



Ministry  
of Defence

Joint Concept Note 2/18

# Information Advantage

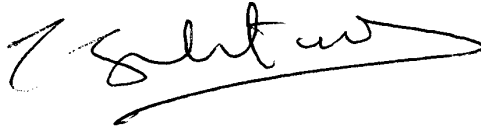




# Joint Concept Note 2/18

## Information Advantage

Joint Concept Note (JCN) 2/18, dated November 2018,  
is promulgated as directed by the Chiefs of Staff

A handwritten signature in black ink, appearing to read 'J. G. ...', with a long horizontal flourish extending to the right.

Director Concepts and Doctrine

### Conditions of release

This publication is UK Ministry of Defence (MOD) Crown copyright. Material and information contained in this publication may be reproduced, stored in a retrieval system and transmitted for UK government and MOD use only, except where authority for use by other organisations or individuals has been authorised by a Patent Officer of the Defence Intellectual Property Rights.

# Authorisation

The Development, Concepts and Doctrine Centre (DCDC) is responsible for publishing strategic trends, joint concepts and doctrine. If you wish to quote our publications as reference material in other work, you should confirm with our editors whether the particular publication and amendment state remains authoritative. We welcome your comments on factual accuracy or amendment proposals. Please send them to:

DCDC, Ministry of Defence Shrivenham, Swindon, Wiltshire, SN6 8RF.

E-mail: [DCDC-DocEds@mod.gov.uk](mailto:DCDC-DocEds@mod.gov.uk)

Telephone: 01793 31 4216/4217/4220

# Copyright

This publication is UK Ministry of Defence © Crown copyright (2018) including all images (unless otherwise stated).

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

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

# Distribution

This publication is distributed by DCDC at the address above. Our other publications, including a biannual DCDC Publications Disk, can be demanded from the LCSLS Operations Centre. Contact the Forms and Publications Section, LCSLS Headquarters and Operations Centre, C16 Site, Ploughley Road, Arncott, Bicester, OX25 1LP.  
LCSLS Help Desk: 01869 256197                      Military Network: 94240 2197

Our publications are available to view and download on defnet (RLI) at:

<https://modgovuk.sharepoint.com/sites/defnet/JFC/Pages/dcdc.aspx>

This publication is also available on the Internet at: [www.gov.uk/mod/dcdc](http://www.gov.uk/mod/dcdc)

# Foreword

We live in a data-rich information age in which the combined power of exponential growth in computer capability, data, and digital connectivity is fundamentally shaping almost every facet of modern life. Those who could adapt have thrived, others have clung to old methods and withered. Information, in all its manifestations, must change the way we execute business and prosecute warfare, both at home and overseas in an era of constant competition. Defence must harness this digital horsepower or be left behind; we have reached the tipping point. Information is no longer just an enabler, it is a fully-fledged national lever of power, a critical enabler to understanding, decision-making and tempo, and a 'weapon' to be used from strategic to tactical level for advantage.

The smart use of information through the mass customisation of messaging, narrative and persuasion, can vastly extend reach and deliver disproportionate influence on targeted audiences. It is underpinned by core digital technologies and digitally savvy people. This digital race – human and machine – is increasingly geopolitical in nature. Currently we are being challenged in a 'grey-zone' short of armed conflict by agile state and non-state actors – notably Russia – who understand our vulnerabilities and seek to exploit them through multifarious asymmetric approaches and the flouting of rules-based norms. Central to these strategic contests are 'information battles'; battles in which information is 'weaponised' and ones in which we increasingly lack the initiative.

To regain the initiative and achieve information advantage we must rapidly up our digital game, fundamentally shift the way we think, act, invest, and move with pace through the incremental development of new capabilities. Defence, as part of a national and allied effort, must become a potent and resilient strategic actor; postured for constant competition both home and away. This requires a cultural transformation and a conceptual foundation that puts information advantage at the heart of 21st Century deterrence and campaign design. Information advantage must become part of our doctrinal lexicon and joint action practice; a bedrock upon which a range of physical, virtual and cognitive effects will be built, including the use of information as an effector in its own right.

This joint concept note explains why information advantage must be at the heart of how Defence operates if we are to enable credible military options and political utility, regain and maintain initiative, and achieve influence in a more complex and competitive world. It has been written primarily for Defence and joint commanders, staffs and students; cross-government and industry partners; and principal allies. I encourage you to read it.

Air Marshal E J Stringer CB CBE

Director General Joint Force Development and Defence Academy

# Contents

Foreword . . . . .	iii
Part 1 – Introduction and context . . . . .	1
Part 2 – Information advantage . . . . .	7
Part 3 – Insights and deductions . . . . .	17
Lexicon . . . . .	23

“

War today is in the process of undergoing another evolution in response to social and political conditions, namely the speed and interconnectivity associated with contemporary globalisation and the information revolution.

”

Emile Simpson  
*War from the Ground Up*



# Introduction and context



1.1. We live in the Information Age in which the combined power of exponential growth in computer capability, data, and connectivity is fundamentally shaping the way people live and work. Today, thanks to smartphones, the Internet and social media, our perception of the world is being manipulated at an extraordinary pace and on a previously unimaginable scale. Never have so many people been connected in an instantly responsive network, through which 'memes' can spread more rapidly than natural viruses. Experts are out, opinion is in; it matters not how verifiable the assertion, it only matters that it attracts attention – true believers, sceptics, conspiracy theorists and artificial intelligence can do the rest. Information is no longer just an enabler, it is a fully-fledged national lever of power and a strategic, operational and tactical weapon. If used in a timely and coherent manner it can generate advantage over an adversary, and deliver both mass effect and precision 'fire', to disrupt, confuse, agitate and radicalise. And it not only fuels conflict, it can create

conflict. This is not some vision of an apocalyptic future; it is here today and it cannot be ignored.

## Purpose

1.2. Joint Concept Note (JCN) 2/18, *Information Advantage* identifies the requirement for a fundamental shift in the way Defence executes its business and prosecutes warfare – a transformational opportunity that must be at the heart of how Defence operates. It outlines the requirement to: further develop our current thinking regarding the use of information; invest and act differently in response to such thinking; and introduces the concept of information advantage to enhance our influence in a complex and uncertain operating environment.



### Russia and information

Vladimir Putin's Russia has many weaknesses but it has seized Crimea, launched a murderous insurrection in eastern Ukraine, meddled in elections and hacked the Danish Ministry of Defence and the Bundestag, among many other acts. Russia has adopted an assertive and constant whole-of-government approach – with disinformation at its core – to achieving strategic objectives. As the Prime Minister, Theresa May stated in November 2017:

'...[Russia] is seeking to weaponise information. Deploying its state-run media organisations to plant fake stories and photo-shopped images, in an attempt to sow discord in the West and undermine our institutions.'

From a national to an individual level, both home and away, we are being outmanoeuvred in a 'grey zone' short of armed conflict by actors unconstrained by previously accepted norms. Central to this strategic contest is an information battle; where we increasingly lack the initiative. In the shades of ambiguous indirect 'grey' that provides the context for constant competition, the Kremlin moves quickly and opportunistically, taking risks and breaking rules. Their aim is known: to play divide and rule games between western nations and within them, exploiting ethnic, political, regional, religious and social elements, increasing polarisation and weakening our political will.

## Context

1.3. Joint Concept Note (JCN) 1/17, *Future Force Concept* recognises the potential of information to deliver transformative change and disproportionate influence. To exploit this opportunity we must up our game in several key areas, and set the requirement across Defence to gain information advantage as a prerequisite for success. This is necessary because we are being outmanoeuvred in the information environment by agile state and non-state actors who understand our vulnerabilities and use multifarious, asymmetric approaches to exploit them. This involves the synchronised and persistent use of the diplomatic, informational, military (if often limited) and economic instruments of power, irrespective of the norms of the rules-based international order.

1.4. Actions by states such as Russia demonstrate that while the deterrent threat or coercive use of force remains a vital means by which military power influences people or changes the course of events, the power of a potent narrative amplified by contemporary technology offers significant advantage to adaptable and agile actors. So, in the contemporary, complex and dynamic environment, we must take account of a much broader audience than simply the 'enemy' – success will prove elusive if we continue to embrace only traditional views of conflict. Strategy is therefore increasingly sensitive to tactical actions and our perceptions of local, regional and global audience opinions. Success is, and will continue to be, significantly influenced by the extent to which competing narratives influence, or fail to connect with, audiences. We therefore need to do things differently if we are to enable credible military options, maintain our freedom of action and political utility, and achieve influence in a more complex and competitive world.

I began to understand that I was caught up in two wars: one fought on the ground with tanks and artillery, and an information war fought largely, though not exclusively, through social media. And, perhaps counter-intuitively, it mattered who won the war of words and narratives (rather) than who had the most potent weaponry.

David Patrikarakos on eastern Ukraine<sup>1</sup>

1.5. Using propaganda and disinformation is not new. What is new is the ease, global reach, speed of propagation of ideas, efficiency and low cost of such efforts, coupled with our political sensitivity to national and global opinion. We cannot control who accesses this capability and we do not hold the initiative – it is driven by commercial, societal and geopolitical forces that will determine how the technology unfolds and is used. It is effective too. The nimble player who can shape perceptions will more likely achieve their objectives. Defence must therefore become a more potent and agile strategic actor; effective in competitive and constantly evolving sensing and shaping activity against adversaries who seek to achieve strategic objectives through a pre-emptive whole-of-government approach including limited, yet swift, use of force. Doing things differently will require us to better integrate information and physical activity across multiple domains – cyber, space, maritime, land and air – to leverage our influence to deter as part of fusion doctrine, a new approach to the orchestration of our national security capabilities.

1.6. In an era of constant competition at home and overseas, influence will only be achieved with a clear and persistent focus on audiences, and effects (reassuring allies whilst presenting multiple dilemmas to adversaries). All activities in all domains must be focussed on, and complementary to, the information strategy to achieve influence. Defence, with information at its core and a clear understanding of freedoms and constraints, must seek to contribute more effectively as part of national and military strategy. Adopting a more proactive approach will require careful consideration of permissions and authorities both within and outside Defence. At the joint force level, enhancing

.....  
1 David Patrikarakos, *War in 140 Characters*, 2017.

joint action<sup>2</sup> seeks to undermine an actor's will. This is achieved by affecting their understanding and capability through the mutually reinforcing integration of information activities with fires, outreach and manoeuvre and will provide more options and greater potential to gain advantage in time and space. Although the smart use of information – through the mass customisation of messaging, narrative and persuasion – can vastly extend reach and deliver disproportionate influence on targeted audiences, our ability to deter will be underpinned by our capability and will to escalate to the use of force.

.....  
2 Joint action is defined as: the deliberate use and orchestration of military capabilities and activities to realise effects on an actor's will, understanding and capability, and the cohesion between them to achieve influence. Joint Doctrine Publication 3-00, *Campaign Execution*, 3rd Edition, Change 1.

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

Benjamin Disraeli, 1804-1881

# Information advantage



2.1. Information advantage is defined as: the credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems.<sup>3</sup> As depicted at Figure 1, information advantage can be conceptualised through four broad lenses. These are:

- information as an enabler;
- information resilience;
- information denial; and
- information as an effecter.

.....  
3 This is a working definition proposed by this publication and has not been endorsed.

# Information advantage

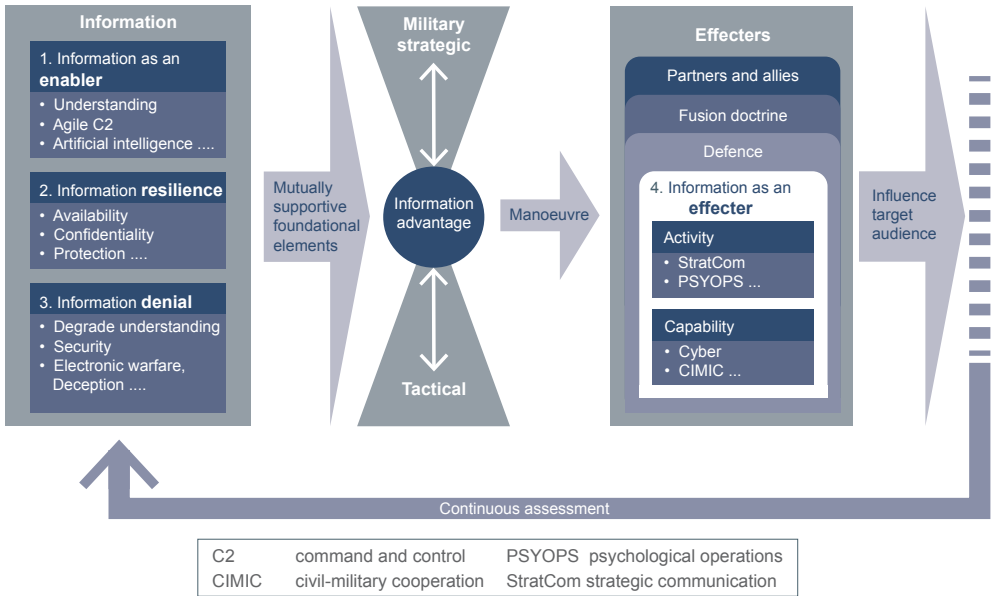


Figure 1 – The concept for information advantage

2.2. The three lenses of ‘enabler’, ‘resilience’<sup>4</sup> and ‘denial’ serve as mutually supporting foundational elements providing the potential for information advantage, specifically enhancing joint action through greater choice over applying information effectors, to influence target audiences. This enables greater opportunities to manoeuvre in the physical and virtual dimensions, which when synchronised, are key to achieving effects in the cognitive, and delivering success both today and in the future. In the cognitive dimension we aim to create friction, uncertainty and even paralysis in our adversaries to create advantage. This has profound implications for an institution imbued with the primacy of fires and physical battlefield manoeuvre. All four lenses are forms of manoeuvre, as they seek to protect and secure, to deter and deceive and ultimately deliver information advantage through effects on an adversary’s understanding, physical capability, will and cohesion.

.....  
 4 Resilience is the ability to withstand shock or disruptive influence, and continue to function (adapted from the *Concise Oxford English Dictionary* definition). Resilience is further developed in this joint concept note (JCN), drawing on recent Development, Concepts and Doctrine Centre (DCDC) research.



## Section 1 – Information as an enabler



© Collin Anderson/Blend Images/Getty Images

'We will see a progression beyond the use of machines to support the intelligence cycle, towards human/machine planning, decision-making and mission execution. Ultimately, humans and technology should be parts of the same team, with either technology providing personal assistance or with humans and machines being agents of the team.'

Joint Concept Note 2/17, *Future of Command and Control*

2.3. Information is a critical enabler to understanding and decision-making; it can significantly enhance tempo and momentum, thereby offering significant advantage. Such decision support includes articulating the credibility or completeness of information that is available, as well as clarifying where information is not available. Timely analysis and assessment, exploitable at a pace better than our adversary, and at least as good as allies, is critical to future mission success.<sup>5</sup> A general shift away from traditional command hierarchies

.....  
5 Defence Intelligence, *Information Advantage Primer* (Draft).

to more dynamic, lateral networks, with greater delegations of authority will allow decision-making to be pushed to the edges of an organisation, and the exploitation of the most relevant information at speed.

2.4. Persistent review of multiple audiences, whether they be adversarial, supportive, unsupportive or undecided, is critical to enhancing our broader understanding. Embracing developing technologies such as artificial intelligence could offer significant advantage in this area. However, we must be mindful that the pace and growth of information can risk undermining comprehension and decision-making and weaken the distinction between information and knowledge. Therefore, to be truly useful, information must be placed within a broader context of history, geography, social behaviour and psychological interactions to emerge as actual knowledge. The increasing capabilities of robotic and artificial intelligence systems will be limited not only by what can be done, but also what actors trust their machines to do. The fundamental factors affecting our trust in systems are: mechanical understanding, predictability, familiarity and context.<sup>6</sup>

## Section 2 – Information resilience



6 JCN 1/18, *Human Machine Teaming*, paragraph 4.16 to 4.17.

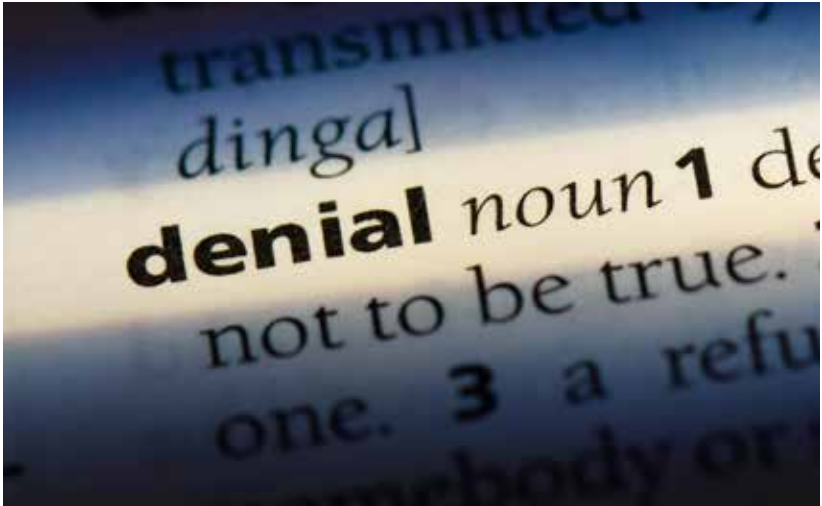
2.5. Resilience matters as it is an essential element for credible deterrence and defence against the full spectrum of hybrid threats. It is also imperative that information systems focus on the protection, confidentiality, integrity and availability of our own information. This will require us to adequately defend the data and networks which help to provide our understanding through the 'enabler' element. The development of multi-layered and multi-spectral intelligence, surveillance and reconnaissance (ISR) systems will help deliver agility and contingency, offering the ability to continue when attacked.

Resilience is about preparedness, about understanding potential vulnerabilities and looking at how best to mitigate them. Resilience is relative as threats evolve and as vulnerabilities change. No organisation, person, network or system can be absolutely resilient and so the key to resilience, whilst subject to constant change, is adaptability. Resistance, reliability, redundancy, response and recovery are the components of resilience.

*Defence Resilience – DCDC study, 2018*

2.6. Information resilience will also require the ability to defend in a contested cyber and electromagnetic domain. Resilient communications and information systems should be interoperable with partners across government and allies, with the necessary bandwidth, security, availability and agility. This resilient foundation, consisting of robust, secure and agile processes, and trained, adaptable people, must be seamless across the operational domains.

## Section 3 – Information denial



2.7. It is critical that we develop mindsets and capabilities that deny information to our adversaries – to degrade their understanding – using a layered sensor and weapon network, incorporating both passive and active measures. This does not have to focus on physical capabilities; it can range from encouraging the responsible use of social media by our own personnel through promoting and developing and continuous reinforcing of a security culture, to camouflage, concealment and deception techniques and jamming across the electromagnetic spectrum.

2.8. We also need to contest an adversary's ability to understand by developing the capability to selectively degrade and deny their space, cyber and electromagnetic capabilities, as well as adopt niche aspects such as counter-artificial intelligence capabilities. Experimentation and testing could help us to determine whether such an approach is more cost-effective than denying such capabilities through traditional kinetic activities.

The People's Liberation Army (PLA) has, over the past 15 years, acquired considerable hardware to boost its anti-access and area denial (A2AD) capabilities. Sea denial has been greatly improved by the acquisition of new submarines, anti-ship cruise missiles and modern sea mines. Several hundred fourth generation combat aircraft, an arsenal of air defence systems, and the development of an anti-satellite capability, combine to deny adversaries the ability to gain information. China is also working hard to improve its offensive and defensive cyber capabilities, including computer network attacks, electronic warfare, and setting up 'information blockades' of its computer networks.

Rajaratnam School of International Studies, Singapore<sup>7</sup>

## Section 4 – Information as an effecter

'In the information age, it's not just whose army wins, but whose story wins.'

Joseph Nye



<sup>7</sup> Summarised from *Countering Anti-Access/Area Denial Challenges, Strategies and Capabilities*, Event Report 1, December 2017.

2.9. A range of non-lethal tools and options can be used to deliver information at speed, mass and reach to effect understanding, perceptions and behaviour. The focus of activities is to create effects in the cognitive dimension and information is being increasingly 'weaponised' in this manner by our adversaries, to gain advantage. They have recognised how technology can be harnessed to amplify the power of a commanding strategic narrative, and influence attitudes, behaviours and perceptions in pursuit of strategic goals.



### Counter-Daesh – information as an effector

The UK Government's counter-Daesh task force created several cross-government bodies that successfully neutered Daesh's online presence. The UK led the coalition communications cell that effectively marshalled overt, international media and communications. This provided a strong counter-narrative, and using consistent messaging then applied a range of increasingly covert operations to negate Daesh's ability to create effect through the information domain. Much of these operations must remain secret, but as Director Government Communications Headquarters (GCHQ) has recently stated, at their most complex we were able to synchronise and fuse the special intelligence agencies output; cyber, kinetic fires, overt and covert messaging, and the military campaign, to render Daesh's online and media persona significantly downgraded to the point that the previously triumphalist ISIL brand looked badly threadbare.

2.10. Since every military action, whether it be through a bomb or a byte, produces a cognitive effect on behaviour, influence will only be achieved with a clear focus on audiences and effects, and by integrating and synchronising kinetic and non-kinetic activities conducted across the physical and virtual domains to try to achieve those effects.<sup>8</sup> Notwithstanding the challenge of orchestrating and assessing information activity we must recognise the ability of strategic communication to shape policy and develop strategy, as well as its ability to communicate our narrative and enable dialogue with audiences. This should be part of a continuous, proactive, national approach that provides a consistent link between strategy and tactics.

.....  
8 JCN 1/17, *Future Force Concept*, paragraph 2.2.



“

Central to the change in method is the idea that military operations can become a form of informational operation and seek political rather than specific military outcomes.

”

David Patrikarakos  
*War in 140 Characters*



# Insights and deductions



3.1. Translating the following insights and deductions into applied capability requirements through experimentation and testing will be critical to delivering information advantage. Development activity should be focussed upon the following elements.



## Cross-cutting elements

a. **Status of information.** At the strategic level, we should elevate the status of information by positioning it as a national lever of power rather than an underpinning element. At the operational and tactical levels, we should adopt information as a joint function and bring together the separate aspects of information operations and information management. These actions will acknowledge the broader use and potentially shaping nature of informational power. This will include such elements as cyber

and electromagnetic activities, security, media communications and intelligence.

b. **Review the levels of warfare.** Serious consideration must be given to the relevance of the accepted levels of warfare in the context of information advantage, not just for current and future military operations but also for any response to 'below threshold' hybrid activity.

c. **Culture.** We must strive to change our culture and instil an information-centric approach, as part of a whole of government effort alongside our partners and allies. Developing of a conceptual and doctrinal base that puts Information Advantage at the heart of Defence, rather than on the periphery, will help to achieve this.

d. **Embrace technology.** Rapid developments in data analytics, machine learning, processing power and connectivity, offer the potential to significantly enhance Information Advantage and raise the prospect of sustained initiative. To capitalise on developing information technologies, we must foster as part of a continuous evolution, partnerships with the commercial sector and leverage their expertise.

e. **Training.** It does not matter how good our equipment or technology is if Defence does not have sufficiently trained, educated and equipped people to exploit it. Individual and collective training must place information advantage at its core.

f. **Recruitment.** In an immensely competitive market place, Defence must fight to attract and retain people with the right skills to deliver information advantage. Data scientists, security specialists, architects, communicators, software engineers, programmers, bloggers and hackers will all have a place. Diversity of thought and perspective will pay significant dividends.



## Information as an enabler

- a. **Linking data.** Data, its management, quality and subsequent exploitation, is at the heart of information advantage; we require data that can be understood, manipulated, shared and exploited. We must cohere and align the constituent elements, including allies and partners, to deliver agility and adaptability; vulnerabilities and stove pipes must be ruthlessly eliminated.
- b. **Enhance understanding.** Defence needs a more pervasive and ubiquitous situational awareness capability, at scale and across the full spectrum of activity. Understanding how individuals, groups and organisations interact is vital to shaping perceptions and behaviours; this can be done through the development of an insight, evaluation and measurement (IE&M) model.<sup>9</sup> We must adopt an audience-centric approach and develop an ‘unblinking eye’, focussed on our target audiences.
- c. **Information architecture.** As part of realising information advantage and improve the effectiveness of information as an enabler Defence needs to strengthen its ability to deliver a government-owned open architecture for information. This must define the necessary interfaces and standards and enable delivery teams and suppliers to realise a system-of-systems that enables information advantage<sup>10</sup> – interoperability necessitates it; across domains, systems, Government and allies.
- d. **Enhance command and control.** Today, every action could reach a global audience in near real time – the time to plan and decide is subsequently dramatically reduced. Full-spectrum operations demand a more adaptable multi-level command and control construct, to assess multiple prospective courses of action and enable faster decision-making. A robustly networked collection of command and control nodes, enabling widespread access to, and the sharing of information, would improve interaction and enable the broadest possible distribution of decision

.....  
 9 Joint Warfare and Niteworks collaborative project.

10 Defence Joint Warfare, *Information Advantage*, Draft concept of employment, version 0.9.

rights.<sup>11</sup> A multi-level Defence command and control construct could also be scalable to provide the same function for Government; Defence is well placed to support the development of a national command and control element.



### Information resilience

- a. **Connectivity.** Assured and secure connectivity could be viewed as the backbone of information advantage. It is essential that resilient communications and systems are interlinked across Defence and Government, and are interoperable with allies, whilst maximising availability and agility.
- b. **Communications.** Multi-path communications can deliver reach and resilience, and enable access to real-time understanding and mission information through a 'combat cloud' resource and enhanced secure (and likely mobile) communications across the entire Defence enterprise.
- c. **Fused.** A joint approach with cross-government and commercial partners will be a fundamental element of ensuring the resilience of our operations in an increasingly contested environment. Simple messages, clearly articulated and disseminated regularly increase information integrity, resilience and confidence.



### Information denial

- a. **Deception.** Deception involves measures designed to mislead adversaries. Information can be used to create deception or as 'camouflage and concealment' to support deception. We must strive to understand where we are being deceived and the possible impact of, and counter to, that deception.
- b. **Multi-domain denial.** We need to develop and harness cyber (including electromagnetic), space, maritime, land, and air capabilities that allow us to contest an adversary's ability to gain information and

<sup>11</sup> This is referred to as 'edge command and control' in Joint Concept Note 2/17, *Future of Command and Control*.

shape the information that they do gain. We must also degrade their understanding and capability, at a time and in a manner of our choosing.



## Information as an effector

- a. **Regulations.** The proliferation of information has outpaced the development of associated rules and regulations. Defence must adapt to catch up in order to better defend its own vulnerabilities and in turn exploit adversary vulnerabilities.
- b. **Behavioural analytics.** This emerging analytical capability looks to deliver a significant capability advantage to Defence. Having greater understanding of how and why individuals and groups behave will enable predictions of how they are likely to act in the future. How information is targeted and projected to have the greatest influence will be central to this capability, which could create operational and strategic effects.
- c. **Permissions.** Within the operational domains, the level of permissions is routinely lowered to enable expeditious action and the seizing of initiative. Effective information activities require a similar degree of delegation albeit central orchestration is required to achieve consistency and to maximise influence. Adopting a more proactive approach to influence the understanding, perceptions and behaviour of specific individuals and groups will require careful consideration of permissions and authorities both within and outside Defence.
- d. **Offensive options.** Our ability to act offensively should be enhanced by adopting a far broader range of conventional and non-conventional options using information. These could include new operational tools such as offensive cyber and information activities.

## Summary

3.2. If we wish to shape the world, rather than be shaped by it, we need a fundamental shift in the way we think, act and invest. We need a strategic and 'front-footed' information advantage posture at the heart of 21st Century deterrence and, more broadly, for achieving better defence and security outcomes for national advantage. And the clock is ticking, as new technology capabilities accelerate and adversaries build skilled human-machine teams to beat us. We need to use information at the heart of a multi-domain approach integrated within a national and partnered endeavour, in a smarter, persistent and more assertive way. Senior leaders and politicians must understand information's potential for disproportionate influence and success.

# Lexicon

## Part 1 – Acronyms and abbreviations

A2AD	anti-access and area denial
DCDC	Development, Concepts and Doctrine Centre
IE&M	insight, evaluation and measurement
ISR	intelligence, surveillance and reconnaissance
GCHQ	Government Communications Headquarters
JCN	joint concept note
JDP	joint doctrine publication
MOD	Ministry of Defence
PLA	People's Liberation Army

## Part 2 – Terms and definitions

### Endorsed terms and definitions

#### **information system**

An assembly of equipment, methods and procedures and, if necessary, personnel, organized to accomplish information processing functions. (NATOTerm)

#### **joint action**

The deliberate use and orchestration of military capabilities and activities to realise effects on an actor's will, understanding and capability, and the cohesion between them to achieve influence. (JDP 3-00, 3rd Edition, Change 1)

### Terms and definitions proposed by this publication

#### **information advantage**

The credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems. (This is a working definition)











Designed by the Development, Concepts and Doctrine Centre  
Crown copyright 11/18

Published by the Ministry of Defence

This publication is also available at [www.gov.uk/mod/dcdc](http://www.gov.uk/mod/dcdc)