of enemy air defences and other targets, and engage them under human supervision. Hypersonic UAS could be used to identify potential threats early and at range.

[30] Current UK policy is that the operation of weapon systems will always be under human control. No planned systems are to have the capability to prosecute targets without involving a human.

[31] Free space optics: hard-to-jam data transmissions through air (or a vacuum) most commonly using some kind of visible or infrared laser.

© BAE Systems

Manned/unmanned teaming working across domains

ARCHIVED

Air mobility

3.83. Air mobility allows rapid military deployment to signal intent and reassure allies; our capacity to deliver combat forces quickly over distance is an important component of modern deterrence. It may be the only means to respond to terrorism or domestic threats that develop quickly in remote locations and is a key element of joint logistics and humanitarian assistance and disaster relief operations. While technological trends indicate the potential for sub-orbital hypersonic transport for rapid strategic deployment in the future, within this concept's time frame the more likely scenario would still require overflight permission and the use of friendly nation airfields for intermediate stops. Adversary coercion of host nations may deny such access and flight direct to forward operating areas could be required. This may force aircraft to operate at greater range, fly into and out of basic airfields that offer little support and survive in a non/semi-permissive environment.

3.84. Air-to-air refuelling may meet the requirement for operating at increased range, but will be in high demand from control of the air, ISR and attack missions. Improved fuel economy through advances in aviation fuel, engine efficiency and improved aerodynamics may mitigate this. Solar power is likely to find application in hybrid air vehicles. These aircraft, though slow, offer the potential to deliver large payloads over great distance at lower cost than fixed-wing heavy lift. They are also able to operate into unprepared fields with little ground support; airlift will be of greater utility if it is not overly reliant on specialist ground handling. To maintain the resupply tempo into basic airfields, all-weather approaches and departures independent of ground-based navigation aids will be required. In the event of a contested EME, they will also need to be independent of global navigation satellite systems.

3.85. Airlift and air-to-air refuelling operations in contested airspace will require threat mitigation. Avoidance through routing, suppression of enemy air defences, and stand-off precision air drop are options. However, air mobility aircraft may be exposed to some threats. Defensive aids, including lasers/directed energy weapons, should help assure survival. Developments in robotics, including gradual societal acceptance, may allow the evolution of highly automated and remotely piloted air mobility aircraft. They would be suited to high-risk missions such as joint personnel recovery and as air ambulances for evacuating the injured from the battlefield. Severely injured casualties will still require the attention of a critical care team, and the more conventional rotary-wing or tilt-rotor extraction with force protection. Beyond the field hospital, aeromedical evacuation on fixed-wing aircraft will be important to move the injured to more capable facilities. On-board care will be enhanced through access to electronic health records and telemedicine.

Defence Engagement

3.86. Reach and speed allow air forces to engage globally and, with sufficient priority, rapidly in response to emerging situations to project influence. UK air forces can also promote our prosperity through supporting the nation's military aviation exports as part of an integrated cross-government effort. The non-combat use of air forces develops understanding of other nations' defence perspectives, supports conflict prevention including deterrence, and builds partners capability and capacity in support of good governance and stability and also to enable interoperability with partners.

ED

Air domain – key deductions and insights

The following are considered priority areas for future force development.

- Operating effectively in contested, degraded environments. Delivering effects in contested and degraded operating environments through cross-domain integration, effective reversionary modes and appropriate mass.

- Better balancing quality and quantity to provide resilience in the face of attrition, (including the manned and unmanned balance), to meet the challenges of reconstitution for war fighting at scale.

- Seizing technological opportunities. Identifying, developing and operationalising key technologies that will enhance operational capability and operating concepts. In particular automated systems, non-kinetic weapons and technology that would enable persistent intelligence, surveillance and reconnaissance and the simultaneous execution of two or more air power roles by a single air platform.

- Delivering an agile air command and control capability that underpins the simultaneous execution of two or more air-power roles by single platforms across multiple areas of responsibility.

- Ensuring that legacy platforms are able to share and receive information with next generation aircraft and with networked weapons from all domains.

Part 4

Deductions and insights

4.1. The following deductions and insights are those judged most critical to guide strategic, joint and command force development. They offer the best prospect of making the joint force fit for the challenges of the future operating environment by exploiting information, being more integrated as a force and more adaptable to changing circumstances. Put simply, they are framed as questions and responses that Defence can ill afford to ignore.

! How do we rapidly develop and sustain the capabilities and skills to exploit the information environment?

4.2. Exploiting the information environment is critical to achieving influence. A greater understanding and focus on audiences (recognising that they are not bound by geography, are facing competing narratives and constantly evolve) will enable influence through enhanced joint action. The ability to gain insight, evaluate and measure underpins successful information activities.

! How can we deliver agile command and control, to offer decisive advantage in response to operational complexity?

4.3. The widespread adoption of resilient, open architecture and mission configurable systems would enhance integration and adaptability by better adapting mission command and the manouevrist approach to the highly contested information environment. Agile command and control will improve our operational gearing by allowing us more opportunities to keep strategy better connected to tactical actions in the fast moving events that characterise the information environment.

! How do we generate future mass effect?

4.4. In a future era of rising personnel and equipment costs, pragmatism will limit UK Defence spending to a capable force, but with less mass than we might desire. The future force will inevitably have insufficient capacity to deter some threats. Working with partners may in part offset our lack of mass, but we should determine the best balance between the quantity and quality of our capabilities. We are unlikely to retain the technological

ARCHIVED

edge that has sustained us in the past, but exquisite technology is not the only route to operational advantage. By building on and enhancing the core strength of our people through greater use of automation and the teaming of manned and automated systems we can offset relative lack of mass, deliver greater resilience, and provide more political choices. Such teaming also offers the prospect of reducing logistic demand, using our people more effectively and efficiently, and at lower risk.

! What must we do to promote and influence conceptual, physical and technical interoperability with partners, on a multilateral basis?

4.5. The prize will be both a safeguarded cornerstone to national security and the considerable financial efficiency that arises from sharing complex defence burdens. NATO remains the only credible response to the challenges of the future, because it has the mass of force and cultural diversity that might provide credible deterrence and collective defence; something that the UK cannot achieve alone. We need partners, but we also need to persuade our partners to adapt more quickly to the strategic environment. This means investing and leading in multilateral alliances like NATO, in preference to bilateral arrangements.

ARCHIVED

! Maintaining freedom of action within contested domains will require the integration of activity in all domains. How can we develop the understanding and skills to achieve this?

4.6. We should expect to operate within contested domains as the norm. Whilst all domains remain equally important, our relative start points for integrating across the domains as a joint force are not. In cyber and space particularly, we must focus extra effort to develop our understanding and awareness of our shortfalls and vulnerabilities. Failure to do so, and an inability to fully integrate all domains, will diminish our ability to overcome anti-access and area denial threats, and therefore limit our freedom of action.

! How will we secure access to the knowledge, skills, experience and talent to operate, innovate and adapt?

4.7. We are increasingly seeking talent in markets where demand significantly outstrips supply and our starting point lags well behind contemporary organisations. The increasingly demanding information environment, and space and cyber domains require us to be innovative in securing access to the skills to be able to project influence. Defence is not the poor relation, though; it has people and skills that industry values highly and constantly seeks to acquire. We should leverage and trade this commodity more imaginatively. We should also actively pursue an expanded and lifelong educational approach to build understanding and awareness. Whilst we are unlikely within existing arrangements to retain and maintain sufficient levels of skills and talent at readiness, we can and must provide a baseline requirement for access to enhanced capabilities. Stronger relationships with other organisations will both build resilience and enhance adaptability, whilst fostering creative thinking and innovation.

! How can we best prepare (training, experimentation and learning) to operate with joint, inter-agency and multinational elements, particularly in complex urban-littoral environments?

4.8. Training and experimentation is where Defence must continue to forge its fighting power in equipment, ideas and fighting spirit. We must encourage a stronger culture of constant training, experimentation and capability development by supporting and rewarding initiatives that challenge accepted wisdom and that accept occasional failure as the price of progress. More effective training environments, which exploit technology to offer greater challenge to our people and teams offer the prospect of increasing returns. Targeted and responsive training will enhance capability, interoperability and adaptability. The training environment offers the ideal opportunity to experiment, to push the boundaries and 'safe to fail.' It will in turn promote faster insertion of new capability, greater command confidence and enhanced fighting spirit.

! How can we best achieve rapid capability insertion?

4.9. Exploiting the increasing pace of technological change, particularly where the rate of development in the civil sector is high, will require a more institutionally agile acquisition system. This requires a culture of collaboration and the necessity to embrace modular approaches, spiral development and open standards and architectures.

! How do we deliver and assure the resilience of the future force for both expeditionary operations and, increasingly, in support of homeland security?

4.10. The resilience of the future force across the range of operations from expeditionary to those in support of homeland security will depend on organisational and individual flexibility. Achieving the optimal balance between frequently conflicting demands will both test our support mechanisms and require hard choices on prioritisation as the strategic environment evolves. Innovation, greater automation and creative thinking, bolstered by well-prepared reversionary modes of operation will sustain our freedom of action. Legality, legitimacy and public support will become increasingly important. So too will robust sustainment and the ability to quickly replace and grow both capacity and capability.

ARCHIVED

ARCHIVED

Lexicon

Part 1 – Acronyms and abbreviations

A2AD	anti-access and area denial
AAP	Allied administrative publication
C2	command and control
CASD	continuous at sea deterrent
CEMA	cyber and electromagnetic activities
COED	*Concise Oxford English Dictionary*
CONOPs	concept of operations
DCDC	Development, Concepts and Doctrine Centre
EME	electromagnetic environment
FFC	*Future Force Concept*
FOE	*Future Operating Environment*
GPS	Global Positioning System
GST	*Global Strategic Trends*
HUMS	health and usage monitoring systems
ISR	intelligence, surveillance and reconnaissance
JCN	joint concept note
JDN	joint doctrine note
JDP	joint doctrine publication
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
PNT	position, navigation and timing
SIE	single information environment
SMAC	social, mobility, analytics and cloud
UAS	unmanned aircraft systems

ARCHIVED

Part 2 – Terms and definitions

This section is divided into two areas. First, we list endorsed terms and their definitions. We then list terms and descriptions that may also be helpful to the reader.

Endorsed terms and definitions

artificial intelligence
The performance by computer systems of tasks normally requiring human intelligence, such as translation between languages. (COED)

cyberspace
An operating environment consisting of the interdependent network of digital technology infrastructures (including platforms, the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein spanning the physical, virtual and cognitive domains. (*Cyber Primer,* 2nd Edition)

Defence Engagement
The means by which we use our Defence assets and activities, short of combat operations, to achieve influence. (JDP 04)

electromagnetic environment
The totality of electromagnetic phenomena existing at a given location. (NATOTerm)

electromagnetic spectrum
The entire and orderly distribution of electromagnetic waves according to their frequency or wavelength.
Note. The electromagnetic spectrum includes radio waves, microwaves, heat radiation, visible light, ultraviolet radiation, x-rays, electromagnetic cosmic rays and gamma rays. (NATOTerm)

hybrid warfare
A form of warfare combining conventional and unconventional military and non-military actions to achieve a specific goal. (This definition is currently proposed and awaiting NATO agreement).

influence
The capacity to have an effect on the character or behaviour of someone or something, or the effect itself. (COED)

joint action
The deliberate use and orchestration of military capabilities and activities to affect an actor's will, understanding and capability, and the cohesion between them to achieve influence. (JDP 3-00)

ARCHIVED

littoral region
Coastal sea areas and that portion of the land which is susceptible to influence or support from the sea. (JDP 0-01.1)

manoeuvrist approach
An approach to operations in which shattering the enemy's overall cohesion and will to fight is paramount. It calls for an attitude of mind in which doing the unexpected, using initiative and seeking originality is combined with a ruthless determination to succeed. (JDP 01)

mission command
A style of command that seeks to convey understanding to subordinates about the intentions of the higher commander and their place within his plan, enabling them to carry out missions with the maximum freedom of action and appropriate resources. (JDP 01)

nanotechnology
Technology on an atomic or molecular scale, concerned with dimensions of less than 100 nanometres. (COED)

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

Other useful terms and descriptions

anti-access area denial
(A2AD)
By 2035, many of our potential adversaries will have capabilities designed to prevent our access to the maritime, air, land, space and cyber/electromagnetic domains. Defence will need to overcome the challenges of anti-access area denial, potentially fighting through to deliver the required effect. The range, resilience and survivability of our capabilities in every environment will become critical factors in maintaining access and our freedom of manoeuvre. (FOE 35)

ARCHIVED

domain
The sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects. (NATO MCM-0255-2015)

full spectrum approach
A full spectrum approach draws on a range of levers available to a state actor in a coordinated way to achieve (geo)political and strategic objectives. This can include overt and covert activities and the use of political, cultural, diplomatic, economic, military and other levers. The UK applies its levers of national power within the rules-based international system. (Her Majesty's Government, *Full Spectrum Approach Primer)*

ARCHIVED

information environment
An environment comprised of the information itself; the individuals, organisations and systems that receive, process and convey the information; and the cognitive, virtual and physical space in which this occurs. (AJP-3.10.1 – not NATO Agreed)

innovation
Innovation questions the routines and systems that underpin core competencies, which can deteriorate quickly without rigorous training, exercises and experience on operations. Innovation may be viewed as threatening existing capabilities in which militaries have made heavy investment and around which sub-community interests and cultures have developed. However, organisational innovation is crucial if we are to develop the capacity to anticipate and prepare for the future characteristics of conflict. (JDP 04)

military adaptation
Military adaptation involves incremental changes to tactics, techniques, procedures, structures and equipment to improve performance. (JDP 04)

organisational learning
Organisational learning requires tolerance of criticism (especially if it challenges routines, special interests and cultural norms), both internal and external. It involves codifying lessons into new or modified routines. Organisational learning should lead to adaptation and, if necessary, innovation. (JDP 04)

quantum technologies
A quantum computer is one that makes use of the quantum states of subatomic particles to store information.

remote and automated system
remote and automated system is a collective term, not confined to a particular domain, used to describe the remotely operated and/or automated system. Examples include unmanned underwater vehicles, unmanned surface vehicles, unmanned aircraft systems and unmanned ground systems.

resilient
Able to withstand or recover quickly from difficult conditions. (COED)
Example of resilience taken from JDP 02. Ability of the community, services, areas or infrastructure to detect, prevent, and, if necessary to withstand, handle and recover from disruptive challenges. (Cabinet Office, *Civil Protection Lexicon* Version 2.1.1, February 2013)

single information environment
A logical construct whereby assured information can pass unhindered from point of origin to point of need. The single information environment will incorporate a single intelligence environment. (Defence Information Strategy, 20 February 2017)

telexistence
Fundamentally a concept named for the general technology that enables a human to have a real-time sensation of being at a place other than where he or she actually exists, and being able to interact with the remote environment, which may be real, virtual, or a combination of both. It also refers to an advanced type of teleoperation system that enables an operator at the control to perform remote tasks dexterously with the feeling of existing in a surrogate robot working in a remote environment.

tunable metamaterial structures
A metamaterial is a material engineered to have a property that is not found in naturally occurring materials. A tunable metamaterial has a variable response to an incident electromagnetic wave and so can be engineered to respond to electromagnetic radiation in ways not normally found in nature.

understanding
In the context of decision-making, understanding is the perception and interpretation of a particular situation in order to provide the context, insight and foresight required for effective decision-making. (JDP 04)

Whole Force approach
The integrated approach is underpinned by our people – regular and reserve service personnel, MOD civil servants, contractors and other civilians. Working together, these different groups form the 'whole force' which delivers Defence outputs. Under the Whole Force approach, Defence places human capability at the heart of its decision-making and ensures that Defence outputs are delivered by the right mix of capable and motivated people now and in the future, and that people are managed as a strategic resource.
(JDP 0-01)

ARCHIVED

Designed by the Development, Concepts and Doctrine Centre
Crown copyright 7/17
Published by the Ministry of Defence

Corporate member of
Plain English Campaign
Committed to clearer
communication
235