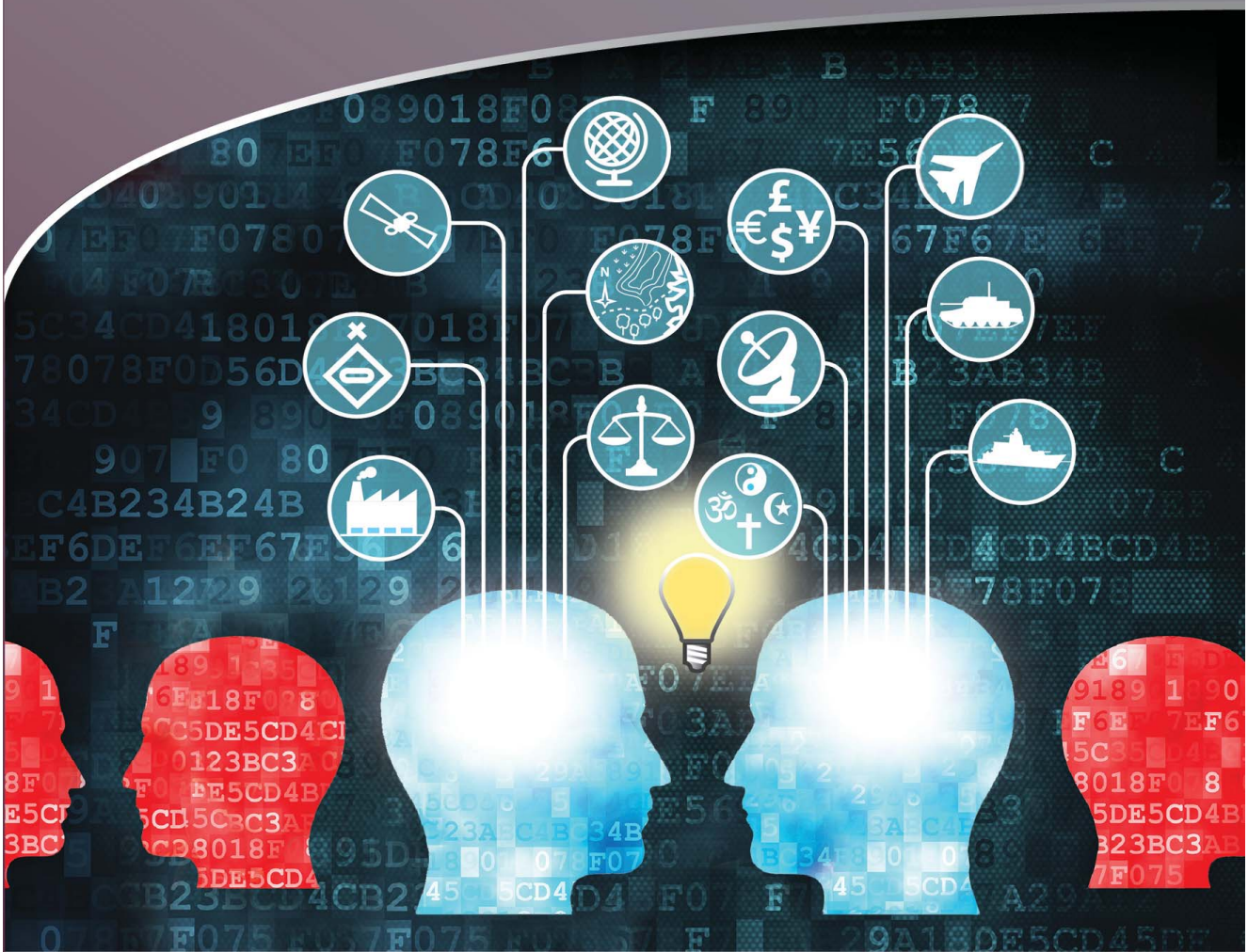
Ministry of Defence

Joint Doctrine Note 2/13

Information Superiority



Development, Concepts and Doctrine Centre

Joint Doctrine Note 2/13

Information Superiority

Joint Doctrine Note 2/13, (JDN 2/13), dated August 2013,
is promulgated
as directed by the Joint Forces Commander and Chiefs of Staff

Head of Doctrine, Air and Space

Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing Joint publications. If you would like to quote our publications as reference material in other work, you should confirm first with our doctrine editors whether the particular publication and amendment state remains authoritative. If you have any comments on the factual accuracy of this publication or would like to suggest an amendment, please contact our doctrine editors at:

The Development, Concepts and Doctrine Centre
Ministry of Defence, Shrivenham
SWINDON, Wiltshire, SN6 8RF
Telephone number: 01793 314216/7
Military network: 96161 4216/4217
Facsimile number: 01793 314232
Military network: 96161 4232
E-mail: DCDC-DocEds@mod.uk

Distribution

Distribution of Joint Doctrine Note (JDN) 2/13, *Information Superiority* is managed by the Forms and Publications Section, LCSLS Headquarters and Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP. Please contact them for further copies of this JDN or any of our publications.

LCSLS help desk: 01869 256052
Military network: 94240 2052

You can view and download the most up-to-date versions of all DCDC's publications (including drafts) at:
http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Organisations/Orgs/DCDC

This publication is also available on the Internet at:
www.gov.uk/development-concepts-and-doctrine-centre

Preface

Introduction

1. The challenges of gaining and using information within conflict situations have been with us since the earliest times – and information has always been critical to successful conflict outcomes. What has substantially altered is the quick way information is widely disseminated and accessed across the world, as well as the substantial increase in its volume and variety. Adding to this challenge is the implicit tension experienced in coalition operations between achieving interoperability and sustaining an information advantage. While some of these challenges will also be faced by our adversaries, the fact that entry costs are low, and cutting-edge technical capabilities can be adopted rapidly, means that they may be equally or better placed to employ information as a force multiplier. Defence must urgently address the issues as the situation is likely to get worse.

2. We should build on recent successes. In Afghanistan, we have recognised how fundamentally important information superiority is, and have improved our processes and practices. However, related doctrine has not kept pace. **There is no consensus across Defence as to what information superiority is, in its most fundamental form, nor is there a single well-understood and endorsed doctrinal definition**. If we are to mitigate the risk to future operations we must rectify this omission.[1] The doctrine should provide this consensus by explaining how to set the conditions so that information superiority can be achieved at anytime, anywhere. It should also indicate how it can then be employed to advantage in competitive situations. The doctrine must include aspects of ongoing information superiority activities relating to day-to-day contexts, such as at the home base or on standing tasks, as well as those aspects relating to specific operations.

[1] The C2 (command and control) Enablers Programme Board sat on the 15 February 2012. Here, the Defence Risk Tool, immature information superiority doctrine was given the Risk Identification Number 11865.

Context

3. Defence must shift its mindset to operate within the future operating environment.[2] Conventional military powers have traditionally been built around fixed processes and hierarchical structures that aim to provide military effect from environmental (maritime, land, air and space) stovepipes. We may need to adapt such structures to maintain their use when faced by decentralised, asymmetric and agile non-state actors, conventional adversaries or any combination of these. We are likely to put greater emphasis on open architectures, flattened organisational structures, mission command and decentralised control to achieve the desired effects. **A strategy of adapting to the changing external environment, rather than seeking to control it, is likely to be fundamental**. This is the context within which we must achieve information superiority.

Aim

4. Joint Doctrine Note (JDN) 2/13 *Information Superiority* aims to clarify the nature of information superiority and give guidance on how to enable, realise, employ and exploit it. We will consider how information superiority supports achieving understanding and how it enables commanders and staff to take, and communicate, effective decisions.

Purpose and scope

5. Given the shortfall in information superiority doctrine, the Development, Concepts and Doctrine Centre (DCDC) was tasked to draw together elements of existing doctrine and current best practice to produce a coherent document for commanders and their staffs. This JDN augments Chapter 3, Section VII of Joint Doctrine Publication (JDP) 04 *Understanding*.

6. Extensive commentary on drafts of this JDN has identified continued and strongly-held diverging views. This document attempts to capture the widest range of views in a coherent manner, but readers should note that the principles and concepts expressed are not yet wholly agreed. This JDN

[2] The Development Concept and Doctrine Centre (DCDC)'s Strategic Trends Programme, *Global Strategic Trends – Out to 2040* (4th edition) suggests that the future threat environment will be contested, congested, cluttered, connected and constrained.

sets a baseline for information superiority within UK Defence from which subsequent debate can be founded.

Audience

7. This publication is aimed at military commanders and staffs (J1-9) at the strategic (MOD), operational (Permanent Joint Headquarters) and higher tactical (component) levels. It should also inform staff and planners working in other government departments who may provide critical information superiority interdependencies. Finally, this JDN should further inform military and civilian staff who are developing related doctrine and procuring future capability.

Structure

8. This JDN is in three chapters with an annex.

- Chapter 1 describes the fundamentals, characteristics and principles of information superiority.
- Chapter 2 describes how information superiority can be enabled.
- Chapter 3 explains how to exploit information superiority.
- Annex A introduces a joint tactics, techniques and procedures (JTTP) hosted online. It introduces developing guidance on information superiority practice.

Linkages

9. This JDN is designed to accompany our joint military strategic doctrine, Joint Doctrine Publication (JDP) 0-01 *British Defence Doctrine* (4th edition) and its immediate family of keystone publications of:

- JDP 01 *Campaigning*, (2nd edition);
- JDP 04 *Understanding*;
- JDP 2-00 *Understanding and Intelligence Support to Joint Operations*, (3rd edition, change 1);
- JDP 3-00 *Campaign Execution*, (3rd edition);

- JDP 4-00 *Logistics for Joint Operations,* (3rd edition);
- JDP 5-00 *Campaign Planning*, (2nd edition, change 2); and
- JDP 6-00 *Communications and Information Systems Support to Joint Operations*, (3rd edition).

10. Additional guidance is contained in:

- JDN 1/12 *Strategic Communication: The Defence Contribution*;
- JDN 3/12 *Cyber Operations: The Defence Contribution*;
- JDN 3/11 *Decision-making and Problem Solving*;
- JDN 4/11 *Integration of Cyber Activities into Military Operations*; and
- JDN 1/10 *Intelligence and Understanding*.

11. Related publications include:

- Books of Reference Doctrine 7747, *Maritime Information Superiority Policy and Guidance*;
- Joint Service Publication (JSP) 747, *Information Management Policy*;
- JSP 747, *Information Management Policy and Protocols*;
- JSP 777, *Network-enabled Capability*;
- Ministry of Defence (MOD) Information Strategy 2011; and
- Multinational Interoperability Council, *Coalition Building Guide* (2nd edition, 2011).

Contents

Joint doctrine publications

The successful conduct of military operations requires an intellectually rigorous, clearly articulated and empirically-based framework of understanding. This gives our Armed Forces, and its likely partners, an advantage when managing conflict. Doctrine provides this common basis of understanding.

The UK adopts NATO doctrine wherever it is practically possible to do so. There are occasions when we need to develop our own national doctrine and endorsed national doctrine is published formally as Joint Doctrine Publications (JDPs). Urgent requirements for doctrine are addressed through Joint Doctrine Notes (JDNs). These notes are not subject to the same rigorous staffing processes as JDPs, particularly in terms of formal external approval. JDNs seek to capture and disseminate best practice or articulate doctrinal solutions which can subsequently be developed as more formal doctrine. Alternatively, a JDN may be issued to place some doctrinal markers in the sand, around which subsequent debate can centre.

Chapter 1 – Information superiority fundamentals, characteristics and principles

'What is called foreknowledge cannot be elicited from spirits or gods, nor by analogy with past events, nor from calculations. It must be obtained from men who know the enemy situation.'

Sun Tzu

Chapter 1 clarifies the basic nature of information superiority and proposes a new definition for information superiority in the military context. We explain the key characteristics of information superiority which, along with the principles, underpin the rest of the publication.

Section 1 – Fundamentals

101. Information superiority is a term that is increasingly used both inside and outside Defence. Yet, there is no clear consensus on what the term means, nor is there a common appreciation of its nature.

102. **Definition.** In this Joint Doctrine Note (JDN), we promote the view that information superiority is much more than just managing information. It is a dynamic state which arises from the behaviours of the 'complex of actors'[1] in operational situations. If achieved, information superiority is a vital enabler of intelligence and understanding in pursuing effective decision-making leading to decisive actions and force protection. Based on research and recent operational experience, we propose information superiority is defined as:

the competitive advantage gained through the continuous, directed and adaptive employment of relevant information principles, capabilities and behaviours.

[1] This complex of actors may include: multinational forces; the indigenous populations; media; diplomats; other governments departments from UK and other nations; international organisations; non-governmental organisations; private military, security and multinational companies and opportunists. Joint Doctrine Publication (JDP) 01 *Campaigning*, 2nd edition.

Commanders should note that information superiority:

- must be command-led;
- is a competitive activity which is situation-dependent;
- changes over time and requires ongoing activity to be sustained;
- is relative to other actors; and
- requires the ability to appropriately adapt ways-of-working to match changing situations.

Information superiority perceptions

103. Figure 1.1 shows the broad range of perceptions about information superiority. We divide these perceptions into two groups, the **conventional** and the **adaptive** views.[2] These views cannot be seen as 'right or wrong' – they reflect different concerns and contexts. The task for commanders is to ensure that these contributions are integrated to enable information superiority.

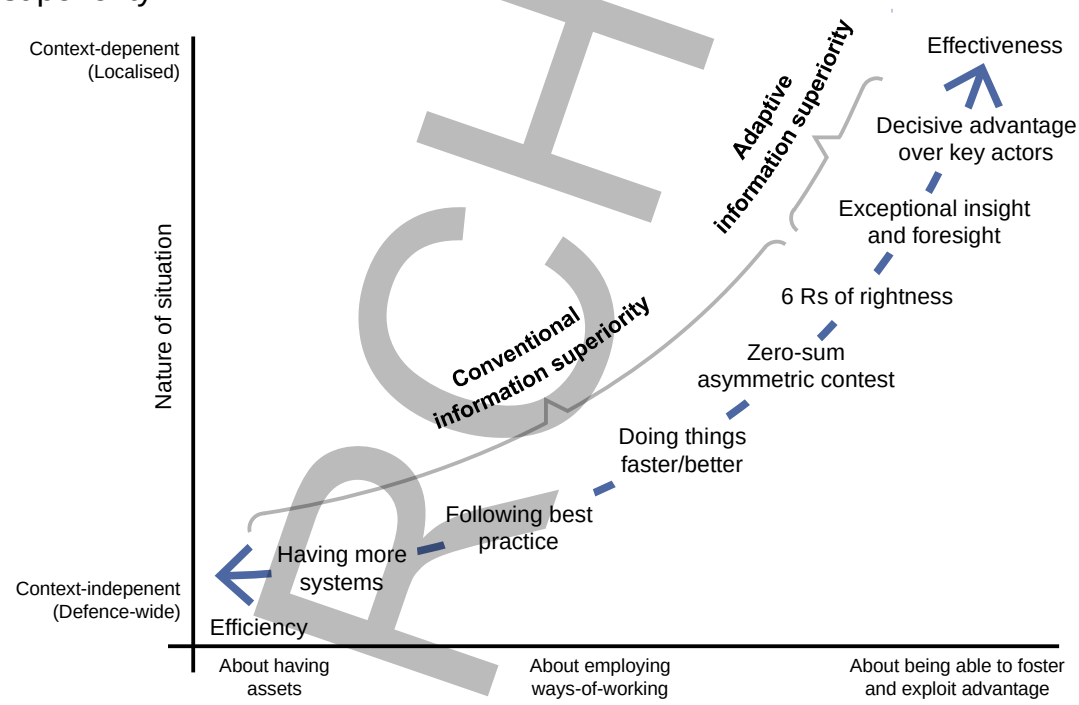


Figure 1.1 – A range of perceptions of information superiority

[2] See JDP 2-00, *Understanding and Intelligence Support to Joint Operations* (3rd edition), page 1-6, paragraphs 111a/b.

104. **Conventional views.** These conventional views see information superiority in terms of the enablers which set the conditions for it, rather than in terms of the ways it can be exploited operationally. This is insufficient for the adaptive information superiority needed by forces in an adversarial context – particularly given the contemporary scenario of dynamically changing situations and rapidly moving technologies. Conventional views are more concerned with our own efficiency, such as, '… managing, in relative terms, information flows better than your adversary …'.[3] This view sees information superiority as something that, once achieved, applies across Defence.[4]

a. The conventional view is that information superiority is achieved by having more information and communication technology. This is often a critical part of what enables information superiority, but simply having lots of these assets does not guarantee information superiority.

b. The conventional view is that information superiority is about following best practice.[5] Following well-defined procedures and processes can contribute to information superiority, but is insufficient on their own. While procedures and processes are required, they must be appropriately responsive to the operational needs of commanders and staffs. Adversaries who have no need to follow procedures will be more agile.

c. The conventional view is that information superiority is achieved simply by working better and faster. Working at an unnecessarily high tempo can exhaust resources. We need the ability to adapt our ways-of-working to the prevailing circumstances rather than working in the same way all the time.

d. The conventional view is that information superiority is like air superiority. Air superiority is a 'zero-sum game', where if we gain the advantage then an adversary must have lost it. Information is not a finite resource like airspace or land, that can be owned exclusively.[6]

[3] See JDP 3-00, *Campaign Execution*, (3rd edition, change 1), page 4-9.
[4] For example, it is appropriate for logistics staffs just to employ the principles in the MoD *Information Strategy*, 2011.
[5] Best practice: such as in Joint Service Publication (JSP) 747, *Information Management Policy and Protocols*, or the 2013 *Defence Operating Model*.
[6] To illustrate that information is not a finite resources think of this example. When you share an apple, you get half each. When you share information you both get everything and when you give information away you still have it.

Absolute information superiority, through exclusive ownership of information, cannot be achieved in modern conflicts except in special cases.

e. The conventional view is that information superiority is achieved by delivering the right information, to the right person, at the right time to make the right decision, which brings about the right effect leading to the right outcome (the six Rs of rightness). Good shared awareness does not automatically mean that commanders have information superiority. In reality, this chain is unachievable because what will be right in each case cannot be identified in advance. Circumstances will determine that at the time – so adaptation must occur. Without that, a chain of events of this sort will be disrupted by adversaries and by unforeseen consequences.

105. **Adaptive views.** The adaptive view takes a situation-dependent and operations-focussed approach to information superiority and how to exploit it.

a. Adaptive information superiority is about developing insight and foresight – usually campaign-specific. This arises from the ability to collaborate and make sense of specific situations from distributed perspectives, especially by adapting the diverse insights from *ad hoc* communities of interest as needed.[7] This is a largely non-technical approach for achieving local, tactical information superiority with potentially global effect.

b. Adaptive information superiority is about gaining decisive advantage over other actors. It depends partly on the ability of commanders to direct, cue and employ their information resources to augment their decision-making.[8] It is also achieved by manipulating adversaries' perceptions.[9] The value of this 'soft' information superiority, which influences actors' behaviours, should not be underestimated. In the 'battle of narratives' commanders must consider influencing not only adversaries, but also other actors, those

[7] For example, see Major General Michael T Flynn's *Blueprint for making intelligence relevant in Afghanistan*, 2010.
[8] As stated on page 80 of the Multinational Interoperability Council's *Coalition Building Guide*, 2nd edition, 2011, 'Competitive advantages from shaping the information environment can become a major factor for mission success'.
[9] See the example on page 366 of Major General Rupert Smith's book, *Utility of Force*, 2005.

who shape public opinion, and the wider public (for example, using social media).

106. The success of adaptive information superiority depends on the ability of commanders to:

- set the conditions for success (discussed in Chapter 2); and
- take advantage of the unforeseen operational asymmetries available in specific contexts (covered in Chapter 3).

In summary, **information superiority is not achieved simply by having technical systems – though they are enablers which help set the conditions for success. It is achieved by commanders who have cunning, insight and strong will along with the confidence to employ new information skills**. Such commanders can exploit all their resources to the full to gain advantage. The success of information superiority, in supporting understanding, is evident in the extent to which commanders can make their decisions with the confidence that their actions will be decisive.

Section 2 – Enduring characteristics

107. The characteristics of information superiority are enduring, relevant to any situation and commanders and staff should exploit them to have effect.[10]

	Key characteristics
Command led	Information superiority does not arise merely by having the appropriate capabilities and procedures in place. Commanders should develop their situation-dependent strategies for achieving information superiority over other actors and prioritise such strategies.

[10] Characteristic: A feature or quality typical of a person, place, or thing. Concise Oxford English Dictionary (COED), 12th edition, 2011.

Key characteristics (continued)	
Competitive	Continuous effort is required to achieve and maintain information superiority. Information superiority is not absolute and will degrade over time. It can also be actively degraded by the information activity of our adversaries and diminished by our own actions.
Comparative	Information superiority exists only when there is some degree of advantageous difference of insight and foresight between ourselves and others. As asymmetries and knowledge change, then so does the degree of information superiority achieved. The changes may be triggered by our own actions, by those of third parties, or by wider effects, such as weather events.
Context dependent	The way that information superiority is achieved is unique for every situation and relative to every set of actors. Although templates for achieving information superiority may be available (based on the principles below) they must be adapted to fit the circumstances.
Changes over time	Information superiority is a dynamically changing state that arises from the adaptive behaviours of people and their use of information systems over time. The degree and nature of information superiority is always in flux, there is no final goal and no end-state. Similar to cyber, the capabilities upon which information superiority is built are continually evolving along with innovations in technology. Therefore, the ways we achieve information superiority in the future will change.

Section 3 – Principles

108. When the enduring characteristics are applied in some adversarial situation, then commanders and staffs should note the following principles below.[11]

109. **Principle 1 – Information superiority is more than just about denying your adversary information.** It is almost impossible to prevent our adversaries from accessing information. Commanders may wish to do the inverse and provide adversaries with information to make them aware of the futility of their position, deceive them or make them dependent on its availability.

110. **Principle 2 – Information superiority involves risk and trade-offs.** The degree of information superiority held will be difficult to assess. This is because information superiority is relative, transitory, subjective, largely intangible and highly context- and personality-dependent. Expending effort to try to know what may be unknowable in advance may be distracting. Commanders must be prepared to proceed, accepting that the situation may become clearer in time. A valid strategy to break an impasse is to take action to trigger a revealing response from other actors. Given changing opportunities and threats there will always be a degree of interpretation and improvisation required by those involved and therefore a degree of risk. To wait for certainty is not an option when faced with the kind of deep uncertainty that might lead to strategic shock. Instead commanders must apply their judgement and experience to move from risk to opportunity.

111. **Principle 3 – Information superiority is a state that supports effective decision-making.** Figure 1.2 shows the position of information superiority in relation to intelligence, understanding and decision-making. Information superiority is their enabler in that it provides the information advantage needed to make effective decisions. It is not a capability in its own right. Information superiority itself can only be achieved when commanders can direct the manner in which information systems are configured and deployed (the two down-pointing arrows, discussed in Chapter 2). Having the ability to employ and adapt information superiority enables commanders to change their understanding and decision-making as operational

[11] Principle: a fundamental truth or proposition serving as the foundation for belief or action. COED, 12th edition, 2011.

imperatives evolve (covered in Chapter 3). It is easier to know when you do not have information superiority than when you do. For example, when commanders notice that they cannot obtain sufficient information to make timely decisions, then it is evident that they do not have information superiority.

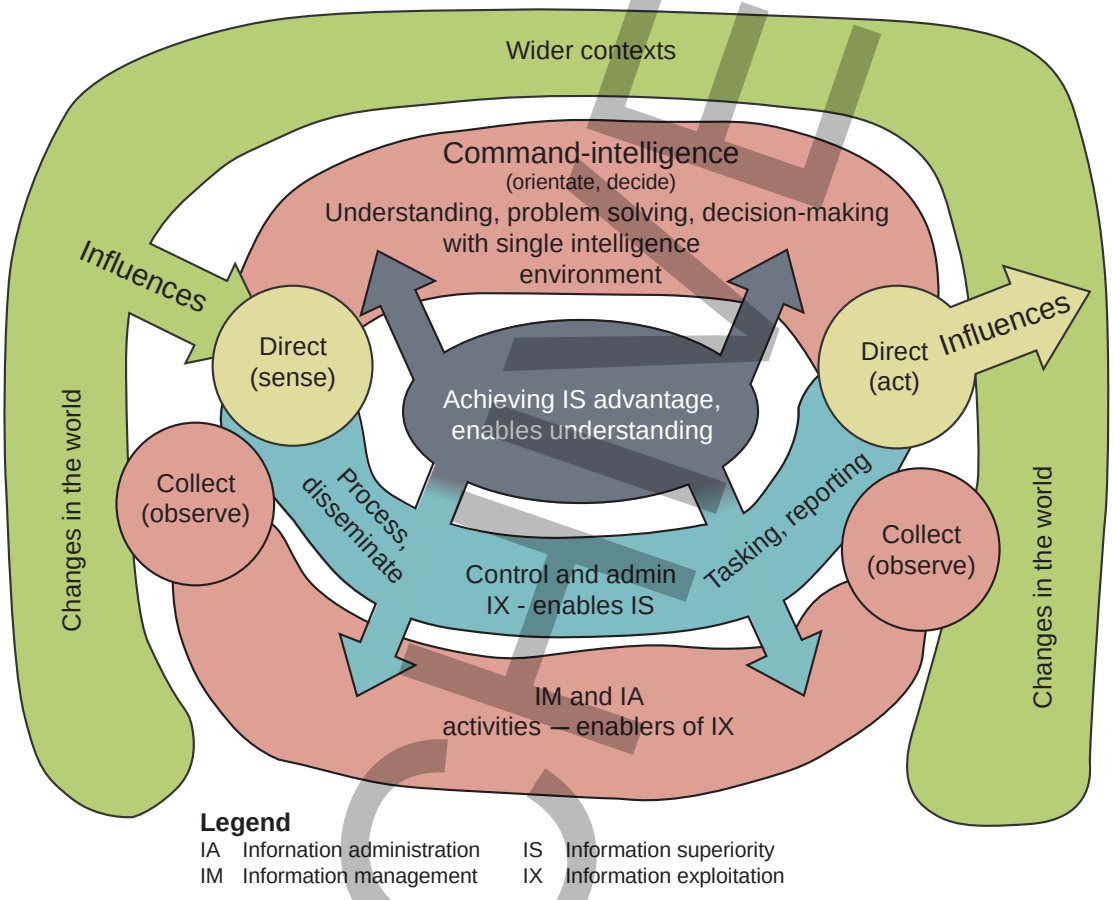


Figure 1.2 – Information superiority in relation to other themes

112. **Principle 4 – Information superiority has environmental aspects.** Some information superiority advantage can come from exploiting geographically-based information differences. This includes the ability to reach across time, space and all environments.[12] To reach across time, for example, commanders must be able to exploit historical records effectively.

[12] The operating environments are: maritime, land, air and space, information (including cyberspace), and electromagnetic. JDP 01 *Campaigning*, 2nd edition.

Analysis of these records can be useful indicators of future intentions and so enable information superiority.

113. **Principle 5 – The character of information superiority changes.** Information superiority has always been present in conflict, but it is not the same now as it was, or as it will be. In the future, information superiority will not only be about increasingly rapid changes in technology; the human dimension will always be a dominant factor. To maintain advantage commanders will need to adjust information superiority strategies and update them as circumstances change.

114. **Principle 6 – The degree of information superiority that can be attained can be influenced directly or indirectly.** Information superiority is an intangible aspect of conflict (like morale). However, it can be adjusted in various ways to change the relative advantage among the actors in the situation. Most circumstances will require direct or indirect influence to change information superiority, noting that other actors and the wider circumstances will also wield influence. Commanders must appreciate these complex linkages and effects (many of which may remain hidden) on their own information superiority. How commanders go about influencing the degree and level of information superiority achieved is covered in Chapter 3.

115. **Principle 7 – Information superiority is about relative advantage.** This advantage can be: relative to other actors; relative to our ability to meet the demands or imperatives of the situation; and affected by the degree to which actors are able to assess these relative advantages.

Notes:

Chapter 2 – Enabling information superiority

'The most successful people in life are generally those who have the best information.'

Benjamin Disraeli, 1804-1881

Chapter 2 explains how to set the conditions for achieving information superiority. It outlines the information superiority estimate and covers the challenges, required capabilities, risks, vulnerabilities and mitigations.

Section 1 – Setting the conditions for information superiority

201. Chapter 1 shows that information superiority does not arise spontaneously. Commanders and their planning staff must set the conditions so that information superiority can be attained, sustained and exploited throughout operations. In setting the conditions, commanders should note that information superiority-related activities will continue – regardless of whether there is an operation or not. Setting the conditions involves designing (planning) and deploying (configuring) capabilities. These are iterative as part of standing tasks, as well as being part of preparing for operations. The advantages of information superiority are then realised where forces adapt to, and shape the realities of, competitive situations (discussed in Chapter 3).

Developing and adapting the information superiority estimate

202. Commanders must achieve information superiority both on a day-to-day basis and in relation to specific operations. They should appreciate how the organisation should look, and behave, to achieve advantage in a current or future context by:

- better understanding threats;
- improving resilience; and
- integrating the perspectives of all decision-makers in contested situations.

This involves commanders considering: in-garrison training and preparation; pre-deployment planning; adaptive execution once deployed; recovery post-operation; and sustained review of the conditions for sustaining information superiority when home-based. These considerations are discussed in more detail below.

a. **Pre-deployment.** Commanders should ensure that they identify the:

- range of information superiority advantages to be achieved;
- base level of understanding that is available;
- enablers to deploy and activate (including assessing the need for information superiority contingencies and mitigations, to deal with shortfalls); and
- policies to shape the enablers to make sure that the necessary flexibility and agility is achieved.

b. **During the deployment.** Commanders should decide how they are going to monitor the degree and nature of information superiority advantage. They should also decide how it is to be adapted or adjusted locally.

c. **Post-deployment.** Measures must be put in place for managed run-down as part of recovery. Appropriate archiving and updating of joint tactics, techniques and procedures will also be necessary.

d. **At the home base.** Commanders should ensure that the levels of excellence in information behaviours achieved on operations are applied in the home base. For example, the possibility of cyber-attacks is always present so personnel should continue to work to sustain information superiority. Commanders should also determine the requirements to retain/maintain information gathered on operations to improve the base level of information to inform future decisions.

203. **Information superiority estimate.** The information superiority estimate is introduced in Annex A. Commanders should judge which organisations, authorities and responsibilities will provide the best chance of

achieving information superiority. Above all, from the estimate, **commanders must develop an integrated directive which identifies the required information superiority enablers. This directive must link all relevant operational, human and technical aspects** and has to be supported by sufficient resources. There are several key elements which inform this process.

a. Commanders should **appreciate the level of the information superiority fight**. They should work out the levels and circumstances which may provide them, and other actors, with the most effective and advantageous information asymmetries over time. These asymmetries, which will change, should be considered as part of the information superiority estimate. In this estimate, clear intent allows effort to be focussed where it will have most leverage on information superiority. It should cover the:

- adversaries' requirement for information;
- adversaries' ability to gain information superiority;
- degree of dominance required over adversaries which will inform the levels of superiority required; and
- relevant indicators and measurement of effectiveness.

b. Commanders should reflect on their information needs given their intent and they, and their staffs, must be **clear about the types of information needed to support decision-making and collaboration** (using the mission thread approach introduced in Section 2 of Annex A). They must also make clear what information should be denied to adversaries or provided as part of deception or influence. This includes identifying our own critical information which must be protected and secured and why.[1]

c. Commanders and staffs **must be trained, confident and capable in information superiority**. Information superiority is undermined if they revert to apparently safe, risk-averse processes, rather than taking the initiative. Key enablers are:

[1] Additional guidance is available in Joint Doctrine Publication (JDP) 3-80.1 *OPSEC, Psychological Operations and Deception*.

- mental agility;
- contextual awareness; and
- understanding how to provide enhanced value to information consumers.

d. As part of the estimate, commanders and staffs should **determine measures of effectiveness**. As these measures are context-dependent we cannot specify them in detail here. Commanders must develop their own, context-specific, indicators and measures of success, and keep them updated.

e. Commanders also need to decide **which ways-of-working are appropriate** to the situation (conventional versus adaptive, see Joint Doctrine Publication (JDP) 2-00 *Understanding and Intelligence Support to Joint Operations*, page 1-6), and then direct their use.[2] This may involve deciding on the style or ethos that commanders wish their staffs to employ (for example, close-hold versus open access versus collaborative), and the degree to which ways-of-working are to be centralised or distributed.

f. Staffs should **assess contributions to or from coalition partners**, and the impacts any differences have on the way information superiority is employed and assessed. Working in coalitions may introduce constraints and opportunities and their effects must be factored into the estimate.

g. Staffs should **consider the impact of non-Defence contributions** to, and constraints on, military force information superiority. These include a wide range of potential influences, such as, the media, social networks and from potential leaks. For example, understanding how social media is being used and how it could be managed in the battlespace, will be important for staff and commanders.

h. Staffs should **ensure that the (technical) enablers meet the operational needs** and the challenges addressed. They will need to

[2] Where the nature of the situation may involve military support to crisis, humanitarian or disaster operations.

decide how to mitigate potential constraints in, for example, bandwidth and spectrum.

i. Staffs should **identify threats and counter them** by having reversionary modes ready to activate.

Information superiority can only be achieved when the information superiority estimate has been developed, the enablers put in place to set the conditions, challenges addressed, risks managed and vulnerabilities mitigated. Thereafter, the ability to adjust levels of information superiority over time should be developed. Finally, the ways of influencing information superiority should also be mastered.[3]

204. **Setting the conditions for information superiority – design aspects.** At its most basic, information superiority can be achieved by people using their intellect, will, judgement and ingenuity – without any technological support. However, in most situations, information systems will be used by commanders and their staffs. Adaptive information superiority is enabled by:[4]

- **competent, trained** personnel who can:
  - collaborate, share and use information effectively; and
  - adjust system behaviours and levels of interoperability;
- **effective** information collection, processing and exploitation;
- **appropriate levels** of information management;
- **reliable and efficient** information administration;
- **robust** information assurance and network defence; and
- **fast and intuitive tools and services**, such as effective indexing and searching and common operating pictures (introduced in Section 4 of Annex A).

The exact capabilities required depend on circumstances. Staffs must ensure they provide the appropriate network connectivity, power, bearers, redundancy and backup capabilities supporting reversionary modes.

[3] Described in Chapter 3.
[4] Enable: give (someone) the ability or means to do something or make it possible. Concise Oxford English Dictionary (COED), 12th edition, 2011.

Systems will also be required for intelligence, surveillance, reconnaissance, collection, processing, dissemination and visualisation.

205. Figure 2.1 can be used to assess the degree to which a force has its enablers in place. In essence, the bigger the hexagon, the greater the capabilities of the information superiority enablers. For example:

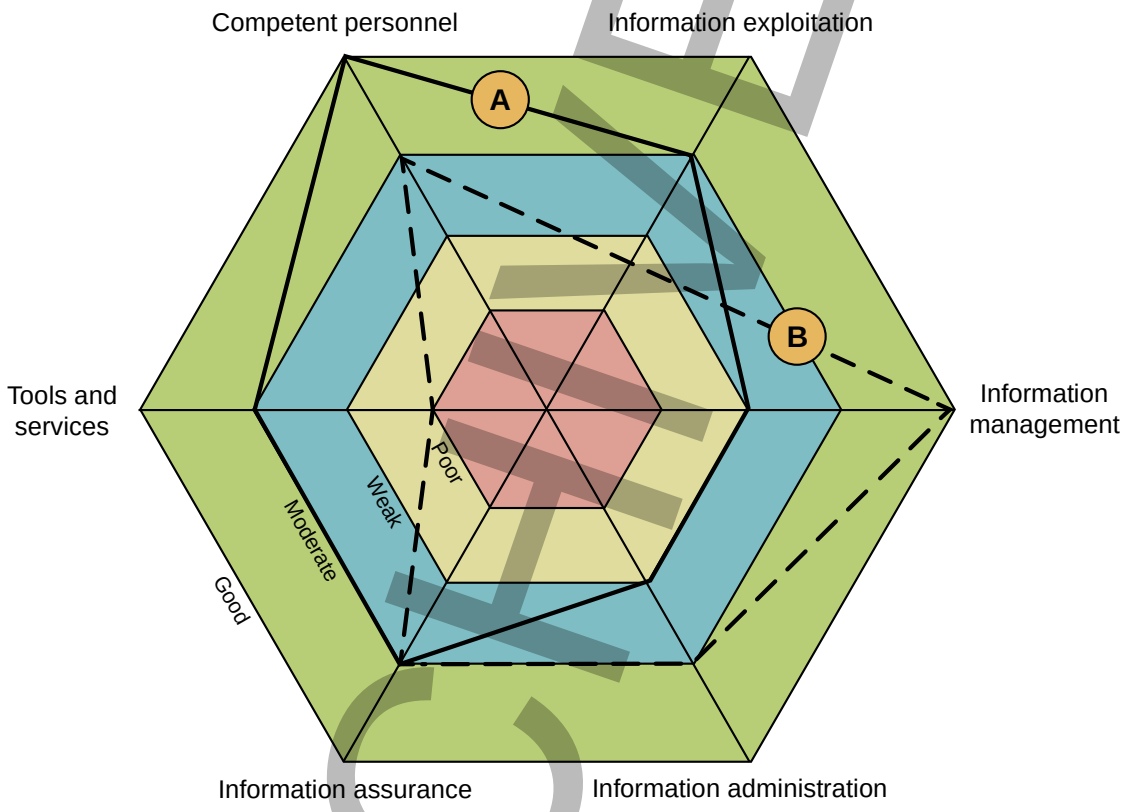


Figure 2.1 – Some enablers of information superiority

a. Organisation A (solid line) has moderate capability in tools and services and information assurance and weak information administration and management. Nevertheless, personnel competence is good and overall information exploitation moderate, so it is in a good position to enable information superiority.

b. Organisation B (dotted line) has poor capability in tools and services, moderate information assurance and good information

management. But, as its personnel's competencies are moderate and information exploitation weak then is it is in an inferior position to enable information superiority.

However, if these enablers are not well employed and information advantage in relation to other actors is poorly exploited, then information superiority will be compromised. An actor dependent on many enablers may struggle to meet these demands and their information superiority may be compromised. In contrast, an actor only requiring a few enablers to achieve information superiority may be able to meet these more limited demands more readily. Hence, the operational effectiveness of information superiority can only be assessed in relation to adversaries or other actors.

Setting the conditions for information superiority – deployment aspects

206. Information superiority is different at the various levels of command and is not the same for maritime, land or air (see Annex A for operational users' perspectives). Commanders must acknowledge these differences and realise that forcing unnecessary uniformity will limit the ability of their subordinates to generate their own 'local' information superiority.

207. As part of the ongoing information superiority estimate, commanders must continually review the type of information superiority that must be realised; it is different depending on the level and role of the command. Figure 2.2 shows that information superiority for those involved in command and intelligence activities (such as exploring possible futures and forming intentions) is not the same as for those involved in control and administration (as in logistics, personnel, medical, tasking and reporting). These types of tasks and levels are often blurred when the 'long screwdriver effect' comes into play. This long reach can be both a benefit and a curse if its consequences for information superiority are not fully appreciated. For example, modern global communications enable a nation's leader to be involved in authorising tactical decisions. This can be of decisive benefit where there may be political impact, and/or a hindrance in time-critical situations.

	Information superiority for command-intelligence (effectiveness)	Information superiority in control and administration (efficiency)
Strategic	Able to achieve relative advantage in global, pan-coalition situations and across concurrent operations	Able to achieve coherent secure information exchange across government departments
Operational	Able to achieve relative advantage in coalition contexts and across concurrent missions	Able to achieve reliable, timely and accurate interoperability for coalitions and across operations
Tactical	Able to achieve relative, local advantage in mission situations (that may have strategic effect)	Able to achieve timely, robust, efficient and accurate tasking and reporting of support activities, for example, logistics, in deployed forces

Figure 2.2 – How information superiority changes with level/role

208. **Changing capabilities – pre-deployment, during and post-deployment.** The scale and complexity of deployed information systems and capabilities must be matched to the changing circumstances. Commanders should aim for their systems to have the maximum effect on information superiority and minimum impact on staffs in terms of the technical burden of operating the equipment and software. As Figure 2.3 shows, effectiveness changes over the life of an operation – good adaptive information superiority (the upper dotted line) can mitigate potentially damaging deteriorations. This includes developing understanding pre-deployment so that it can be accessed and used by the deployed forces. The effect of roulements can be both bad and good as, after the initial drop, the next unit's insights are likely to enhance and extend information superiority and hence levels of understanding and operational effectiveness. Commanders should ensure that the ongoing information superiority estimate assesses current levels of effectiveness and considers necessary adaptations iteratively.

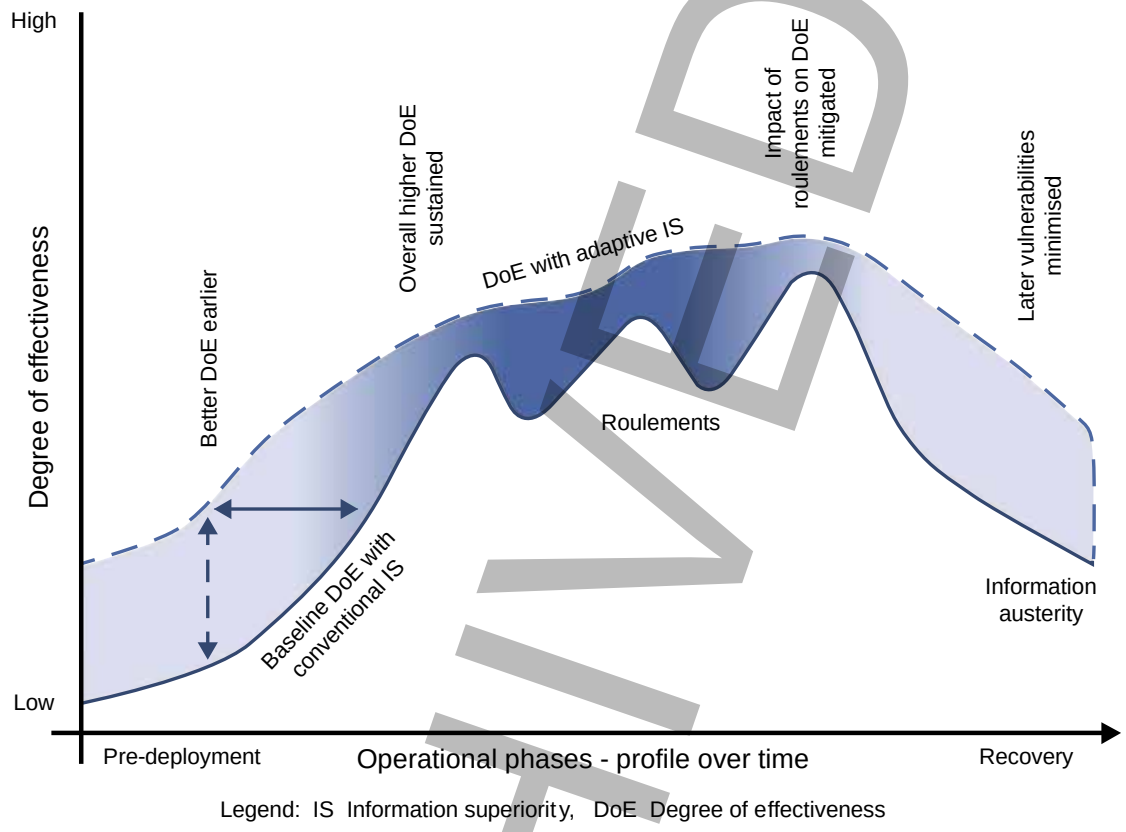


Figure 2.3 – Changes in effectiveness over time

209. **Adapting appropriate processing techniques.** The required degree of processing varies depending on the nature of the task-critical information. At times, this may involve 'rule-breaking' in the sense of improvising to seize opportunities. Staffs should frequently review the effectiveness of the procedures being used and initiate appropriate changes in ways-of-working.

Section 2 – Challenges, vulnerabilities and mitigations

210. This section describes the challenges that commanders and staffs face in achieving information superiority. It also examines vulnerabilities and how they may be mitigated. Commanders and staffs should assess these factors as part of the information superiority estimate.

Challenges to achieving and sustaining information superiority

211. **Information anarchy.** Without appropriate procedures, information disorder and incoherence may occur – whether caused by our own actions or triggered by our adversaries. Commanders must balance the desire for control of the information environment against enabling subordinates' freedom to exercise the initiative, flexibility and agility needed to exploit information superiority.

212. **Information austerity.** This is likely to occur both at the beginning of operations, as systems and procedures are deployed, activated and scaled up, and towards the end as they are withdrawn and scaled down. The careful application of reachback during times of austerity is an important consideration. As vital information may be absent at critical points, staffs must proactively manage these changes to ensure that information superiority is not undermined.

213. **Organisational immaturity.** Information superiority depends on all levels of the organisation being sufficiently mature, agile, flexible and adaptable to work in the ways needed for information superiority. In coalitions, the mismatch of maturities of technologies available may be a limiting factor, as may differences in perspectives, ways-of-working and interpretations. Addressing effective information superiority challenges should be a fundamental part of exercises with allies and potential partners.

214. **Cultural resistance.** UK Defence will develop and exercise the ways-of-working needed to exploit adaptive information superiority. Training can remove constraints such as change-averse behaviour and policies can remove inappropriate blame/reward regimes that stifle initiative.

215. **Lack of financial support.** Procurement processes require the benefits and value-for-money of information superiority to be demonstrated before any operation. This can lead to undervaluation as the true benefit may not be apparent until after an operation – if ever. The risk is that the Government may not invest in information superiority. To mitigate this, the MOD must clearly articulate the function, potential value and the political and operational benefits that can be accrued.

216. **Providing adequate bandwidth and processing power.** The availability of bandwidth, spectrum and processing power is not guaranteed. Therefore, staffs must take positive steps to manage demand and availability, including using techniques to support disadvantaged platforms. They must also be careful not to underestimate the related importance of the threats and opportunities from cyber and electronic warfare.[5] This includes appreciating the impacts on friendly forces' operations and on other friendly and non-belligerent activity resulting from deploying electronic warfare capabilities.

217. **Lack of attention to Defence lines of development.** The MOD must address the information superiority-specific aspects of the Defence lines of development during force development and procurement. Particularly relevant are: selecting staff with the appropriate aptitudes and attitudes; identifying relevant skillsets; providing the training to develop them; and enabling the career pathways to professionalise them.

218. **Over-reliance on information systems.** Over-reliance on information systems and procedures at the expense of the judgement of commanders and planners will constrain thinking to the inward-looking, technical conventional information superiority. Such over-reliance can undermine operational capacity by injecting unhelpful friction into operational activities. This will inhibit the force's ability to exploit other, more adaptive, ways of information superiority. Commanders and planners should ensure that systems support, rather than determine, their activities. Striking the right balance can be achieved using experience gained through exercises and staff training, and using subject-matter expertise.

Vulnerabilities and mitigations

219. A poor appreciation of the vulnerabilities of information superiority may lead to commanders and staff being over-confident that they have information superiority. This can be exacerbated by poor assumptions such as, considering adversaries as inferior, or failing to appreciate the complex nature of opposition allegiances. Commanders and staffs must understand:

- what information superiority can and cannot achieve;

[5] Relevant doctrine is provided in Allied Joint Publication (AJP) 3.6(A) *Allied Joint Electronic Warfare Doctrine.*

- how to exploit it; and
- what its vulnerabilities are.

Some examples follow.

220. **Over-categorising information.** If data does not fit pre-defined taxonomies or paradigms, it may be ignored or discarded. This could lead to evidence or subtle indicators being missed. Staffs and system administrators should avoid the temptation to standardise data simply for technical efficiency – they should first take account of intelligence and operational needs. Unstructured data can hold as much value as structured data, and extracting the insights offered by both are important processes that need to be better understood and resourced.[6]

221. **Over-classifying information.** When staffs are poorly resourced to access classified information, their information superiority will be diminished. Staffs should 'write for release' by default, and have the appropriate resources to do this.

222. **Information overload.** Information overload results from the ease with which data-rich products, as opposed to analysed material, can be passed across increased communications capabilities. This will diminish information superiority if not countered through effective procedures and training to instil good information handling and sharing habits.

223. **Destructively high tempo.** Staffs may be pressured because heavy workloads are actually being generated by the high frequency of cyberspace/software interactions and information exchanges. This may lead to burn-out. Commanders should actively monitor working tempo and adjust its drivers as required to focus on quality.

224. **An over-reliance on the outputs from technical intelligence, surveillance and reconnaissance.** This over-reliance not only increases our susceptibility to adversarial information operations and deception, but also leads to product dependency. Symptoms include believing the machine

[6] See: Treverton, 2003: "Reshaping national Intelligence for and Age of Information. RAND

rather than our own senses, and losing the initiative when systems fail. Commands should routinely exercise in information-austere modes.

225. **Distractions arising from shared situational awareness and connectedness.** Global inter-connectedness increases the possibility of panic. As news travels quickly, personnel may become (inappropriately) fixated on things they cannot influence. This can lead to self-inflicted denial of service. Commanders should ensure that training mitigates any tendency to be distracted by irrelevant matters.

226. **Balancing the need for security against compliance.** Headquarters routinely work in a secure manner where, for example, documents no longer needed are shredded or deleted. However, the legal demands for compliance and record-keeping require the opposite – that everything must be kept. Commanders must inform themselves of the legal compliance policies and, with their staffs, develop appropriate, realistic and feasible ways-of-working.

227. **Loss of coalition interoperability.** Commanders should not assume that data fidelity (as a component of information superiority) can be maintained within, and between, coalition networks unless rigorous information management and data standards are adopted, maintained and controlled by that coalition.

228. **Inertia of Defence policy and governance.** The slow rate, relative to an adversary, at which policy and governance arrangements can be changed may put UK forces at a disadvantage. For example, relative to adversaries who might use social media routinely (such as, Facebook and Twitter), commanders and staffs may not be able to access the same influence avenues. Commanders should be given authority to waive certain policies, for example, to authorise the use of social media, based on operational imperative. Annex A introduces ongoing governance developments.

229. **Lack of appreciation of cyber issues.** Commanders will face new threats from cyber because it is contested and compromised (being an environment which we can never fully control). Moreover, the threat from cyberspace can never be fully mitigated, although it also presents new opportunities (such as the use of social media to achieve extensive

influence).[7] Staffs should establish measures to protect critical infrastructure. Example threats include the spread of malware from botnets[8] (such as the Stuxnet virus which attacked Iran's industrial capability) and denial of service attacks on network providers. An introduction to cyber mitigations is provided in Section 8 of Annex A.

Georgia (2008)

The Russian invasion of Georgia was preceded by an intensive series of cyber attacks attempting to disrupt Georgian governmental and civilian online infrastructure. This inhibited the Georgian Government's ability to communicate their strategic narrative and enabled the Russians to claim there was popular support (as evidenced by the hackers who, it was said, were just ordinary Russians) for the invasion. The confusion generated by claim and counter-claim made it difficult for international opinion to bear weight. Russian cyber information superiority was an important factor in an integrated campaign.

230. **Information dependency.** In the home base, personnel may become dependent on the accessibility and availability of information. In austere low-technology situations, there may be serious limitations and shortfalls in capability. Commanders should ensure, through education and training, that personnel are able to adapt their ways-of-working and information needs to match the local information environment.

231. **Slow procurement of solutions to meet urgent requirements.** Procurement has inherently long capability delivery lead times. This may limit operational flexibility and agility. Commanders should be empowered to authorise staffs to improvise where capability is lacking; and where the operational imperative demands action, to sustain information superiority. Commanders must strike a balance between wanting to respond to change (where everyone immediately wants the latest technology), versus the ability to train people to use new capability effectively. Enough stability is required so that standard procedures can be established. But, if the procedures are in place too long, this risks stagnation. Being able to adapt to imposed changes

[7] See Joint Doctrine Note (JDN) 3/12 *Cyber Operations: The Defence Contribution*.
[8] A network of private computers infected with malicious software and controlled as a group without the owners' knowledge. For example, to send spam emails. Concise Oxford English Dictionary, 12th edition, 2011.

(for example, software upgrades) is essential, as is being able to understand the potential impact of changes, and engaging with the controlling governance arrangements of change management.

232. **Not being able to compensate for system shortfalls.** Systems have known functionality shortfalls that will affect information superiority. Where there are capability gaps, commanders and their staffs should improvise and develop temporary 'work-arounds' while ensuring that remedial measures are taken. Commanders should take care not to institutionalise 'work-arounds', but formally address the identified shortfalls at the earliest opportunity. Staffs need to make sure that reversionary modes are provided in the event of technical failures (such as loss of power). They must assess such vulnerabilities and actively mitigate them as part of protection and sustainment activities. This could involve the use of business continuity approaches which consider primary, alternative, contingency, and emergency stances (PACE) planning.

Chapter 3 – Exploiting information superiority

'All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know by knowing what you do.'

Arthur Wellesley, Duke of Wellington, 1769-1852

The purpose of Chapter 3 is to explain how to realise, employ and exploit information superiority behaviours.[1] It describes how to gain operational advantage by influencing the degree of information superiority and summarises the benefits that information superiority can provide.

Section 1 – Realising information superiority

301. Information superiority can only be fully realised when the two complementary facets shown in Figure 3.1 are maximised.

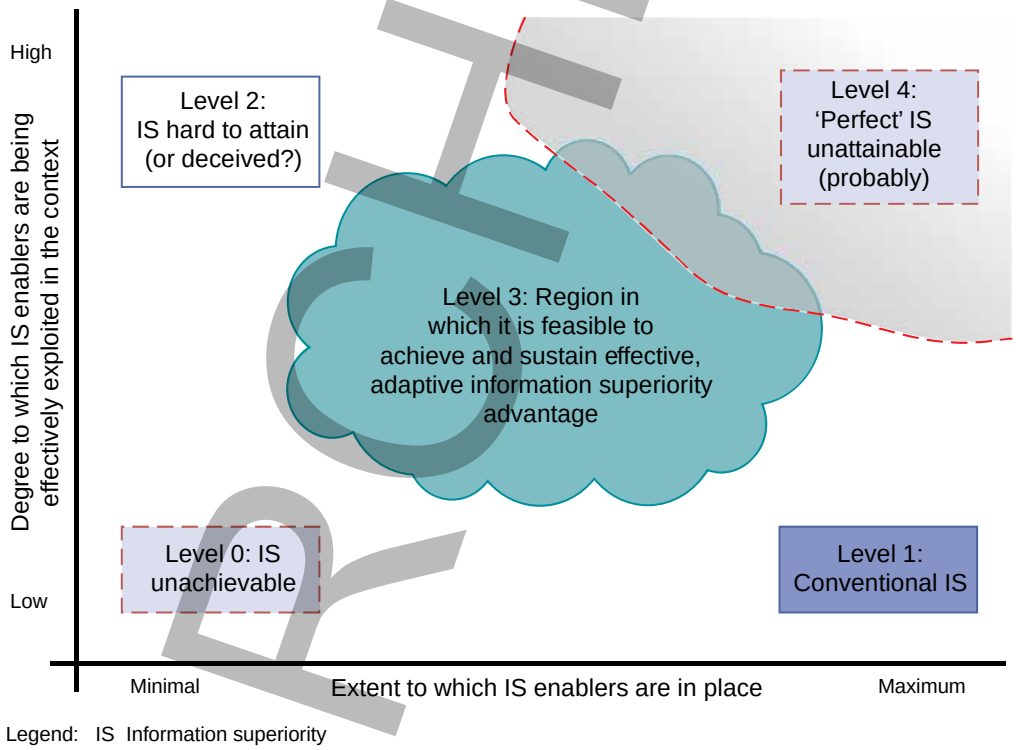


Figure 3.1 – The two complementary facets of information superiority

[1] Exploit: *make use of or derive benefit (from something)*. Concise Oxford English Dictionary (COED), 12th edition, 2011.

The first facet, discussed in Chapter 2, concerns the enablers of information superiority (horizontal axis). The second facet is the degree to which these enablers are effectively exploited to achieve advantage in some situation (vertical axis).

302. Figure 3.1 indicates where different levels of information superiority are being achieved. In the lower-left corner information superiority has failed because few enablers are in place and they are not being effectively exploited in relation to adversaries. To the top right is a region where achieving and sustaining perfect information superiority is probably unattainable. We may aspire to this level 4 information superiority, but in reality other actors and circumstances will most likely prevent it. Level 2 is hard to attain with only a minimal amount of enablers in place. Level 3 is where we have capable enough systems in place but we are not always able to use them effectively. In practice, the level 3 region is the one where we are most likely to be able to gain and sustain advantageous information superiority. When information superiority is achieved commanders will want to press the advantage and, wherever possible, sustain that advantage over time.

303. Figure 3.1, taken together with Figure 2.2, shows that information superiority is different in all situations. Therefore, the nature of the information superiority being sought depends on the military task and the operating situation. Commanders must dynamically adjust the levers of information superiority described later, and assess indicators and measures of information superiority which are appropriate to the mission.

304. **Exploiting an information superiority advantage.** Once information superiority has been obtained, it is a force multiplier which can be exploited offensively and defensively.

a. **Offensive information superiority.** Information superiority can be used to set the agenda for other actors. A dominant position allows us to manipulate the perceptions of other actors and influence their actions because they cannot appreciate the wider context and are vulnerable. This enhances the manoeuvrist approach. A dominant position, if achieved, should not be taken for granted. However, total

'decision-dominance' is relatively rare in conflict as adversaries, if they realise they are weak, will avoid conflict.

First Gulf War (1990-91)

In Iraq, the US-led coalition forces had total oversight and almost absolute information superiority because of superior surveillance capabilities. The open desert on which the battles were waged was also a factor in enabling collection assets to be so effective. The defeat of Saddam Hussein's forces that followed showed how completely the West's forces had achieved 'full-spectrum dominance'. The likelihood of 'war among the people' in urban environments will complicate surveillance and 'full spectrum dominance' in such conditions will not be possible.[2]

b. **Defensive information superiority.** In this type of information superiority, which is non-discretionary, our defended position is used to observe what others are doing, gain information and, in the background, set the scene for our own actions. This may involve detecting who is attacking our information superiority position overtly and covertly as well as using this information to formulate how our partnering or coercion strategies may need to change.

Section 2 – Information superiority behaviours

305. Figure 3.2 illustrates offensive and defensive information superiority behaviours for a simplified situation involving two actors (where an actor's effectiveness is neutralised by raising them off the ground to a point where they are unable to influence outcomes). This dynamic struggle for advantage occurs concurrently, as in a football match, and not sequentially as in a chess match. In Figure 3.2, the actor to the left (us) has a more extensive set of information capabilities (indicated by the bigger hexagon), but has not enabled them well (dotted line within the hexagon). The opposites hold true for the other actor (them) who has more limited, but better-enabled, capabilities and so they start with an advantage (1). We try to counter directly (1a, for example, by better understanding the threat). A coalition partner may add weight to help us (1b, for example, by providing extra

[2] The phrase 'war among the people' was coined by General Sir Rupert Smith in his book, *Utility of Force*, 2005.

cultural insight). Through our deception (2, for example, a deliberately clumsy press release) the adversary takes action which actually disadvantages them. Realising this, they try to counter by influencing us indirectly (2a, for example, maybe through an intermediary (not shown) who leaks compromising material via Twitter). We try to change the context to our advantage by fundamentally altering the nature and degree of asymmetry (3, for example, a defector to our cause agrees to publicly discredit our adversary and change the narrative). They attempt to counter this (3a) to maintain their previous advantage, but public opinion has now turned against them and the lever swings our way (not shown). This simple illustration shows how some of the features of adaptive information superiority can be exploited dynamically to gain advantage.

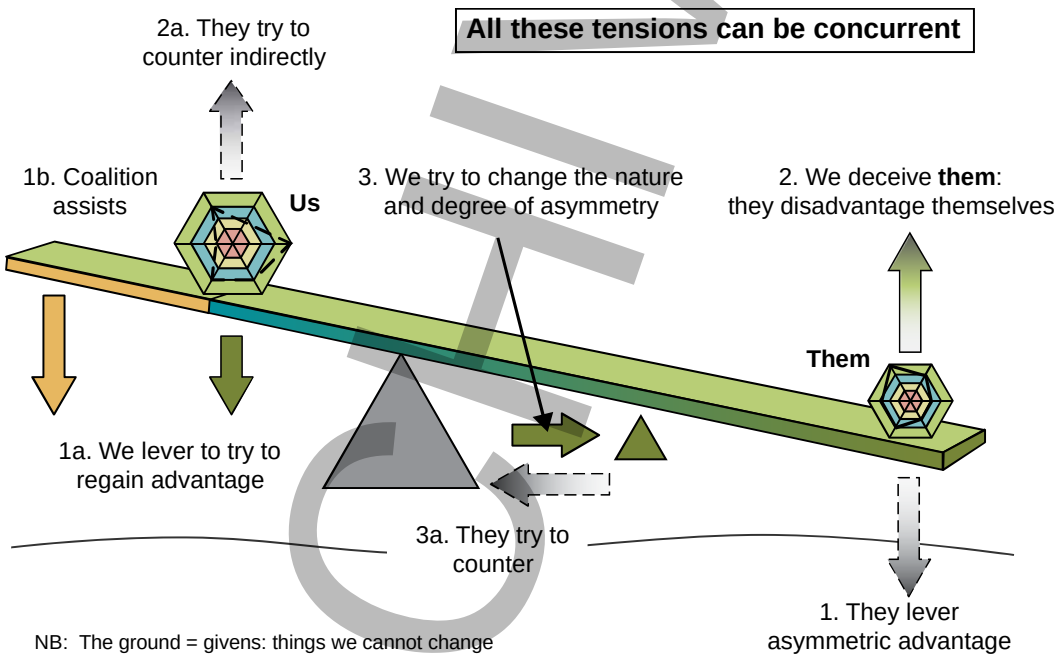
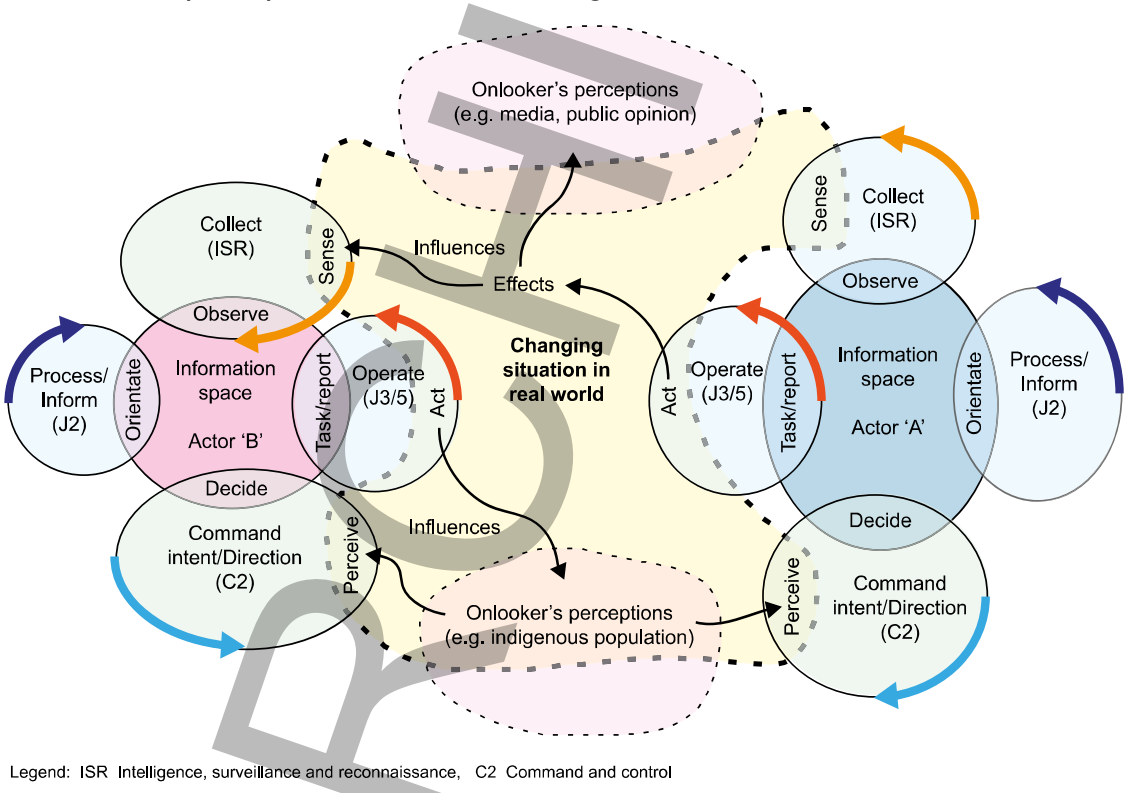


Figure 3.2 – Information superiority behaviours

Section 3 – Information superiority in practice

306. Though information superiority is an intangible aspect of conflict, it can be altered and adjusted in various ways. Commanders can, under certain circumstances, pull levers to refine it. Examples are discussed below using the schematic at Figure 3.3 for illustration.[3] Note that this example is, again, simplified to show two actors – in reality there will always be more. Commanders and staffs must always consider the 'complex of actors', including red, white and blue (and potentially grey and green) actors.

307. Each actor has an **information space** which enables cross-functional interaction and shared awareness of self, others and the changing situation over time. It pervades the cognitive, virtual and physical domains. It also contributes to, and draws upon, the four main loops of operation activity. The information space provides much of the 'glue' which enables coherence.



Legend: ISR Intelligence, surveillance and reconnaissance, C2 Command and control

Figure 3.3 – Two actors striving for information superiority

[3] This 'two actors' schematic is based partly on John Boyd's model – observe, orientate, decide, act (OODA) and on the 'generic networked information environment model' on page 7 of Joint Service Publication (JSP) 777, *Network-Enabled Capability.*

a. The **operate** loop acts to bring about effects and influence. Its use of the information space mainly involves tasking and reporting.

b. The **collect** loop is cued by commanders' needs to sense changes. Ongoing observations update the information space accordingly.

c. The **process** loop, through intelligence analysis, adds value and meaning to items in the information space. This informs decision-making and problem solving in the other loops.

d. The **command** loop is where intent, guidance and direction is developed through insight and foresight, informed by commanders' perceptions of the information space.

308. It is wrong to think of the loops occurring in a linear sequence, one after another. These four functional areas work concurrently, and semi-autonomously. They collaborate within the commander's overall intent supported by the shared information space – updating information for the benefit of others and accessing insights that others have provided.

Information superiority – operational application

309. The rest of this section provides examples of how information superiority may be gained or manipulated, using the levers of information superiority.

310. **Relative advantage.** Commanders should appreciate and then exploit the nature of their relative advantage over other actors. This requires an understanding of the differences in complexity between their and other actors' situations. Where an adversary has simple information needs that can be easily fulfilled, they are at an implicit advantage. To negate this advantage, commanders should identify and exploit decisive information asymmetries. This may mean reducing the complexity, scope or timeliness of their own requirements to refocus resources on those identified as offering decisive advantage.

311. **Changing perspectives and red teaming.** By deliberately taking alternative perspectives, such as those of the other actors and onlookers (Figure 3.3), commanders can identify weaknesses and opportunities against which to apply the levers.[4] This may have to be done indirectly or through third parties who may be closer to the key actors and better able (for example, culturally and/or linguistically) to gauge other views and opinions than we are. The understanding gained can be used to identify, and then exploit, potential asymmetric advantages. Commanders should be aware of the tendency to reject minority or dissenting views, otherwise consensus (that may lead to groupthink) could undermine information superiority.

312. **Adjusting tempo.** Commanders can adopt the appropriate tempo to adjust the degree of overmatch of adversaries' information capabilities. There is a trade-off in the extent to which high-tempo can be sustained. For example, we may have decided to overwhelm an adversary through tempo but we must simultaneously avoid any detrimental effect on our own forces. Having information superiority enables us to dictate the pace and tune the extent of our overmatch. Commanders can then decide how to alter the tempo of the loops (shown in Figure 3.3 as the bold arrows). But this does not always mean faster. For example, in enduring operations, there are elements which play out over months or even years. Here information superiority is not about instant decision-making, but is more to do with being able to sustain persistent, heightened awareness over long periods of time.

313. **Manipulating personal power relationships.** The nature of the advantage achieved may depend more on knowing the individuals' vulnerabilities rather than the vulnerabilities of their information systems. Commanders who meet other actors face-to-face may be able to influence information superiority directly by force of will or personality.

[4] This is part of the operational security (OPSEC) process for assessing the vulnerabilities of our own information.

Cuban missile crisis (1962)

The Soviet Union was in the process of secretly building nuclear missile sites in Cuba and the US was adamant that this was not to happen and established a blockade. The Soviet Premier, Nikita Khrushchev, publicly accused the US President, John F Kennedy, of 'an act of aggression propelling human kind into the abyss of a world nuclear-missile war'. Surveillance flights by U2 spyplanes gathered clear evidence that, despite Soviet protestations to the contrary, the Soviets were deploying nuclear missile capabilities. Kennedy was able to use the evidence to change international opinion, therefore neutralising the Soviet's military (and political) advantage. Kennedy's information superiority proved decisive.

314. **Altering the release of, or protection of, information.** In certain situations, commanders may wish to supply actors with information as part of coercion or deception. This may include 'junk' information to overwhelm our adversaries' cognitive capacities. This release, or protection of, information at a key moment may be one of the tasks of the act part of the **operate** loop (Figure 3.3).

315. **Adjusting expectations and risk appetite.** Commanders may face a trade-off between acting on 80% of information now and waiting for more detail which may arrive too late to be useful. Demanding certainty from the activities of all the four functions in Figure 3.3 wastes effort. Commanders can adjust levels of expectation, expressed in their critical information requirements, to enable information superiority to be achieved more easily. For example, Figure 3.4 shows a simplified case with two actors.

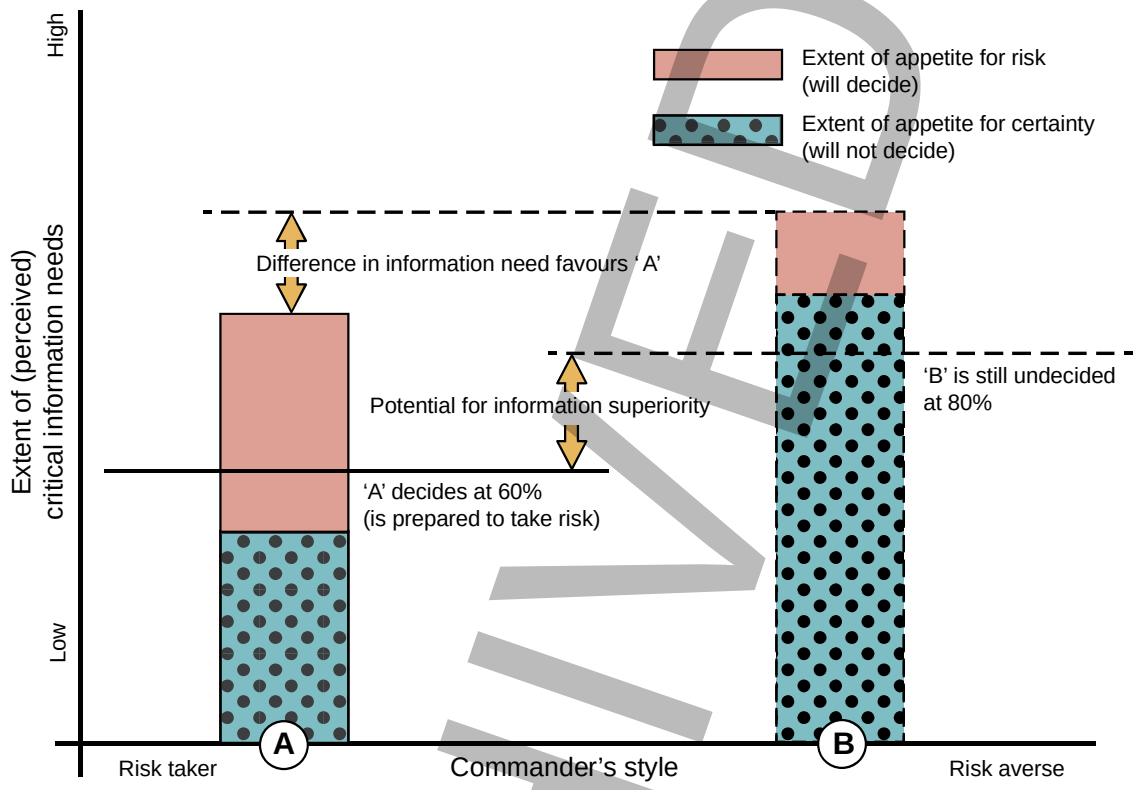


Figure 3.4 – Risk appetite and information superiority

Commander A is comfortable with risk, Commander B is risk averse. Also A's information needs are less than B's, which gives significant advantage. Commander A is prepared to accept risk and make decisions sooner based on less information. This gives A an information superiority advantage over B – both in terms of initiative and being less demanding on the collecting, processing and analysis functional loops in Figure 3.3.

316. **Command style.** By decentralising authorities and delegating responsibilities, commanders can increase the degree of initiative available to subordinates. This enables those in the best position at the time and in the right situation to seize fleeting opportunities, and act decisively on local information superiority. In effect, this involves both delegating aspects of command to the **operate** loop (Figure 3.3) and ensuring that the informational space has the necessary intelligence required to act. All part of mission command.

317. **Changing scale and reach.** Commanders need to compare and contrast information from deep, close and rear, and from all environments, to reveal important insights. By adjusting the scale of attention and ensuring a sufficiently broad and deep information space commanders will circumvent any risk of situational-myopia[5] and ideally overmatch an adversary's capabilities.

318. **Manipulating our adversaries' information superiority.** An assessment should be made as to how easy it is to degrade or manipulate an adversary's ability to sustain information superiority. If we are continually outwitting them (unless it is a feint on their part) then we can be reasonably confident that we have information superiority relative to them. Commanders should analyse adversaries' capabilities using Figure 3.3 as a guide.

319. **Adjusting the volume and velocity of information being manipulated.**[6] By promoting 'resource-aware' behaviours, commanders can tune the volume, velocity and throughput of information. Thereby, altering the degree of information superiority achieved. This can prevent information overload, but advantage relative to an adversary must be sustained. Cyberspace techniques can be used to make certain types of information available and see if our adversaries access it.[7] For their own forces, commanders should provide guidance on the levels of detail and amount of data retained in the information space. Such a judgement will be key to preventing personnel and systems being overloaded, particularly in an austere environment.

Information superiority on a range of operations

320. Figure 3.5 shows ways in which information superiority varies with scale and duration of operations.

[5] Myopia – short-sightedness; lack of foresight or intellectual insight. Concise Oxford English Dictionary, 12th edition, 2011.
[6] In this publication, velocity not only refers to the speed of information but the rate of change of the trajectory of information, driven by circumstance.
[7] An example would be after WIkiLeaks established its influence in 2010. A large number of WikiLeak look-alike sites appeared which tempted people with 'secrets' but which would then load malware onto the visitors. Certain agencies also took advantage of this to identify the dissenters who were being attracted.

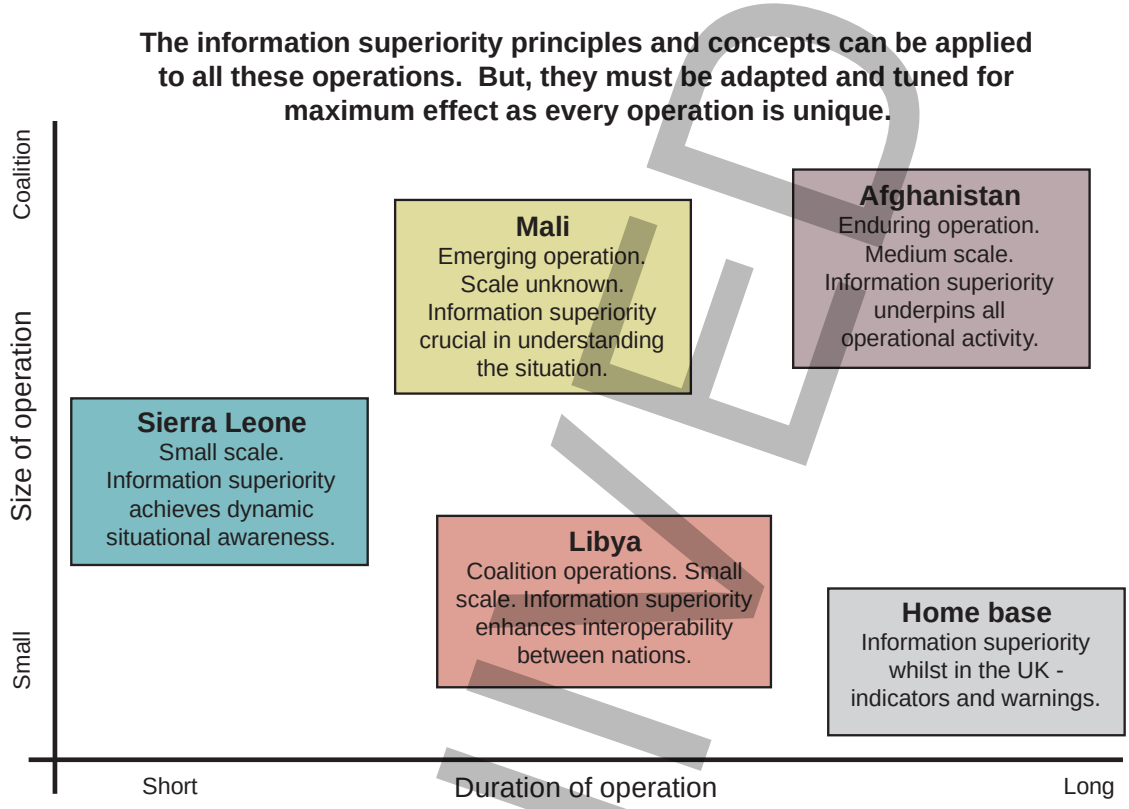


Figure 3.5 – Information superiority and example operations

321. **Home base.** At their home base, military staffs will still be engaged with other government departments in sustaining information superiority. This is both part of readiness preparations upstream of any operation and in support of forward-deployed standing tasks. Responsive or deployed forces then start with the best possible information position. Access to home-based information, allowing it to be used and refined by the deployed force, is key. Deployed forces should, however, retain sufficient resources and capacity to operate without reachback and in information-austere environments. Such conditions could be imposed by the environment or when operating in regions of intermittent connectivity.

322. **Mali – Operation Serval, 2013.**[8] This is a complex operation where it is difficult to identify the key actors and their motivations. Information superiority will depend on obtaining rich and meaningful local and cultural insights, otherwise the risk is that historic stereotypes will be applied.

[8] Operation Newcombe is the operational name for the UK contribution to the French-led Operation Serval.

323. **Sierra Leone – Operation Barras, 2000.** This small-scale operation was characterised by the rate at which events on the ground changed. The level of media and political oversight required concurrent time-critical politico-strategic and tactical information superiority. This was achieved despite the fluid nature of the tactical engagements.

324. **In Libya – Operation Ellamy, 2011.** The UK participated in a diverse and unexpected coalition. A particular challenge was the fragmented nature of the opposition forces. Information superiority was eventually achieved once interoperability was effected between all the actors, many of whom were irregulars who worked through third parties.

325. **Afghanistan – Operation Herrick, 2002 onwards.** Coalition operations have involved both dealing with a complex insurgency, using a 'shape, clear, hold and build' approach, but also supporting rebuilding institutions to support a return to political normality. These activities occur in many spheres of influence and over various levels and timescales. The coalition itself is complex with multiple partners, all of whom have different opportunities for achieving information superiority. Given this, there have been examples of successes and failures of information superiority which have been well documented elsewhere.

326. **Lesson.** Looking at these examples, we can see that each situation is context-specific. So, for success in any operation, commanders and staff should use the information superiority characteristics and principles outlined in this JDN and adapt accordingly.

Section 4 – Information superiority benefits

327. The benefits of having information superiority are not accrued in the information environment.[9] The advantages are realised through more acute and relevant understanding of situations and hence more effective and appropriate decision-making. Paragraphs 327 to 337 cover the wider operational use of having information superiority.

328. **Making adversaries vulnerable.** The decision to deliberately create asymmetric information advantage should be part of a coordinated approach. These asymmetries fundamentally undermine an adversary's sense of mastery of the situation and increase their vulnerability.

329. **Being well-positioned to develop insight, foresight and understanding.** Information superiority allows commanders to identify future challenges, and develop the insight and foresight to exploit them. It is also not just about having an advantageous information position relative to other actors; it is about developing heightened awareness of the nature of change and opportunity in context, and determining what to do as a result.

330. **Supporting different types of operations.** When engaged in deception or when supporting covert operations, the nature of the information superiority changes. Much of what matters must remain hidden, ambiguous or contradictory – keeping track of this web of alternative interpretations is a human skill. It is beyond the capability of machines to do this.

331. **Enabling decision superiority.** When information superiority has been achieved, commanders will be in a position to gain decisive advantage in a way that would enable decision superiority. This involves:

- gaining understanding of the environment;
- using pattern-recognition capabilities to enable commanders to detect sensitive changes in the environment; and

[9] Information environment – the virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems. NATO Military Committee (MC) 422/3.

- a decision-making culture that encourages commanders to act quickly, but appropriately, on the basis of incomplete information.[10]

332. **Adapting operational tempo dynamically.** Having good information superiority allows commanders to adjust and exploit tempo and timeliness opportunities. For example, if we can predict an adversary's way-of-working we can release key pieces of information, or time deception activities, when they will have maximum impact. This is helped by effective use of the speed and reach of cyber capabilities.

333. **Supporting unity of effort in coalition working.** Being an effective coalition partner is a key part of the UK's Defence Policy. Commanders will have to adapt national ways-of-working such that they contribute to effective, interoperable coalition working and hence information superiority.

334. **Enhancing situational awareness.** Information superiority allows a commander to see the real picture. However, if information superiority declines, or is lost, then confusion follows. This is more than just the maintenance of common operational pictures. It is about how they are used and interpreted by staffs to gain decisive insight.

335. **Achieving information superiority via third parties.** Where commanders may struggle to develop our own information superiority, they may work with, or through, actors in a better position to gain more effective and even different asymmetries of advantage. A benefit of such collaboration, which goes beyond that achieved in coalition, is that potential allies will have confidence to engage with the UK in a manner that they might not otherwise have done.

336. **Enabling disproportionate effect.** Because information superiority is assessed in relation to other actors, it is not necessary to have 'perfect' information superiority, only the degree of information superiority necessary. Good information superiority is a force multiplier – poor information superiority can lead to unexpected failure.

[10] From David Kilcullen, Australian Army Future Land Operating Concept, *Complex Warfighting,* 2004.

337. **Enabling accountability, rebuttal, repudiation and effective governance.** Information superiority enables MOD governance responsibilities to be achieved. For example, good information superiority will:

- support rebuttal;
- reduce compensation claims;
- help prosecute and defend against claims of war crimes;
- assist in defending our actions to journalists and the electorate;
- support freedom of information requests;
- influence the strategic narrative; and
- defend the MOD's actions in coroners' courts.

Kosovo War (1999)

NATO's Operation Allied Force was notable for a number of information superiority failures.

- In March, an F-117 Stealth Fighter was shot down. To achieve this the Serbians used a combination of: real-time media reports (showing fighters taking off from Aviano air base); simple speed and distance calculations to estimate position; listening devices and a network of observers. This combination of low-technology tactics, rapid learning, and astute improvisation converged to enable an SA-3 not operating in its normal, radar-guided mode to down the aircraft.
- Low-technology techniques were used to defeat known vulnerabilities in the high-technology systems being used by NATO and so negate their potential contribution to information superiority. These approaches included: burning tyres to confuse laser-guided missile sensors; the use of decoys (which were then bombed) to deceive NATO into thinking that enemy capabilities were being destroyed; and old-fashioned technology being used which deceived modern systems.
- There was an inability to gain information superiority over Milosevic's 'police' units. This was because they used a system of delegated intent which did not require them to employ the type of active command and control networks that NATO was trying to interdict.

338. **The aspiration – achieving highly-dynamic, persistent information superiority.** Operational effectiveness is affected by the degree of information superiority that can be achieved. In future, only the command-led coordination and integration of information will enable information superiority. This must be from an operator's perspective rather than a technical one. The aspiration must be to enable decision-makers to access and manipulate whatever information they need, whenever they need it and in a form that makes sense given the situation at the time. Commanders should:

- understand the characteristics of information superiority;
- apply information superiority principles and guidance;
- ensure they can dynamically adapt information behaviours to gain advantage operationally; and finally,
- direct their staffs to note the evolving resources available online through the links provided in the Annex.

Exploiting information superiority

Notes:

Introduction to JTTP 2/13.1 – Joint tactics, techniques and procedures for enabling information superiority

Annex A introduces evolving guidance on information superiority practice. This guidance will be developed as an online, Permanent Joint Headquarters (PJHQ)-owned, Joint tactics, techniques and procedures (JTTP) 2/13.1. The JTTP is a living document and will be updated by the appropriate stakeholders as required. This annex therefore introduces best practice as at the time of publication – July 2013.

JTTP 2/13.1 is hosted on the information superiority home page at: http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Reference/Publications/Pages/IS-JTTP.aspx

1. This Annex on information superiority enablers summarises the contents of the online JTTP in eight sections (as at time of publication). It should be noted, however, that the online resource is designed to be expandable as practice and discussions evolve.

- Section 1: Developing and employing an information superiority estimate.
- Section 2: Mission threads.
- Section 3: Coalition working and future mission-configurable network.
- Section 4: Common operating pictures and information superiority.
- Section 5: Operational users' perspectives.
- Section 6: Archiving and recovery of operational information.
- Section 7: Information operating model: information superiority governance.
- Section 8: Links to online information superiority-related topics and resources.

Section 1 – Developing and using an information superiority estimate

Rationale

2. The information superiority estimate is used to develop information superiority plans and produce directives. Iterative planning is essential as it enables information superiority capabilities to be matched to commanders' needs in changing circumstances. This section provides an exemplar process for commanders and staffs to follow when planning capability provision.

Executive summary

3. Currently, military forces produce information plans which merely detail the technical capabilities needed to support command and control activities (including administration, logistics, medical and liaison tasks). The information superiority estimate is more than an information plan as it factors in other actors' intents and capabilities, and the ways that advantage can be achieved.

4. Commanders must use an information superiority estimate template, like the one provided in the online JTTP. It takes account of the characteristics, principles, insights and behaviours laid out in this JDN. The information superiority estimate is linked to the command estimate through the use of mission threads and enables planning to take place.

5. In outline, information superiority planning gains an understanding of the commander's intent and of what needs to be achieved, against an assessment of capabilities and services expected to be available. From this, J6 staff can specify the:

- systems, services and tools required for each purpose, as well as where and when;
- training needed to use them effectively;
- support that J6 staff will provide in configuring the tools and services for the context;

- expected shortfalls and mitigations;
- maintenance tasks required; and
- any cost implications.

This may involve the use of business continuity approaches which consider the mitigations needed to deal with primary, alternative, contingency, and emergency situations (PACE Planning). The directive produced, when actioned by staffs, sets the conditions so that information superiority can be achieved.

Section 2 – Mission threads

Rationale

6. The need to match the commander's intent to the tasks that users need to perform, and the services required to support them, uses the technique of mission threads. Mission threads is a planning tool used to develop the information superiority estimate. The online JTTP explains how mission threads are used to assist in setting the conditions for achieving information superiority.

Executive summary

7. The mission threads approach is used to make sure services are provided efficiently to support command tasks. The mission threads used are:

- command and control and battlespace management;
- full spectrum targeting and effects;
- joint intelligence, surveillance and reconnaissance;
- force protection of own force elements;
- coalition interoperability; and
- logistics and medical support.

Situational awareness is not a mission thread on its own, it arises from the common operating picture(s) and the work of staffs in exploiting them to

develop shared appreciation. By working with the user community, and by considering which of these mission threads is required to support the mission, the appropriate information superiority-related tools and services can be identified.

Section 3 – Coalition working and future mission-configurable network

Rationale

8. Information superiority is fundamental to successful coalition operations and the challenges of integrating people, processes and technology must be addressed across all partners. The online JTTP includes the information superiority-specific aspects of coalition working. It also shows how information superiority can be achieved both in coalitions, and in more formal alliances (such as NATO). The online JTTP provides a summary of the essential elements of governance arrangements used to achieve coalition interoperability and how they should be employed.

Executive summary

9. There can be no single 'one-size-fits-all' standing mission-configured network as each situation is different. Although baseline configurations are available, commanders need to understand the differences between the baseline and the needs of their actual situation. They should then direct their staffs to make the necessary adjustments. The ability to interactively scale-up and scale-down and mix-and-match capabilities as part of preparing, deploying and adapting is an important part of coalition working. The online JTTP provides information on the design of previous mission networks and guidance on configurating future ones. It briefly explores the requirements for achieving coalition information superiority and looks at examples, obstacles and next steps. A key aspect of condition setting is achieving coalition interoperability and the Afghan Mission Network governance is cited as best practice.

Background

10. The latter years of the International Security Assistance Force (ISAF) campaign in Afghanistan demonstrated that, through establishing minimum essential governance with a clear operational focus and minimal bureaucracy, it was possible to provide a theatre-wide mission network supporting the operational information needs of more than 40 nations. Coalitions have always recognised the need to understand each other to operate effectively together. This understanding and interoperability arises from:

- becoming confident and competent at operating together through exercising together (the people dimension);
- agreeing common doctrinal and tactical procedures and ways-of-working (the process dimension); and
- using the same system or similar systems which use compatible, preferably open, standards (the technology dimension).

Lesson

11. NATO has developed Allied Publications addressing technical standards and warfighting tactics which enable coalition partners to come together with a degree of interoperability. ISAF introduced an interoperability solution across a much wider coalition that incorporated an unprecedented richness of information exchange and took some 12-18 months to establish. The solution continues to evolve. The Libya crisis of 2011 defaulted to NATO command and information systems as the primary mission network, which resulted in some important coalition partners being excluded. For the Mali operation (2013), which involved a number of nations in direct support of France, no coalition mission network was established, undermining interoperability.

Fundamentals

12. Commanders should note that interoperability will only be achieved through effective governance arrangements, whether standing (essential for immediate capability), or developed rapidly where arrangements are lacking.

Merely desiring interoperability achieves nothing. For maximum operational effect, commanders should ensure that:

- governance is provided with a small number of closely coupled and adequately resourced user and technical working groups (excessive bureaucracy will hinder essential agility);
- each coalition member maintains interoperability as systems, software and procedures evolve (this requires coalition interoperability assurance and validation capabilities to be in place); and
- regular and robust exercising and training with actual or potential coalition partners takes place.

13. Recent experience highlights the requirement to have coalition interoperability capability at a 'fight tonight' level of readiness. The immediate challenge is to get agreement amongst potential coalition partners on what this could mean in practice. NATO has a future mission network programme which aims to develop a set of open standards and processes which potential coalition nations would comply with. This includes nations having a permanent coalition interoperability assurance and validation capability. The US has plans for a mission-partnering environment and the UK is developing a mission-configurable capability. The challenge is to ensure all these initiatives amount to one and the same thing.

14. There are no current UK or coalition policies which capture these fundamentals on an enduring basis. In the online resources there is a link to the current Afghan Mission Network governance documents which are under regular review to keep pace with operational developments.

The Afghan Mission Network

Successive ISAF Commanders directed use of the Afghan Mission Network (AMN) as the single, coalition-wide mechanism for information exchange in support of the ISAF mission objectives.

NATO established a core communications and information systems capability managed by a loose, but formalised, governance arrangement of a single NATO 2* steering group, an OF-5 executive group and a number of working groups (operations, technical, architecture and assurance). All were coordinated by a small secretariat of voluntary national contributions of coalition members.

The AMN requirements were based on theatre pull, which prioritised mission threads and shaped the focus of the working groups.

Along with a short overarching governance document, the key document is a comprehensive joining, membership and exit instruction (JMEI) which sets out the standards for each nation to comply with. This includes a supporting coalition interoperability assurance and validation process designed to keep coalition partners in technical step with each other.

JMEIs made provisions for different nations to participate on the AMN in ways commensurate with the scale of their national commitment, but all the ways aimed for interoperability.

Section 4 – Common operating pictures and information superiority

Rationale

15. In a digital world, common operating pictures are fundamental to developing situational awareness and enabling effective decision-making. Thus, they are directly relevant to achieving information superiority. The term 'common operating picture' is widely used with many interpretations. The online JTTP explores some earlier common operating picture concepts and compares them with recent and emerging examples. It draws out fundamental principles and cites an exemplar.

Executive summary

16. The concept of a common operating picture is that information which commanders feel is most critical to aid decision-making can be readily appreciated. However, we should not think of common operating pictures as necessarily ‘common’ or simply ‘pictures’. Rather, they are windows to shared information resources with the views configured to let viewers achieve their functional purposes in relation to their tasks. These views aid users in exploring issues, gaining insights, assessing options and making effective decisions. Commanders and staffs should note that these views cannot provide an unambiguous 'single view of the truth' as the underlying information resources:

- will be incomplete;
- may have been filtered and annotated inappropriately;
- may not be up to date;
- may have been manipulated by other actors to deceive or undermine our information superiority; and
- may be interpreted differently by different viewers.

Background

17. In recent years, the term common operating picture has been widely and loosely applied to specific information resources such as the 'recognised maritime/land/air pictures'. The requirement for tactical systems offering a view of the battlespace has been the principal objective. The idea of a common operating picture was useful to support the notion of component commanders developing situational awareness based on access to a common tactical picture. However, there is still a lack of clarity on both what is required and how to deliver coherent solutions.

Developments

18. The information revolution, recent digitization programmes and the maturity of information superiority practice and process in Afghanistan have led to an expectation of information wealth on operations. Where this is not available to commanders, operations must be planned accordingly and

mitigation measures put in place where necessary. Where available, the quality, quantity, volumes and velocities of information associated with modern systems can create real challenges as well as opportunities. The traditional J1-9 functions of the various elements of headquarters' staffs were appropriate when the challenge was primarily one of gathering information. But now, where information is abundant, the challenge becomes increasingly one of filtering and analysis to derive operationally exploitable value.

Fundamentals

19. Commanders must define their operation-specific common operating picture requirements as part of their information superiority estimate. Subordinate functional commanders will need to define their specific functional information requirements, including how best to view this information to support understanding and decision-making. All staff will need to develop tailored views of the vast streams of information available to focus on their functional priorities and provide the most effective support to their commanders. Though it is reasonable to 'design once and use many times', the practice of providing fixed, institutionalised views which deliver pre-formatted data to users (which they cannot adapt) should be restricted to those following defined processes. A better principle is that users, as active decision-makers, should be able to access what they want, when they need it and be able to tailor the views, supported by information management specialists, such that the information makes sense to them.

Applications

20. Applications have been developed in recent years to display information from shared resources but these have often been bespoke, aiming to deliver a more comprehensive and dynamic view of the digitized battlespace. The emerging generation of common operating picture applications recognise the greater range of potential information services and the need for greater flexibility of views. As well as processes for developing the recognised maritime/land/air picture to support common operating picture requirement, we are beginning to see ideas such as cyber common operating pictures, J6 common operating pictures, recognised eligible persons, and a national operations centre common operating picture supporting the US homeland security programme.

Governance

21. There are no current UK policies which address common operating pictures. The online JTTP provides examples of concepts of operation for common operating pictures.

Section 5 – Operational users' perspectives

Rationale

22. The online JTTP outlines the various operational users' perspectives on information superiority. It also provides links to their relevant doctrine, tactics, techniques and procedures and standard operating procedures.

Executive summary

23. **Information superiority in the maritime environment**.

a. In the maritime environment, information superiority is termed 'information warfare'. This is because the notion of 'warfare officers' is well understood. Information warfare is not a separate branch of warfare akin to 'above water' or 'under water warfare' which are clearly defined. Rather it is the holistic consideration of networks, the electromagnetic spectrum, global media and cyber as an information environment which is a key enabler of warfare as a whole.

b. The Maritime Warfare Centre defines information warfare as: influencing target audiences by optimising and controlling our information flows whilst denying our adversaries the ability to do the same.[1] The online documentation provides an understanding of what information warfare includes and what it can achieve.

24. **Information superiority in the land environment**. Land information superiority policy/guidance is evolving. Relevant documentation will be published on the website once it becomes available.

[1] Definition taken from the *Maritime Information Warfare Concept of Operations (CONOPS)* Paper released June 2013. It is available at http://cui4-uk.diif.r.mil.uk/r/163/SDev/MISP/Doctrine/Forms/AllItems.aspx

25. **Information superiority in the air environment**. Air information superiority policy/guidance is evolving. Relevant documentation will be published on the website once it becomes available.

Section 6 – Archiving and recovery of operational information

Rationale

26. An important part of information superiority is assuring access to previously collected, processed and annotated material. Access will be required to fulfil commanders' responsibilities for compliance, which may be a constraint if not appropriately accommodated. The online JTTP covers extant policy for retaining operational information and factors to be considered from the outset when planning for the retaining and archiving of material. They include: the information superiority-specific aspects of information repatriation; and how to maximise its value through operational record keeping for accountability purposes, for learning, for historical analysis and subsequent use on operations.

Executive summary

27. There is a fundamental need for historical data to be available to the 'corporate body' of the UK and its allies. An important operational aspect of accessing previously acquired material is that information-gathering activities should not have to be repeated. For information superiority, a key aspect will be to be able to retrieve information. Retrieval must be timely, from and to any location, and available to any authorised user, wherever and whenever they require it.[2] Successful retrieval will rely on the availability of tools and applications that can read the materials from any format or file type, regardless of how old the material is. It may be impossible, in advance, to know whether or not particular pieces of material may be of value, hence, if in doubt, commanders should always mandate storage rather than deletion. Long-term archiving and storage solutions must be identified – most operational information will be stored at the Defence Archive Service at Northwood.

[2] This may include from non-defence archives and even from private collections.

Governance

28. The compliance element is largely driven by the Department of Judicial Engagement Policy (DJEP) task to present the pertinent information requests as part of Inquires. This is a legally-driven requirement. The policy is detailed in Joint Service Publication (JSP) 441, *The Defence Records Management* with additional direction given in DIN 2013DIN03-009: *Document and Material Retention and Preservation – Iraq and Afghanistan Operational Theatres*. All types of information are within the scope of compliance policy. This includes, but is not limited to, war diaries, photographs, videos, emails, chat-room conversations and forum threads. Other potential sources are machine-to-machine communications. This includes date stamps on phone calls, modem and fax logs, system installation records, error and firewall logs and records of system failures and malicious activity or virus infiltrations. Compliance policies and rules are still being developed (July 2013). Commanders and staffs should refer to the online resources for the most current guidance.

Section 7 – Information operating model: information superiority governance

Rationale

29. The information operating model is the governance model for providing and delivering all information superiority-related capability. The online JTTP includes a summary of the governance arrangements for all C4ISR[3] activity. It emphasises how these arrangements must accommodate the need for evolution driven by the information superiority imperatives from theatre. The online JTTP outlines the information operating model, including the role of the Defence Authority for C4ISR in supporting the achievement of information superiority.

[3] Command, control, communication, computers, intelligence, surveillance and reconnaissance.

Executive summary

30. Over the next three years, the new information operating model will deliver:

- a single focus in Joint Forces Command (JFC) for all military C4ISR joint enablers and coherence across the single Services;
- a single trading environment across information systems, led by JFC, but accommodating corporate service requirements;
- a chief information officer held to account for defining, regulating, assuring and enforcing information and communication technologies strategies and policies across Defence as well as managing and implementing cross-government requirements; and
- a common infrastructure that will meet the variety of needs across Defence, whilst driving substantial efficiency benefits.

The information operating model is being developed and guidance updated. One concern is whether the model takes sufficient note of the nature of deployed operational theatres particularly in respect to tactical adaptation. Defence transformation activity is ongoing as at the time of publishing, therefore, commanders and staffs should refer to the online resources for current information.

Section 8 – Links to online information superiority-related topics and resources

Rationale

31. This section highlights information superiority topics which are available online and provides links/hyperlinks to where these evolving electronic documents can be found.

Cyberspace resources

32. Cyberspace is an environment which has different characteristics to the physical world. Commanders will wish to exploit its properties to achieve their aims and must understand these characteristics well. Cyberspace can

be both a route to reach out and influence other actors, and a battlespace in its own right. Information superiority is different in each case. In the former, cyberspace is merely a capability to be employed to achieve effects. For example, the use of social media, video, sound clips, emails, texts and blogs which will be read by people with the intent of changing perceptions. In the latter, cyberspace is the contested space and the nature of the actors and effects, and the kind of information superiority that can be achieved are different from the real world. Monitoring cyberspace activity demands novel situational awareness capabilities. These may need to attend to the behaviour of, for example, software agents, malware and other non-human entities down to minute detail.

Additional resources

33. As additional information superiority resources are made available they will be hosted at the following URL:
http://defenceintranet.diif.r.mil.uk/Organisations/Orgs/JFC/Reference/Publications/Pages/IS-JTTP

Lexicon

Part 1 – Acronyms and abbreviations

AJP	Allied Joint Publication
AMN	Afghan Mission Network
C4ISR	Command, control, communication, computers, intelligence, surveillance and reconnaissance
COED	Concise Oxford English Dictionary
DCDC	Development, Concepts and Doctrine Centre
DJEP	Department of Judicial Engagement Policy
ISAF	International Security Assistance Force
JDN	Joint Doctrine Note
JDP	Joint Doctrine Publication
JFC	Joint Forces Command
JMEI	Joining, membership and exist instruction
JSP	Joint Service Publication
JTTP	Joint, tactics, techniques and procedures
MOD	Ministry of Defence
NATO	North Atlantic Treaty Organization
PJHQ	Permanent Joint Headquarters
UK	United Kingdom

Part 2 – Terms and definitions

Part 2 is divided into three areas. Firstly, it describes those terms used in this publication. Secondly, it lists those terms for which new definitions are proposed. Finally, it lists more general, endorsed terms and definitions, with the source annotated in brackets.

Terms used in this publication (for clarity only)

adaptable
Able to adapt oneself to new conditions.
(Concise Oxford English Dictionary (COED),12th edition, 2011).

characteristic
A feature or quality belonging typically to a person, place, or thing and serving to identify it. (COED, 12th edition, 2011).

enable
Give the means or authority to do something or make it possible.
(COED, 12th edition, 2011).

exploit
Make use of or derive benefit (from something). (COED, 12th edition, 2011).

principle
Fundamental truth or law as the basis for reasoning or action.
(COED, 12th edition, 2011).

Proposed term and its definition

information superiority
Information superiority is the competitive advantage gained through the continuous, directed and adaptive employment of relevant information principles, capabilities and behaviours. (JDN 2/13).

Endorsed terms and their definitions

adaptive approach
The adaptive approach requires a flexible and more open system, where agencies work together in a way that 'resembles jazz musicians improvising on a theme' to focus their efforts at a point of need. (JDP 2-00, 3rd edition).

conventional approach
The conventional approach has fixed lines and boundaries between departments that include rules for interagency cooperation. In effect it is a closed system. (JDP 2-00, 3rd edition).

information assurance
The confidence that the information within the Defence community is maintained reliably, accurately, securely and is available when required. (JDP 6-00, 3rd edition).

information administration
The structuring and handling of information to enable it to be stored, archived, located and retrieved efficiently, whilst ensuring its integrity. (JDP 6-00, 3rd edition).

information exploitation
The use of information to gain advantage and improve situational awareness to enable effective planning, decision-making, and coordination of those activities required to realise effects. (JDP 6-00, 3rd edition).

information management
Integrated management processes and services that provide exploitable information on time, in the right place and format, to maximise freedom of action (JDP 6-00, 3rd edition).

joint action
The deliberate use and orchestration of military capabilities and activities to realise effects on an actors' will, understanding and capability, and the cohesion between them. (JDP 3-00, 3rd edition).

manoeuvrist approach
Co-ordinated activities necessary to gain advantage within a situation in time and physical or computer-generated space. (JDP 5-00, 2nd edition).

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