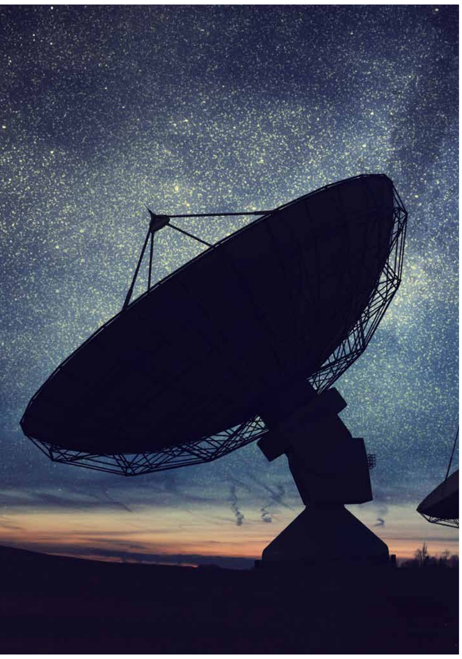
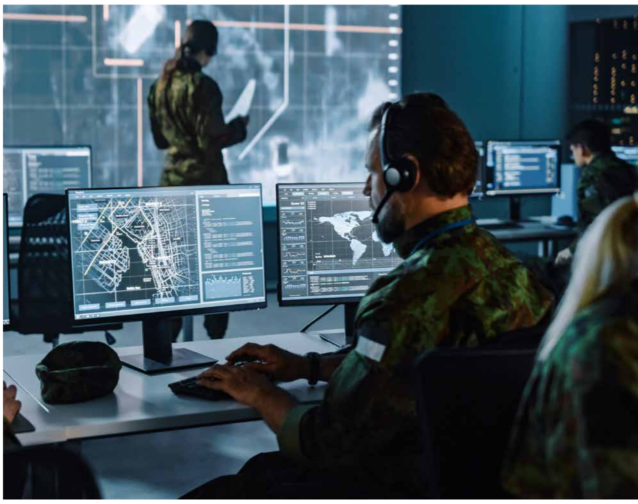




RAND EUROPE

nsc

UNIVERSITY OF EXETER

Multi-Domain Integration in Defence

Conceptual Approaches and Lessons from Russia, China, Iran and North Korea

James Black, Alice Lynch, Kristian Gustafson, David Blagden, Pauline Paille and Fiona Quimbre

For more information on this publication, visit www.rand.org/t/RRA528-1

GLOBAL
STRATEGIC
PARTNERSHIP

The Global Strategic Partnership (GSP), a consortium of research, academic and industry organisations that is led by RAND Europe, provides ongoing analytical support to the UK Ministry of Defence.

About RAND Europe

RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity

Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

Cover images (clockwise from top left): HMS Queen Elizabeth - Adobe Stock, British special forces soldiers - Adobe Stock, Military Surveillance Officer - Adobe Stock, F-35 Lightning jet lands onboard HMS Queen Elizabeth - UK MOD © Crown copyright 2020, Silhouettes of satellite dishes - Adobe Stock

Preface

This short study, led by RAND Europe on behalf of the Global Strategic Partnership (GSP), aims to review existing literature and perspectives on whether potential UK adversaries (specifically, in descending order of priority: Russia, China, Iran and North Korea) are developing similar or equivalent concepts of Multi-Domain Integration (MDI) / Operations (MDO) and, if so, how and to what effect.

The outputs of this analysis were used to help inform development of the UK's own definition and concept for MDI in the summer of 2020. This thinking was reflected in Joint Concept Note (JCN) 1/20, which was first published by the UK Ministry of Defence (MOD) in November 2020.

The GSP is an independent consortium that provides rolling academic and analytical support to the Development, Concepts and Doctrine Centre (DCDC) of the UK MOD and other parts of government. It is led by RAND Europe, a not-for-profit research institute that is part of the RAND Corporation. RAND's mission is to help improve policy- and decision-making through objective research and analysis.

For more information on the study, the GSP or RAND Europe, please contact:

James Black

Research Leader – Defence, Security & Infrastructure

RAND Europe

Westbrook Centre, Milton Rd

Cambridge, CB4 1YG

United Kingdom

jblack@randeurope.org

Table of contents

Figures, tables and boxes

Abbreviations

A2AD	Anti-Access, Area Denial
AFGS	Iranian Armed Forces General Staff
AI	Artificial Intelligence
AMS	Chinese Academy of Military Science
ASAT	Anti-Satellite
BTG	Battalion Tactical Group
C2	Command and Control
C3I	Command, Control, Communications and Information
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CCP	Chinese Communist Party
CDC	Cross-Domain Coercion
CDD	Cross-Domain Deterrence
CMC	Central Military Commission
DCDC	Development, Concepts and Doctrine Centre
DIA	US Defense Intelligence Agency
DOD	US Department of Defense
EM	Electromagnetic
EW	Electronic Warfare
GDP	Gross Domestic Product
GSP	Global Strategic Partnership
INEW	Integrated Network Electronic Warfare
IOpC	Integrated Operating Concept
IPW	Initial Period of War
IRGC	Islamic Revolutionary Guard Corps

ISR	Intelligence, Surveillance and Reconnaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
JADC2	Joint All-Domain Command and Control
JADO	Joint All-Domain Operations
JCN	Joint Concept Note
JDP	Joint Doctrine Publication
JLSF	Joint Logistics Support Force
KPA	Korean People's Army
LOC	Lines of Communication
MCF	Military-Civil Fusion
MDB	Multi-Domain Battle
MDC2	Multi-Domain Command and Control
MDI	Multi-Domain Integration
MDO	Multi-Domain Operations
ML	Machine Learning
MLRS	Multiple Launch Rocket System
MOD	Ministry of Defence
MR	Military Region
NATO	North Atlantic Treaty Organisation
NDCC	National Defence Control Centre
OODA	Observe, Orient, Decide, Act
PGM	Precision Guided Munition
PLA	People's Liberation Army
PRC	People's Republic of China
REB	Radio-Electronic Combat
ROK	Republic of Korea
SOE	State-Owned Enterprise
SSBN	Nuclear-Powered Ballistic Missile Submarine
SSF	Strategic Support Force
SSGN	Nuclear-Powered Guided Missile Submarine
SSN	Nuclear-Powered Attack Submarine

S&T	Science and Technology
TC	Theatre Command
TRADOC	Training and Doctrine Command
UAV	Unmanned Aerial Vehicle
UK	United Kingdom of Great Britain and Northern Ireland
USA	United States of America
USAF	United States Air Force

Acknowledgements

The RAND and GSP teams are grateful to several individuals for their support in the conduct of this study. Firstly, the team is thankful to DCDC for commissioning this research and to the Concepts Team for their support throughout delivery. Thanks are owed to Colonel Alan Livingstone, Commander Ben McGreal and Major Rupert Riley for their contributions. Secondly, the team is grateful to those RAND Europe and RAND Corporation experts who provided insights through internal study interviews and discussions. Finally, the team wish to thank the two RAND Quality Assurance reviewers, Ruth Harris and Luke Huxtable, and colleagues, Paola Fusaro and Zudik Hernandez, for their feedback and comments on the draft report.

While all these individuals have made important and valued contributions to this study, any and all errors contained in this report remain the sole responsibility of the authors.

1. Introduction

1.1. Context and purpose of this research

1.1.1. The UK is confronted with a strategic and operational environment characterised by complex interactions between multiple domains and fronts

To counter perceived Western military advantages, potential adversaries of the UK have developed ways of expanding the battlespace and blurring traditional conceptual distinctions between war and peace, between public and private, between domestic and foreign, and between the physical and the virtual. Against this backdrop of complexity and interconnectivity, the UK now operates in an era of persistent competition, both above and below the threshold of war. Military forces deployed on land, in the air and at sea face an increasing array of threats – whether high-tech or low-cost and improvised. Both state and non-state actors are also developing new ways and means of achieving effect in and through space, cyberspace, the electromagnetic (EM) spectrum and the information environment. At the same time, these new operational domains and environments present the UK and its allies and partners with new opportunities to exploit the vulnerabilities of adversaries.[1] Advances in Information and Communications Technologies (ICTs), as well as artificial intelligence (AI) and other emerging technologies, are also facilitating unprecedented integration across and between the domains.[2]

This proliferation of domains – and the complex interactions within and across them – increases the difficulty of developing and implementing effective strategy and operational art. This mounting challenge necessitates the development of new concepts as a guide to future capability and force development, ensuring that the UK has a coherent theory of how to prepare, operate, deter, fight and win.[3]

[1] Space and cyberspace are considered 'new' in terms of the degree to which they are now operationalised. However, it should be noted that both space and cyberspace have existed as an operating domain, to some degree, since the mid-20th century. For example, there is early evidence of electronic warfare (EW) in the First World War, as British forces experimented with jamming enemy wireless intercept operations; similarly in 1946, the RAND Corporation provided the US Pentagon with a study on the feasibility of satellites for military applications such as reconnaissance, weather surveillance, communications and missile navigation. See: Finkelstein and Govern (2015); Cleary (2020).

[2] DCDC (2015).

[3] Lindsay & Gartzke (2020).

1.1.2. DCDC has developed a concept of MDI to enable the UK to maintain advantage by exploiting the integration of activities across domains

In December 2019, General Sir Nicholas Carter, Chief of the Defence Staff, announced the UK's ambition to move beyond 'jointery' (the use of joint forces in operations) and towards 'integration'. He affirmed that deeper and more seamless integration across all of the five domains recognised in UK doctrine (land, maritime, air, cyber and EM, and space) would 'change the way we fight'.[4] To realise this vision, Strategic Command was charged with driving the transformation needed to integrate the joint force and achieve multi-domain effect.

In September 2020, the Development, Concepts and Doctrine Centre (DCDC) of the Ministry of Defence (MOD) delivered the Integrated Operating Concept (IOpC).[5] This key guidance document for the MOD and Armed Forces further emphasised the importance of integration for achieving and maximising advantage through a multi-domain approach. This includes vertical integration through the levels of warfare (i.e. tactical, operational, strategic), as well as horizontal integration across operating domains, across government (i.e. an 'integrated approach') and with external allies, partners and industry. It also entails enhanced collection and exploitation of data and metadata to enhance situational awareness, inform decision making and enable effective command and control (C2) across these different domains, levels and organisations. This guidance document recognises the key role of information in making such integration possible and thereby enabling the UK and its allies and partners to gain a competitive edge. According to the IOpC, it is through effective integration of this kind that all levers of power (diplomatic, information, military, economic, etc.) can coalesce to generate an effect that is 'greater than the sum of its parts'.

In November 2020, DCDC published a concept for Multi-Domain Integration (MDI). This set out ways by which the MOD and Armed Forces might realise the principles and objectives set out in the IOpC. The purpose of this Joint Concept Note (JCN) 1/20 is to[6]:

1. Provide and clarify the UK interpretation of MDI. As such, JCN 1/20 defines MDI as 'the posturing of military capabilities in concert with other instruments of national power, allies and partners; configured to sense, understand and orchestrate effects at the optimal tempo, across the operational domains and levels of warfare.'[7]

2. Describe the modus operandi for the operational and strategic ways outlined in the IOpC, setting out how they should be most effectively executed. Specifically, JCN 1/20 conveys how integration can be achieved across Defence (whilst acknowledging the importance of integration across other parts of government and beyond). This includes force development and management, force posture, capabilities, organisational culture, and the planning and conduct of operations.

3. Present the UK's level of ambition for MDI.

[4] Curtis (2020).

[5] UK MOD (2020a).

[6] UK MOD (2020b).

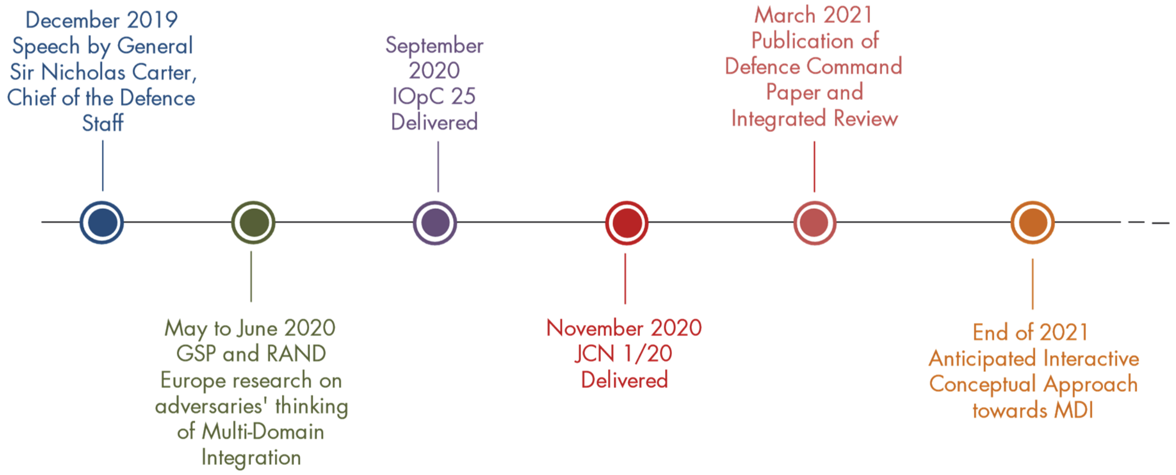
[7] UK MOD (2020b).

4. Inform the Defence Experimentation Pathway laid out in the Defence Experimentation for Force Development Handbook, recognising that further thinking is needed to inform and realise MDI.[8]

More generally, JCN 1/20 seeks to provide an initial assessment to explore and develop the UK MDI ambition. It is set to be further revised iteratively, with a new iteration and formal review scheduled for 2022.[9]

Following the publication of the first edition of JCN 1/20, in March 2021 the UK government released the Integrated Review of Security, Defence, Development and Foreign Policy.[10] This further embedded in the UK's national security strategy the logic of integration to tackle global challenges and competition. In the same month, the MOD also released the Defence Command Paper, which reaffirmed the importance of integration to achieving advantage by introducing the policy requirement for MDI.[11]

Figure 1: Timeline of development of MDI concept for the UK


December 2019
Speech by General Sir Nicholas Carter, Chief of the Defence Staff
May to June 2020
GSP and RAND Europe research on adversaries' thinking of Multi-Domain Integration
September 2020
IOpC 25 Delivered
November 2020
JCN 1/20 Delivered
March 2021
Publication of Defence Command Paper and Integrated Review
End of 2021
Anticipated Interactive Conceptual Approach towards MDI

Source: RAND Europe.

1.1.3. RAND supported DCDC's development of JCN 1/20 by investigating the nature, extent and drivers of adversaries' own evolving thinking on this topic

In developing and refining its understanding of the theory and practice of MDI, the UK not only drew on internal analysis and expertise, but also on international perspectives. This included close engagement with key allies and partners, most notably bilaterally with the United States and multilaterally through the North Atlantic Treaty Organisation (NATO). This also included gaining an enhanced understanding of the UK's adversaries' own potential concepts of MDI, as laid out in Chapter 1 of JCN 1/20 (dated November 2020).

To this aim, in May 2020 DCDC commissioned the Global Strategic Partnership (GSP), a research consortium led by RAND Europe, to examine if and to what extent the UK's potential adversaries are developing multi-domain concepts of their own, and if so, how. Specifically, DCDC tasked RAND, with

[8] UK MOD (2021a).

[9] UK MOD (2020b).

[10] Cabinet Office (2021).

[11] UK MOD (2021b).

support from Newman & Spurr Consultancy and the University of Exeter, to conduct a targeted review of open-source literature and past research into the evolving perspectives of, in order of priority: Russia, China, Iran and North Korea.

To do so, the RAND-led team spent three weeks between May and June 2020 to:

1. Review relevant open-source materials and past RAND research reports on Russian, Chinese, Iranian and North Korean concepts of – or subjects analogous to – multi-domain integration;
2. Conduct five interviews with RAND experts;
3. Generate a series of case studies outlining key concepts and the drivers behind thinking about multi-domain integration (or related ideas) in each of the four defence establishments; and
4. Identify any initial implications and cross-cutting themes arising from this analysis for further consideration in the development of the UK's own concept for MDI.

Given the limited timeframe, as well as the reliance on unclassified and primarily open-source data, the findings presented in this report are not intended to be definitive. Rather, they provide an insight into select international actors' evolving thinking on MDI and related concepts, and offer the basis for further investigation and deductions.

The outputs of this analysis were used to help inform the development of the UK's own definitions and concepts of MDI in the course of June and July 2020. In particular, they provided wider context for Chapter 1 of JCN 1/20 (dated November 2020).

1.2. Structure of this document

This draft report presents the findings emerging from this GSP analysis. It comprises the following short core chapters, as well as more detailed national case studies on Russia and China as annexes[12]:

- **Chapter 1:** Introduction
- **Chapter 2:** Outline of origin and scope of MDI
- **Chapter 3:** Overview of key trends in international approaches to MDI
- **Chapter 4:** Lessons and implications for the UK
- **Annex A:** Case study on Russia
- **Annex B:** Case study on China

[12] The research team did not include detailed case studies for Iran and North Korea due to the relative lack of publicly available information and analysis on evolving military concepts and doctrine in those two countries.

2. What is meant by Multi-Domain Integration?

The following sections examine the definitions and origins of MDI and similar concepts and terminology, most notably within the US military since the latter half of the Cold War. It also briefly considers the distinctions between 'multi-domain' concepts and related notions such as 'joint'. In doing so, it provides a baseline for comparison with non-Western thinking in subsequent chapters.

2.1. Understanding MDI

2.1.1. What are 'domains' (and how are these different or similar to 'environments'), and what does 'multi-domain' mean in high-level terms?

There is no internationally agreed definition of 'domain', and understandings of what constitutes a domain vary between countries. Latest thinking lined up with DCDC defines an 'operating domain' as:

> A distinctive sphere of capabilities and activities principally capable of, or optimised for, action in particular environments.[13]

Another useful definition currently used by NATO[14] is put forward by Dr Jeffrey Riley, who conceptualises a domain as a 'critical macro manoeuvre space whose access or control is vital to the freedom of action and superiority required by the mission'.[15]

Latest thinking lined up with DCDC recognises five operating domains that are underpinned by the information environment: namely maritime, land, air, space and cyber and EM.[16] In addition to these five operating domains, the UK MOD also acknowledges other (enabling and/or complementary) spheres of capabilities and activities, or civilian domains – such as the diplomatic and economic spheres – which may have relevance to defence operations.[17]

[13] RAND consultation with DCDC (2021). [14]

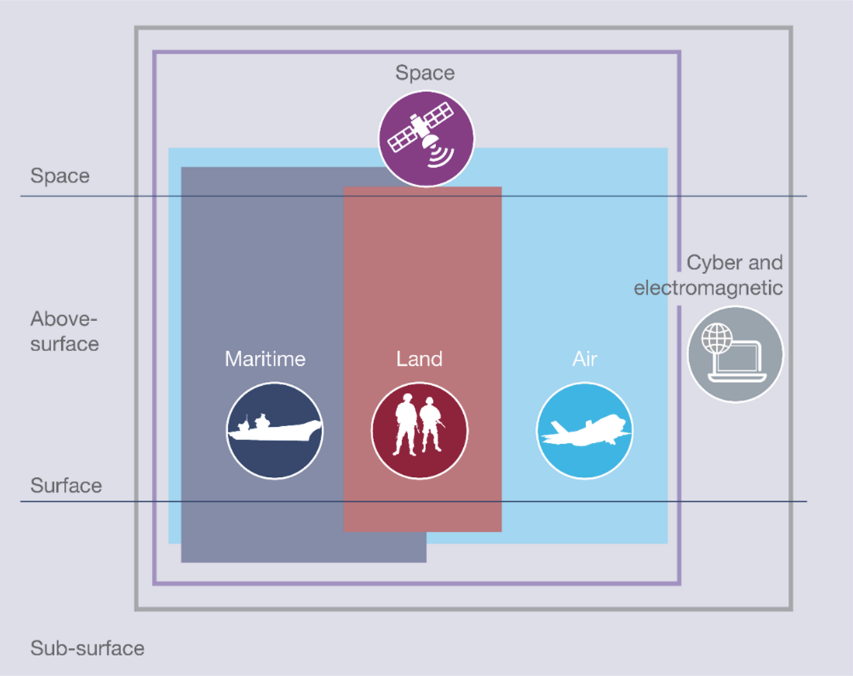
NATO C2COE (2021).

[15] Griesemer (2018).

[16] RAND consultation with DCDC (2021).

[17] RAND consultation with DCDC (2021).

Figure 2. Illustration of the UK definition of the five operating domains



Source: UK MOD (2020b).

In the military context, 'domains' are distinct from 'environments'. While these terms are conceptually similar, they should not be conflated. Latest thinking lined up with DCDC defines 'operating environments' as 'the surroundings for activities [which] exist prior to, during and after their occurrence'.[18] Joint Doctrine Publication (JDP) 0-01 also defines the 'joint operational environment'[19] as the 'overall space, conditions and surroundings within which military forces operate.'[20] By this definition, an operating environment may encompass one, some or all domains, depending on where and how a force needs to operate. In this regard, the notion of the joint operational environment more closely resembles the multi-domain concept, where the commander will utilise capabilities across a variety of domains to achieve operational and strategic goals.[21]

At a basic level, then, multi-domain concepts centre on the notion that integration across two or more of these five domains can produce an effect that is greater than the sum of its parts.[22] The new domains of space and cyber and EM further extend the reach and aim to improve the efficiency of military operations, whilst also offering alternatives to the use of military force altogether.[23]

[18] RAND consultation with DCDC (2021).

[19] UK MOD (2019a).

[20] DCDC (2015).

[21] Donnelly & Farley (2018).

[22] Lindsay & Gartzke (2020).

[23] Lindsay & Gartzke (2020).

2.1.2. What has been the evolution of MDI and related concepts (e.g. multi-domain battle, multi-domain operations or multi-domain command and control)?

Many of today's 'multi-domain' concepts have emerged from debates in the United States. In broad terms, the evolution of multi-domain thinking over the past four decades has been driven by the desire to identify solutions for the United States and NATO's most pressing military problems. These have ranged from the threat posed by the Soviet Union in the 1970s and 1980s, through to the more recent erosion of NATO's military superiority in the 2010s and the growing need to address the 'anti-access, area denial' (A2AD), 'counter intervention' and other challenges posed by potential adversaries in the European or Indo-Pacific theatres. Hostile activities by adversaries operating between the threshold of war, the exploitation of new technology and the centrality of the land battle have also heavily influenced multi-domain thinking as it has evolved.[24]

A key evolutionary step that lay the foundations for multi-domain thinking was **AirLand Battle**.[25] This concept was developed by the US Army and US Air Force (USAF) in the latter decades of the Cold War as part of a joint effort to address the challenges facing NATO planners in the European theatre. Allied forces were confronted with numerically superior and increasingly sophisticated Warsaw Pact forces, and both political and military leadership were eager to avoid having to resort to tactical or strategic nuclear weapons in the case of a mass Soviet assault. The key characteristics of AirLand Battle were the ideas of Integrated Battle and the Extended Battlefield. Integrated Battle required every asset of the air-ground team at a commander's disposal to be employed together to defeat the adversary. The Extended Battlefield idea stipulated that all echelons of the adversary's formations should be attacked simultaneously.

This concept was also closely linked with the United States' **Second Offset Strategy**, which sought to use new technologies to offset the Warsaw Pact's three-to-one numerical advantage in Central Europe. At the core of this offset strategy was heavy investment in technologies that enabled greater understanding of the battlefield, improved connectivity and increased precision. Though the Soviet Union collapsed without the United States needing to employ AirLand Battle in the warfighting scenarios for which it had been created, its principles were expanded and applied alongside new technologies as part of the so-called 'revolution in military affairs' that the United States and its allies demonstrated to swift and devastating effect in the First Gulf War of 1991.

While AirLand Battle was the product of a specific operational challenge – and certainly not a panacea for the enduring interservice rivalries within the US military and other practical limits on interoperability between domains – many of its core principles endured and evolved within Western thinking.[26] These ideas have subsequently guided development of current US, UK and NATO doctrine on joint operations, as well as being manifest in force structures, capabilities and professional military education.

Such approaches may no longer be enough. Much of today's multi-domain thinking has been driven by a growing recognition that the West's 'competitive edge has eroded in every domain of warfare, air, land, sea,

[24] Knighton (2019).

[25] D. Johnson (2018).

[26] D. Johnson (2018).

space and cyberspace, and it is continuing to erode.'[27] Over the past several decades, potential adversaries have analysed the ways in which the United States and NATO have employed modern military capabilities and tactics, and have developed doctrine and capabilities to offset or undermine Western advantages. US military thinkers have particularly focused on the challenges posed by adversaries' strategies for preventing Western forces from gaining access to theatres of operations and limiting freedom of manoeuvre; often described in the West as A2AD. The US response has included publication in 2012 of both the Capstone Concept for Joint Operations and the Joint Operational Access Concept.[28] Central to these concepts was the notion that cross-domain integration and increased jointness could offer a solution to the A2AD problem, just as AirLand Battle had sought to address the acute Soviet challenge in the latter part of the Cold War.[29]

The concepts underlying today's language and debates around **'multi-domain'** arise out of a 2013 article by Frank Hoffman and Michael C. Davies, entitled 'Joint Force 2020 and The Human Domain: Time for A New Conceptual Framework?', which appeared in *The Small Wars Journal*. This paper, which proposed the 'multi-domain' idea – though not the term itself – borrowed several intellectual positions and visualisations set out in the UK's own JDP-04, notably the concept of the 'Human Domain'.[30] It then extended them to offer a new postulate on the conduct of war:

> …we need to recognise that the Human Domain can be thought of as part of the manoeuvre space that we seek to operate within. However, this requires a broader understanding of manoeuvre, as having full spectrum and cross-domain context and applicability.[31]

Drift into 'multi-domain' terminology occurred from 2013 to the point of its formal expression in US doctrine in 2017. A flurry of articles in 2015 and 2016 clearly reflected the developing thinking on the topic within US Army Training and Doctrine Command (TRADOC) and across the US Combatant Commands (CCMD). Admiral Harry Harris, Commander of US Pacific Command (USPACOM), captured the urgency of responding to the new operational challenges facing the joint force[32]:

> I believe the future security environment will require the Services to exert influence in non-traditional domains as these domains converge and become more complex, especially if our combatant commands are to achieve dominance across those domains… [that] means the Army's got to be able to sink ships, neutralise satellites, shoot down missiles and deny the enemy the ability to command and control its forces.

[27] Knighton (2019). It should also be noted that the notion of the erosion of Western dominance is challenged by some commentators; for example, Zhang and Marquis (2015) and Huang (2019) dispute the extent to which China has, or can, fully 'catch up' with the West economically, and therefore also technologically and militarily.

[28] US DOD (2012a); US DOD (2012b).

[29] Knighton (2019).

[30] DCDC (2010, iv).

[31] Hoffman & Davies (2013).

[32] Palazzo & McLain (2016).

A speech by then Deputy Secretary of Defense Bob Work at the US Army War College in 2015 marked an important milestone. This charged the US Army with developing **AirLand Battle 2.0** as a conceptual response to 21st-century threats and scenarios. Multi-domain thinking was subsequently articulated as a concept in a joint US Army and Marine Corps white paper in 2016.[33] Secretary Work's mandate then led directly to development of the US Army's **Multi-Domain Battle** concept in 2017, as well as the USAF's own ideas around **Multi-Domain Command and Control** (MDC2),[34] and subsequent efforts to align these two streams of thinking through the 2018 **Multi-Domain Operations** (MDO) concept.[35]

The terminology used in the US Department of Defence has since begun to evolve subtly, from 'multi-domain' toward 'joint all-domain', as shown in Box 1, though the underlying principles remain similar.

Box 1. US definitions of multi-domain and related concepts

Multi-Domain Battle (MDB): The predecessor to MDO, MDB describes how US Army forces, as part of the Joint Force and with multinational partners, would operate, fight, and campaign successfully across all domains – space, cyberspace, air, land, maritime – against peer adversaries in the 2025–2040 timeframe.

Multi-Domain Operations (MDO): The current US Army TRADOC MDO concept recognises that any future war will take place across all domains. MDO aims to remove the institutional segregation of military capabilities and elevate the role of branches typically regarded as support. The main stated purpose of MDO is to prepare the United States for future joint operations against adversaries with advanced A2AD or 'counter intervention' capabilities. The focus of MDO is broader than that of MDB, extending beyond the tactical level to encompass a range of operational and strategic concerns, including approaches for shaping the theatre in the 'grey zone'.[36]

Multi-Domain Command and Control (MDC2): MDC2 is USAF's counterpart to the US Army's MDB and MDO, described as 'the ability to seamlessly analyse, fuse, and share what was once domain-centric information into a single C2 system that supports all domains and all levels of war.'

Joint All-Domain Command and Control (JADC2): JADC2 is the US Department of Defense (DOD)'s concept 'to connect sensors from all of the military services – Air Force, Army, Marine Corps, Navy, and Space Force – into a single network'.[37] The DoD often 'uses ride-sharing service Uber as an analogy to describe its desired end state for JADC2' – seamlessly sharing, fusing and analysing data from a wide variety of sources, and then supporting decision makers in cueing up the capability (here, kinetic or non-kinetic effects) needed to fulfil the mission.[38]

Joint All-Domain Operations (JADO): JADO is in many respects the United States' counterpart to the UK's concept of MDI, defined as 'comprised of air, land, maritime, cyberspace and space domains, plus the EM spectrum. Actions by the joint force in all domains that are integrated in planning and synchronised in execution, at speed and scale needed to gain advantage and accomplish the mission'.[39]

At the international level, in September 2021 NATO developed a working definition of MDC2: 'the art of establishing and incorporating pre-existing organisation structures and processes, employed to identify and

[33] Knighton (2019).

[34] Zadalis (2018).

[35] Knighton (2019).

[36] Freedberg (2018).

[37] Congressional Research Service (2021).

[38] Congressional Research Service (2021).

[39] US Air Force (2020).

counter challenges and accomplish missions to achieve objectives in a complex (and at times ambiguous) layered operating environment that may include, but is not limited to, other military actors, non-governmental organisations, and government agencies'.[40] NATO also developed its own preliminary definition of 'multi-domain', which it understood as 'occurring in more than one domain'.[41] This working approach to multi-domain – which will be further refined, most likely in the next Allied Joint Publication (AJP)-3 – does not limit the conceptualisation of domains to physical and non-physical spaces (e.g. land, air, sea, space and cyberspace), but also incorporates characteristics such as events, actors and actions. As such, NATO's working definition of multi-domain goes beyond existing US definitions by prompting thinking on the potential integration of not only forces and capabilities, but also goals and broader means. In that regard, it melds US MDO and UK MDI approaches.

Beyond the debates of defence establishments, there has also been a recent flurry of theoretical and empirical work in think-tanks and academia examining **cross-domain** aspects of strategy; a term that is sometimes used as synonymous with 'multi-domain' operations. This phraseology has been particularly prevalent in debates around '**cross-domain deterrence**' (CDD) and '**cross-domain coercion**' (CDC); namely, the practice of achieving deterrence or coercion in one domain by threatening costs (denial and/or punishment) in another domain.[42] A recurring feature in these recent works is the role of issue-linkage and escalation to achieve deterrent or coercive effect, for example with actors creating the prospect of escalatory costs in one domain to achieve initial deterrent or coercive aims in another.[43] The forces of globalisation and technological development have heightened concerns relating to CDD and CDC. The associated interdependencies and subsequent vulnerabilities within critical infrastructure, especially in space and cyberspace, are only becoming more prominent during this interconnected age, and these complex linkages create new domains in which deterrence and coercion might be practiced.[44]

2.2. Differentiating MDI from related concepts and terms

2.2.1. How is 'multi-domain' different from and related to 'joint'?

In UK doctrine, 'joint' activities require the participation of at least two Services (e.g. the Royal Navy, British Army and Royal Air Force) or the cross-cutting UK Strategic Command.[45] In other words, an operation may be described as 'joint' when actions in one domain support those in another, but there may also be situations where a single Service is operating in multiple domains, or where multiple Services engage in joint operations within just one domain. For example, the RAF does not only operate aircraft but also has specialist ground forces for airfield defence – the RAF Regiment – and an important role to play at sea through maritime patrol or the Royal Navy's carrier strike capability; while the Army and the Royal Marines – part of the Navy – have in recent decades frequently conducted joint operations in the land domain.

[40] NATO C2COE (2021).

[41] NATO C2COE (2021).

[42] Lindsay & Gartzke (2019); Blagden (2020).

[43] Internal engagement with GSP expert, June 2020.

[44] Hadi (2020).

[45] UK MOD (2019b).

The emergence of multi-domain thinking has been driven by a recognition that, in the contemporary operating environment, the focus on 'joint' is therefore no longer enough. The term 'joint' also typically refers only to the operational level; in contrast, multi-domain seeks to integrate at every level, from the strategic down to the tactical.[46] Multi-domain concepts thereby involve the convergence of capabilities within and from multiple domains; the greatest value can be achieved by drawing in as many capabilities as possible to find the most potent combinations to exploit the vulnerabilities of the adversary and meet the objectives of the activities in question. This implies a higher level of ambition and greater flexibility.

The distinction between joint and multi-domain thinking is usefully articulated by the Australian Air Power Development Centre:

> …in contrast to a joint force, multi-domain integration creates the flexibility necessary to rapidly reconfigure the existing force to design a force fit for purpose in a contextual manner.[47]

Taking a multi-domain perspective, the domains can be viewed as one ecosystem. A shift away from 'joint' towards multi-domain thinking therefore entails a requirement for new approaches to how military forces are structured and employed, as well as efforts to overcome enduring conceptual, cultural and practical barriers to greater alignment and interoperability between the Services – let alone among allied nations. Ultimately, MDI will only be fully achieved when all operational domains are combined into a single 'all-of-one' domain, at which point the very concept of being 'multi-domain' will have served its purpose and ceased to be either theoretically coherent or a useful driver of change.

2.2.2. How is 'multi-domain' different from and related to 'sub-threshold' or 'grey zone' operations?

As is the case with 'joint', the terms 'multi-domain' and 'sub-threshold' are also separate but overlapping. The lexicon and thinking around MDI is intended to guide development of the concepts and capabilities needed to operate successfully in a context not only of conventional military conflict, but also involving 'sub-threshold' or 'grey zone' operations. These describe competition between states (and non-state actors where applicable) below the threshold of open armed conflict, including the combination of military means with political warfare, economic coercion, information operations, and other levers of influence.[48] Such competition may often involve elements of ambiguity, deniability and purposeful testing and stretching of thresholds for triggering a political or military response, without spilling over into open warfighting.

The emphasis on information advantage that such grey zone competition entails, along with the related focus on harnessing synergies across the space, cyber, EM and human/psychological domains, are among the more notable similarities between multi-domain and sub-threshold concepts.[49]

The objectives presented in the US concept of MDB, for example, include 'compete short of war'; 'make denied spaces contested spaces'; 'defeat enemy campaign' and 'consolidate gains'. These reflect an

[46] Carter (2019).

[47] Air Power Development Centre (2018).

[48] Carter (2019).

[49] Galeotti (2016).

understanding of armed conflict as part of a wider continuum of competition, as well as emphasising the need for deterrence and for a theory of victory that will also enable de-escalation and political resolution. However, multi-domain concepts also encompass the full spectrum, from the sub-threshold to high-end warfighting. In this regard, characteristics that could be likened to sub-threshold concepts can be considered one aspect of multi-domain concepts, but only one part of a larger picture.

2.2.3. In outline, how is MDI conceptualised by the UK and how does this differ from other international definitions (such as those in the United States)?

In the United States today, the high-level principles of multi-domain or joint-all-domain concepts are generally well-developed; however, it remains unclear how exactly these concepts should be operationalised in practice. While the United States has begun to conduct wargames to test new conceptual thinking, many of the details are yet to be clarified.[50] While its own understanding of MDI is still maturing, the UK can draw lessons from the experiences of the United States and other nations in developing and operationalising similar concepts of their own.

At the same time, the UK does not seek to replicate US MDO/JADO or its predecessor concepts wholesale. Rather, any understanding of MDI across the UK MOD and Armed Forces must take into consideration the UK's unique geostrategic context, force structure, military capabilities and finite resources, recognising the important distinctions between the US context and the UK's position as a medium power. A key potential differentiator between the latest US and UK concepts is their different starting points: the development of US multi- or joint-all-domain concepts has been largely driven by a perceived threat from China and a need to counter Chinese A2AD in the Indo-Pacific; whereas the UK's MDI approach must be tailored to its own threat perceptions, available resources and location in the North Atlantic and Europe.

Conscious of the need to understand alternative approaches, but also where and why these diverge from the unique position and priorities of the UK, the following chapter considers cross-cutting themes emerging from how multi-domain and related concepts are being approached in both theory and practice by a selection of non-Western nations. Namely, it examines the extent to which similar ideas and debates can be inferred from military literature, investments and activities in Russia, China, Iran and North Korea.

[50] Internal interview with RAND expert, 29 May 2020.

3. What are key trends, similarities and differences in international approaches to MDI?

This chapter summarises the high-level themes arising from each of the country case studies presented in the subsequent chapters. It considers how some of the language of 'multi-domain' or similar principles to the UK's own definition and concept of MDI are expressed both in theory and in practice by each of the focus countries (Russia, China, Iran and North Korea), and provides some cross-cutting comparisons. While none of these countries have a direct and explicit analogue to the UK's MDI, there are aspects of their evolving thinking that tackle similar themes, challenges and opportunities (e.g. from new technology, from the enhanced use of information, or from new domains such as space, cyber and EM).

More detailed information is provided on Russian and Chinese perspectives in the annexes to this report. This reflects the particular significance of these two actors to concept and force development within the UK, US and NATO, as well as the greater availability of open-source information on these two nations' militaries and evolving thinking, as compared to Iran or highly secretive North Korea.

3.1. Russian Federation

Russia is refining its own variants of MDI concepts and putting theory into practice in ongoing military reforms, capability development and operations. Russia is leveraging elements of thinking analogous to multi-domain concepts to pursue asymmetric warfare against a perceived Western aggressor. This strategy focuses on the use of information to control adversary behaviour and shape the strategic environment in Russia's favour, as well as exploiting its adversaries' weaknesses to achieve maximum effect with minimal expenditure of Russia's own constrained resources. The information environment is viewed as underpinning and integrating all other operational domains (land, air, sea, space, cyber and EM), and is therefore critical for achieving asymmetric advantage and Russian success at the tactical, operational and strategic levels.

Russia adopts a broad understanding of competition, looking beyond the military domain to pursue asymmetric strategies beyond the battlefield. Russia's approach to MDI in the narrower sense of military combat operations sits within a broader Russian understanding of global strategic competition and the changing nature of warfare.[51] In preparing for future war, Russian strategists have emphasised that a whole-of-government approach to address increasingly integrated threats will be critical in high-intensity conflict.

[51] Kilcullen (2020).

In line with this vision, Russia is intentionally moving towards its own interpretations of what the UK or US might term 'multi-domain', while also incorporating elements of a 'comprehensive approach'.[52]

Russian approaches to MDI in both a broad (competition) and narrow (conflict) sense represent adaptations to Russia's perceived strengths and weaknesses. When considering the extent to which MDI concepts map across to Russian thinking, while 'the West considers non-military measures to be ways of *avoiding* war, Russia considers them *part of* war'.[53] The use of non-military measures offers an asymmetric counter to NATO's perceived battlefield dominance in 'network-centric warfare', by using a 'non-linear' or 'liminal' strategy of deploying covert, ambiguous, flexible and unconventional means to avoid the need for conflict by achieving Russian goals in the competition or shaping phase.

Russia's approach to thinking about domains and multi-domain integration does not map neatly against Western frameworks, though this is too often overlooked. The Russian military adopts its own nuanced line on the notion of domains that does not translate directly across to Western conceptual frameworks. Russian military literature often frames discussions of the contemporary or future battlefield in terms of 'systems thinking': developing a 'theory of war that posits the adversary as a system with key sub-systems or nodes', whereby the goal for Russia is to 'look past the [adversary's] force and attain strategic effects by simultaneously targeting key military, supporting or decision-making functions'. Through this theory of war, Russia would seek to break the Alliance's will to fight by exerting targeted pressure on the overall 'system' through a mix of kinetic and non-kinetic means.[54]

Even when thinking in the narrower sense of MDI for combat operations, Russia charts a course based on its ground-centric forces and setting. The Russian Armed Forces rely heavily on ground force capabilities;[55] this heightened emphasis on the land component means that missions that are necessarily 'multi-domain' and joint for the UK or US might be conducted solely by one Service (and in one domain) in the Russian context. Russian military theory and practice are also informed by geographical realities that are quite different to those of the Western Pacific theatre around which the latest US and Chinese warfighting concepts are primarily evolving.[56] Understanding the differing drivers and barriers to operationalising MDI in a Russian setting is not only important to understanding Russian thinking about integration across multiple domains. It also helps to ensure that any Western concept of MDI originally developed for a given adversary (e.g. China) and context (e.g. the Indo-Pacific) is as transferrable as possible, including to a potential future conflict with Russia in the Euro-Atlantic.[57]

Looking to the future, Russia is developing its theory and practice of integrated operations across multiple domains through several interrelated concepts. Russia is preparing for complex warfare by leveraging multiple domains and placing emphasis on emerging threats and opportunities in the information, cyber, electronic and space domains. This increasing focus on integration and information superiority is also

[52] Griesemer (2018).

[53] Kilcullen (2020) citing and paraphrasing Bartles (2016).

[54] Kofman (2019).

[55] Radin et al. (2019).

[56] Thomas (2019).

[57] Kofman (2019).

reinforced through other concepts prominent within Russian military theory and practice. Together these aim to enable Russia to seize a decisive advantage in the shaping phase of any potential future conflict:

- **New-Type Warfare:** Asymmetric operations that are waged across multiple domains, including the physical and informational, under the aegis of Russia's nuclear capabilities, to manipulate the adversary's perception, influence its decision-making process and shape its strategic behaviour in favourable directions, while minimising the use and scale of kinetic force.[58]
- **Information Warfare:** Russian understanding of information warfare has typically been divided into information-technical and information-psychological categories; these two aspects are now becoming increasingly integrated and mutually supportive.[59]
- **Reflexive Control:** A method of creating favourable conditions in order to accomplish an assigned mission by deceiving, persuading, coercing and otherwise manipulating an opponent with information specially developed for their consumption.
- **Disorganisation:** A strategy for imposing costs and disrupting an adversary's C2 in order to impede their ability to coordinate and integrate the various aspects of their plans and, in turn, provide Russia with decision-making superiority and improved likelihood of victory.
- **Seizing Advantage in the Initial Period of War (IPW):** This is rooted in the notion that readiness and willingness to fight can be the greatest determinant of success in armed conflict, and that swift and devastating action in the early phases of future conflict may be decisive.

Russian leaders follow NATO – and especially US – concepts and capability development efforts closely, both as a source of learning and alarm. The evolution of Russian military concepts has been driven in large part by a perceived threat from the West and a need to prepare for future high-tech warfare; leveraging cross-domain synergies is viewed as a means for achieving this.[60] This includes careful observation of the effectiveness of US combat operations in the First Gulf War in 1991 – which applied principles derived from AirLand Battle – and the subsequent evolution of network-centric warfare within NATO more widely.

Contemporary Russian military thinking also draws on its rich inheritance from its Soviet predecessor, while updating these concepts to reflect new technology. There are some enduring similarities between contemporary doctrine and the way that both strategic thinking and the operational art were expressed in the Soviet era. Some of the main continuities between Soviet and modern Russian thinking include: a fear of encirclement; an emphasis on seizing advantage in the IPW through decisive offensive operations that disorient, overwhelm and break the will of the adversary; and a focus on a reconnaissance-fires complex and the importance of the deep battle.[61] Old ideas are increasingly being reinterpreted and recast in light of new domains (e.g. cyber and EM) and the threats and opportunities offered by new technologies.

[58] Adamsky (2015).

[59] For example, an information-technical cyber-attack against an adversary's banking sector could expose or manipulate data about the banking sector that causes information-psychological panic in the general population. Equally, the strategic disclosure of an information-technical achievement such as a status-6 nuclear torpedo could have a considerable impact on the information-psychological stability of a US coastal region that could be a hypothetical target of such a torpedo

[60] Griesemer (2018).

[61] Thomas (2019).

Russia has also demonstrated a capacity to identify and operationalise the lessons learned from experiences in Chechnya, Georgia, Ukraine and Syria. Russian military thought has benefited from the conduct of serious lessons-learned analyses of combat operations and battlefield experimentation with new ways of warfare. Combat experiences have driven its understanding of strategic information confrontation and have influenced the development of both the theory and practice of disorganisation. Recent examples of Russian operations in Ukraine highlight how Russia has begun to operationalise its concepts analogous to multi-domain thinking through new-type war to achieve 'time, space and operational advantage'.[62]

Russia continues to implement major reforms and invest in new equipment and research to help integrate and modernise its forces, but important barriers to MDI remain. The restructuring of Russia's military over the past two decades highlights its deliberate efforts to create a more cohesive, integrated force. Recent modernisation and procurement efforts appear to reflect a recognition of the requirements for practical integration across the Armed Forces, within the constraints of available financial and technical resources.

Russia remains beset by structural challenges and shortcomings but continues to adapt in pursuit of advantage across military and non-military domains. Despite its difficulties, it is expected that Russia's thinking on MDI and related theories will continue to evolve; new concepts, tactics and methods are being continuously developed, drawn from lessons learned from its ongoing operations, as well as being driven by technological developments, observations of Western (and emerging Chinese) approaches and a desire to exploit the opportunities that these present.[63] The way in which Russia is continuing to consolidate and reinterpret established (often Soviet) strategic and operational concepts to address new domains and new technologies is expected to provide a model for further conceptual development in the future.[64]

3.2. People's Republic of China

The People's Liberation Army (PLA) envisages future warfighting as a multi-domain confrontation between competing 'systems of systems', but China seeks to avoid needing to fight openly by integrating all levers of power to gain dominance in the competition phase. When conceptualising China's approach to MDI or related concepts, it is useful to distinguish between 'broad' (geopolitical and strategic competition) and 'narrow' (military operational) concepts.[65] China's evolving strategic concepts are characterised by a multitude of layers of multi-domain thinking; they are broadly defined and designed to affect future military engagement, but with various degrees of removal from the actual battlespace, in what Chinese military writing calls the *war space* (to be differentiated with the *combat space*, where physical conflict occurs).[66]

China's broad understanding of strategic competition is reflected in theories of 'Unrestricted Warfare', as well as its 'Three Warfares' doctrine. China understands the current state of great power competition as a continuous effort to bring all available military and non-military levers to bear in pursuit of its grand strategic objectives; this is reflected in its emphasis on Military-Civil Fusion (MCF) and on the Three

[62] Sprang (2018).

[63] Thomas (2016); Griesemer (2018).

[64] Griesemer (2018).

[65] Internal interviews with RAND expert, 29 May 2020.

[66] Burke et al. (2020).

Warfares doctrine, which built on the tenets of Unrestricted Warfare.[67] Parallels can be drawn with Western notions of a 'whole-of-government', 'comprehensive' or 'integrated approach', although distinguished by the unique structures and levers both of the Chinese state and of the Chinese Communist Party (CCP) behind it.

In parallel, China is preparing for the possibility of future high-intensity warfighting, based around concepts of 'informatised warfare'[68] and multi-domain 'systems confrontation'. China employs an unconventional approach, using all levers of power to position itself for advantage below the threshold of armed conflict. Nonetheless, the PLA's ongoing efforts to prepare for future multi-domain conflict present a 'pacing threat' to the United States' and NATO's military dominance.[69] This means that, in addition to its bandwidth challenge from Chinese strategic competition by non-military means, the West is also distracted by the need to defend a diminishing lead in terms of its capacity and capability for open military confrontation.

Chinese literature recognises the growing importance of cyber, space and the electromagnetic environment, as well as the cognitive domain. PLA literature suggests that China's understanding of military domains encompasses the traditional domains of air, sea and land, as well as increasing formal recognition of the space,[70] cyber and electromagnetic domains – with the information domain as first and foremost in importance.[71] The PLA appears to be seeking to develop increasingly integrated systems and force structures that can conduct operations in and across all these domains to combine a range of kinetic and non-kinetic effects.[72] The PLA has also expressed wishes to deepen integration between all command levels – including at strategic, operational and tactical level – in support of its approach to integrated joint operations.[73]

The PLA focuses on military operations under informatised conditions, seeking to confront, disrupt and ultimately prevail over an adversary's system of systems. Most important to the PLA's theory and practice of 'integrated joint operations' are the notions of 'informatisation' and 'systems confrontation', which share many of the central characteristics of what the West might describe as multi-domain concepts[74]:

- **Informatised Warfare:** This term describes the process of acquiring, transmitting, processing and using information to conduct joint military operations across the military domains during a

[67] Qiao & Xiangsui (1999).

[68] China's concept of 'informatised warfare' is currently evolving into a new, closely related concept of 'intelligentised warfare', catalysed by the advent of Artificial Intelligence/Machine Learning (AI/ML), advanced data analytics and cloud computing. Intelligentised warfare seeks to leverage the opportunities of disruptive technologies to enable human-computer hybrid operations in support of an evolved systems-of-systems approach to armed conflict. See: Burke et al. (2020).

[69] In this context, a 'pacing threat' refers to a competitor who may most plausibly contest, and thus shapes, the adversary's defence strategy.

[70] China officially designated space a new domain in its 2015 Defense White Paper.

[71] Beauchamp-Mustafaga (2019).

[72] Internal interview with RAND expert, 2 June 2020.

[73] Burke et al. (2020).

[74] Scouras et al. (2017).

conflict, utilising 'near-real-time shared awareness of the battlefield in enabling quick, unified effort to seize tactical opportunities'.[75]

- **Systems Confrontation:** China's 'basic operational method' of warfare seeks to overcome advanced adversaries by systematically targeting the linkages and nodes that hold an advanced network-centric force together as a cohesive whole, rather than focusing on destruction of individual forces or platforms (e.g. troops, aircraft, naval vessels).[76] This idea is also sometimes known as 'target-centric warfare' (TCW).[77]

Contemporary Chinese theory and preparations for future high-end warfighting shares parallels with Western thinking, but is tailored to China's unique context. China appears to be developing its own multi-domain concepts that take into account its own military culture and history, and both its capabilities and capability gaps. While the space and cyber domains are viewed in a similar manner to the United States, Chinese doctrine arguably places even greater emphasis on the role of information, which it views as critical for shaping the strategic environment in its own favour and gaining and maintaining advantage against a militarily superior adversary.[78]

Contemporary Chinese thinking is informed both by internal factors as well as lessons derived from US-led military operations since the First Gulf War. Much of China's contemporary thinking on the future of multi-domain concepts (such as systems thinking and informatisation) appears to be drawn directly from observing lessons learned from two decades of US post-Cold War operations and the revolutionary impact of information systems in these contexts,[79] then developing its own concepts in response based on its own military culture, geostrategic position and own technical capabilities.[80]

Geostrategic considerations and China's growing political ambitions have also given impetus to an increasing focus by the PLA on more offensive operations. The capability and force structure requirements of system confrontation are actively driving PLA reform, acquisitions, training and doctrine to prepare China for integrated operations in informatised conflicts against an advanced adversary.[81]

Modernisation of the PLA remains an incomplete and ongoing effort, but there is evidence for progress in operationalising China's own multi-domain concepts. The ambitious scheme of military modernisation, reforms and restructuring pursued by the PLA in recent years has been designed to enhance the PLA's ability to engage in integrated operations between services and across the military domains.[82] China's recent and ongoing procurement efforts similarly reflect its pursuit of informatisation, which requires the incorporation of information systems throughout the PLA. The PLA has also implemented a range of personnel, education

[75] DIA (2019a).

[76] US Joint Staff (2018).

[77] Burke et al. (2020).

[78] Internal interview with RAND expert, 1 June 2020.

[79] Engstrom (2018).

[80] Internal interview with RAND expert, 1 June 2020.

[81] US Joint Staff (2018).

[82] Cozad (2016); Kania & Costello (2018); DIA (2019a).

and training reforms, and recent exercises across the military services indicate a focus on greater connectivity and integration between services and across the domains.[83]

China's concept of systems attack is not yet fully reconciled with its current capabilities, but it is investing heavily to make its theory of victory a reality. It is unclear when the PLA expects to achieve its desired level of dominance, or the 'ability to win informationised local wars'. Some PLA sources expect that this may be achieved in the 2020s, but other sources indicate that this will not be feasible until President Xi's 2050 aimpoint.[84] China's integrated, informatised multi-domain doctrine is reflected in its current acquisitions, capability development and training patterns, but in future it may be demonstrated in its operations.[85]

3.3. Islamic Republic of Iran

Iran's military strategy is driven by historical distrust of the United States, as well as its military resources and geostrategic position. Iran's military strategy is shaped by five main drivers: historical distrust and ongoing confrontation with the United States; the need for military self-reliance, as Iran must provide for its own security without support from foreign allies; the need to optimise military expenditures and develop indigenous military technologies, given the impact of decades of sanctions; the need to adopt a strategy of asymmetric warfare, given the mismatch it faces between threats and resources; and the need to project influence into the wider Middle East, including through proxy groups and unconventional warfare, to counter US (and also Saudi) influence and target the US military presence and basing.[86]

From its strategic writings, Iran appears to view modern warfare as a spectrum with multiple levels of conflict, including 'soft' and 'hard' war.[87] Iran perceives the United States and its regional and global allies to be engaged in a 'hybrid war' to subvert the Iranian regime and its objectives, blending conventional and unconventional tactics with all levers of state power.[88]

Iranian concepts of future warfare are grounded in an overarching strategy of 'active defence' and deterrence, employing conventional but also asymmetric capabilities, to resist US invasion. This does not mean that military leadership in Iran understands modern warfighting as defence-dominant; instead, this is a concession to the necessities of Iran's geopolitical position in a divided region surrounded by US allies, as well as Tehran's constraints in accessing foreign technologies or systems to outfit its Armed Forces for conventional power projection and offensive operations. This active defence strategy involves a focus on conventional and unconventional capabilities for A2AD, as well as projecting regional influence and even targeting the United States itself.

Accordingly, offensive doctrine is 'distinctive or notably absent' in Iranian strategy and capabilities. Specific concepts and capabilities for conducting joint offensive operations are comparatively immature, given this longstanding focus on active defence (if with regional power projection through proxies and

[83] IHS Jane's (2020b).

[84] IHS Jane's (2020a).

[85] Gibson (2019).

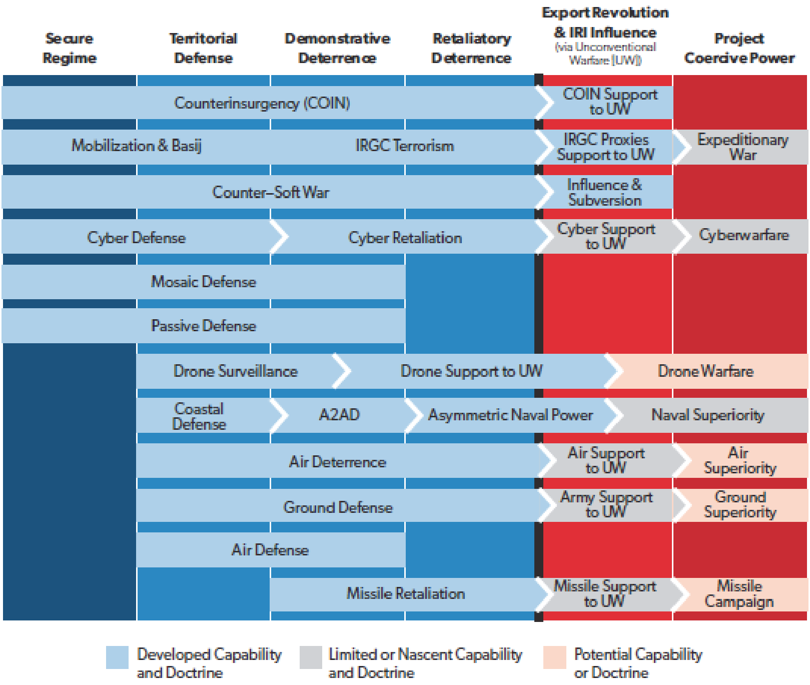
[86] Ajili & Rouhi (2019, 140).

[87] McInnis (2017).

[88] DIA (2019b, 23).

unconventional forces), as outlined in Figure 3 below. Overall, Iran continues to lack offensive doctrine for the projection of conventional military power aiming to coerce an opponent; seize ground, air, or maritime space; or destroy an enemy's forces. However, in support of Tehran's regional and global foreign policies, the Islamic Revolutionary Guard Corps (IRGC) or its proxy forces conduct unconventional or asymmetric warfare, including information operations, cyber-attacks and covert activities, against Iran's adversaries.[89]

Figure 3. Summary of mature and emerging Iranian doctrinal concepts



Source: McInnis (2017).

Iran understands conflict in 360 degrees, with its conventional and unconventional forces tasked with territorial defence against external aggression, but also resistance of internal unrest or subversion. Tehran understands the enduring necessity of developing capabilities to deter and resist foreign – assumed to be US-led – military incursion, but also prioritises securing the regime against threats on the domestic front. This not only relates to internal repression, but also demonstrates a strong focus in Iranian military thought on the threat of hostile information operations, including through psychological warfare, espionage, cyber and EW means, and targeted deployment of special operations forces. Iran has consequently created specific organisations – such as the Basij – for domestic mobilisation to counter this.

Against hostile conventional forces, Iran emphasises 'passive and mosaic defence doctrines to provide cost-imposing deterrence strategies in addition to more creative physical defences'.[90] The concept of 'Mosaic Warfare' recognises the effectiveness of US network-centric warfare and the importance of maintaining a capable Iranian resistance even when key nodes in Iran's overarching C2 system have been neutralised through kinetic and non-kinetic attack. Through mosaic warfare Tehran aims to promote flexibility and creativity, empowering local commanders to utilise multi-domain capabilities (and

[89] Paul et al. (2018).

[90] McInnis (2017).

unconventional forces) to mount a layered defence and prepare their area of responsibility for sustained insurgency within Iran's borders, even in the absence of instructions.

This approach seeks to develop overall resilience within the integrated Iranian defence 'system', as opposed to relying on the survivability of key nodes or linkages within that system in the face of a possible sustained assault by a US-led coalition employing sophisticated precision strike capabilities as well as cyber and EW. In many respects, this represents a defensively oriented mirror to Russian and Chinese 'systems thinking' (see Section 3.1 and 3.2).

Iran's doctrine of 'Retaliatory Deterrence' includes asymmetric warfare in combination with missile forces, and increasingly involves the use of cyber. Iran's deterrence strategy is centred on the principle of 'Retaliatory Deterrence' or 'Threat in Response to Threat'; namely, the principle of responding to an attack through retaliatory actions that inflict pain on the adversary, to dissuade them from aggression or to de-escalate quickly.[91] Iranian military leaders often refer to this doctrine as Threat in Response to Threat.

Iran is shifting towards a multi-pronged approach to retaliatory deterrence that exploits the opportunities offered by new domains and technologies. In addition to the enduring threat of terrorism and insurgency posed by the IRGC's Quds Force and regional proxies, Iran continues to develop long-range ballistic and cruise missile systems[92] to compensate for a lack of long-range airpower,[93] while also increasingly investing in forces and capabilities for cyber and information warfare.[94]

There is also an ongoing effort by Tehran to develop 'more professional, integrated and interoperable Armed Forces'.[95] This is reflected in reform and restructuring of the Armed Forces General Staff (AFGS) from 2016. This reshuffling included replacements for the AFGS deputies for logistics and interservice coordination, which may indicate a recognition of 'the need to better manage Artesh-IRGC joint operations overseas' in light of experiences in Iraq, Syria and elsewhere.[96] However, the enduring competition and duplication between the Islamic Republic of Iran Army (the Artesh) and the IRGC represents a continuing barrier to efforts to boost interoperability for joint and multi-domain operations.

3.4. Democratic People's Republic of Korea

There is comparatively little official information in the public domain on North Korean concepts and doctrine, including how these relate to Western notions of MDI. The lack of regime transparency makes it difficult to understand in detail what capabilities are being developed, how mature these are, and what overarching strategy and concepts of operations are being put in place.[97] This includes uncertainty over the

[91] McInnis (2017).

[92] Iran's ballistic missiles remain relatively inaccurate, meaning that they remain primarily terror weapons that cannot be used to deliberately destroy an adversary's critical nodes, although the IRGC's cruise missiles may close this capability gap. See McInnis (2017, 17–20).

[93] DIA (2019b).

[94] Paul et al. (2018).

[95] McInnis (2017).

[96] McInnis (2017).

[97] Bennett, cited in Tasic (2019).

nature or extent of North Korean concepts analogous to MDI, and the salience of the entire framework of 'domains' as a guide within North Korea's own military thinking.

North Korean strategy and tactics have evolved in line with the regime's 'juche' ideology, as well as from lessons learned from Soviet combined arms doctrine and Chinese irregular warfare. The Korean People's Army (KPA) identifies as a 'Maoist-style army that relies heavily on large armour, infantry and artillery formations', with comparatively less emphasis on multi-domain operations using airpower, given the limited capacity of the Air Force to conduct precision strikes or contest air superiority against modern forces.

Combined arms and joint operations are important pillars of KPA doctrine for conventional warfighting. The KPA doctrine states that joint operations should be used for most missions, and any major attack against long-term adversary South Korea/the Republic of Korea (ROK) is expected to involve integration of Korean People's Air Force (KPAF) and Korean People's Navy (KPN) units into the adversary's rear areas in support of a primary ground offensive.[98]

North Korean conventional military actions in recent years have showed the limitations of the KPA and precipitated a shift towards alternative approaches beyond the land, air and maritime domains. Experiences such as the Yeonpyeong Island incident in November 2010 exposed the limitations of North Korean conventional warfighting capabilities. This has precipitated a shift towards nuclear deterrence and bargaining, as well as developing asymmetric capabilities in emerging operational domains.

North Korea's approach to conceptual and capability development in the last decade suggests an 'asymmetric strategy' in preparation to conduct 'hybrid war'.[99] This approach seeks to 'oppose an adversary of greater military power and capabilities' and specifically 'targets key vulnerabilities or dependencies of that adversary to create a major psychological impact that affects initiatives, actions or will'.[100] North Korea 'relies on nuclear and ballistic missiles and a huge standing army, along with other asymmetric capabilities – such as cyber, electronic and information warfare – to deter aggression from outside entities'.[101] There is also a growing emphasis on the North Korean Special Operations Forces (NKSOFs) to conduct sabotage, disrupt adversary lines of communications (LOCs) and seize or neutralise key command, control, communications and information (C3I) nodes within the ROK.[102]

North Korea has recognised the growing importance of the information domain, as well as use of cyber, EW and space to exploit adversaries' vulnerabilities. The shift in North Korean priorities from developing conventional military forces for land, and to a lesser extent air and sea, is reflected in the move away from a focus on developing artillery and missile systems before 2012, to EW and offensive cyber capabilities between 2012 and 2017, as well as electromagnetic pulse weapons thereafter.[103] There appears to be a growing interest in developing ways and means of exploiting perceived US and ROK vulnerabilities in the information domain, seeking to bring national will and alliance cohesion by targeting the fabric of the adversary's society, economy and critical infrastructure. In future, this could include 'using physical and

[98] US Army TRADOC (2015, 17).

[99] Hoffman (2007).

[100] Tasic (2019).

[101] Paul et al. (2018).

[102] Tasic (2019).

[103] Tasic (2019).

virtual networks to mobilise support and disseminate information; and employing psychological operations and perception-management techniques at the domestic, regional and global levels to maintain favourable information-management flows'.[104]

Integrating and coordinating effects across multiple domains is viewed as a 'force multiplier' and the North Korean regime 'effectively synchronises its propaganda and official statements with bellicose actions, including missile launches, in an attempt to reinforce the severity of its threats' to enhance deterrence.[105]

This embrace of new operational domains has been reinforced by the establishment of dedicated units, though the effectiveness of joint and multi-domain integration remains unclear. North Korea has developed specialised military and civilian units dedicated to electronic, cyber and information warfare, along with 'surprisingly sophisticated computer and informational capabilities, as well as the institutional base to support these activities'.[106] Internally, the regime also has near total control of all forms of media, including the Kwangmyong (North Korea's limited version of the Internet), supporting its psychological targeting of domestic audiences to promote regime survival.

North Korea's use of both information and cyber warfare 'has largely been viewed as successful' and an efficient use of finite resources. This is important even with the regime's military-first doctrine and heavy spending on defence as a proportion of Gross Domestic Product (GDP), given the small size and fragility of the North Korean economic base. By some reports, North Korea invests 10–20 per cent of its military budget in cyber.[107]

3.5. Summary of cross-cutting themes

While national approaches to multi-domain thinking are shaped by their unique environments, aims, military and political cultures and historical doctrine, several common themes can be identified:

[104] Tasic (2019).

[105] Paul et al. (2018, 138).

[106] Paul et al. (2018, 127).

[107] Paganini, cited in Paul et al. (2018).

Box 2. Summary of cross-cutting themes

In understanding the multi-domain approaches of potential adversaries, it is useful to distinguish the 'narrow' military operational aspects from the broader context of geopolitical and strategic competition. In their strategic thinking, both Russia and China transcend the military domains, also drawing upon non-military levers to shape the strategic environment in their favour, with the aim of avoiding military confrontation while achieving desired military-strategic effects. Iran and North Korea similarly understand themselves to be engaged in an ongoing 'hybrid' war with the United States and its allies, and seek to exert influence regionally to avoid direct armed confrontation.

Russia, China, Iran and North Korea emphasise superiority in the information domain as critical to success in a multi-domain conflict. In their emerging multi-domain thinking, Russia and China place primacy on the role of the information domain; both as a critical integrator across the other operational domains, and for deceiving, confusing, disrupting, dividing, influencing and ultimately defeating an adversary with superior conventional forces. Iran and North Korea also see information superiority as essential, both to target perceived vulnerabilities in adversaries' societies and decision making, as well as to secure their regimes against internal subversion.

The emergence of multi-domain thinking in Russia, China, Iran and North Korea has been largely reactive, shaped by threat perceptions and their own geostrategic realities. While also shaped by their own military cultures and historical doctrine, Russian and Chinese thinking on multi-domain concepts has been shaped by a perceived threat from Western adversaries and a need to counter an advanced opponent through asymmetric means; for example by seeking to exploit vulnerabilities in information and communications systems.

'Systems thinking' shapes adversary approaches to countering perceived Western military superiority. Potential adversaries have analysed Western systems, capabilities and tactics, observing the critical and growing continued reliance on timely cross-domain information-sharing between separate air, land, maritime, space and cyber. Russian and Chinese strategies seek to exploit the vulnerabilities in the interdependent systems of their opponents to minimize their advantage in every domain. Systems matter more than domains, as reflected also in the ways in which responsibility for multiple domains are integrated within single armed services. Iran similarly seeks to increase the resilience of its own 'system' to mitigate the effects of adversary action against its C3I, including through promotion of passive defence and mosaic warfare doctrines.

In the absence of explicit doctrine, some activities are indicative of multi-domain concepts. Neither Russian, Chinese nor Iranian doctrine contains explicit reference to MDI. North Korean thinking is even more difficult to discern, given the lack of regime transparency. However, it is possible to infer a multi-domain posture from these nations' force configurations. Recent modernisation efforts and military reforms in Russia and China highlight deliberate efforts to operationalise multi-domain concepts; both countries are pursuing more integrated force structures to achieve combined effect across the domains. Iran and North Korea have similarly invested heavily in new capabilities and force structures to exploit the cyber domain and electronic and information environments.

Russian and Chinese theories of victory emphasise seizing a decisive advantage in early stages of conflict. The emergence of cyber, EW and information technologies has provided Russia and China with early windows of opportunity for success, by degrading or denying the adversary's access to information in the early stages of conflict. This approach is designed to achieve greater effect against a militarily superior adversary, while reducing risk to its forces or mission. North Korea similarly envisages a decisive and devastating assault on the ROK – or the use of threats to that effect – to achieve its strategic objectives before US firepower can be brought to bear.

Source: RAND Europe analysis.

The annexes provide a much more detailed examination of the ways in which Russia (Annex A) and China (Annex B) are approaching multi-domain integration or related ideas, both in theory and in practice. Additional annexes are not provided for Iran and North Korea, given the relative paucity of open-source information on their respective concepts, doctrine and capabilities – especially in relation to their relevance to MDI. Some key lessons and implications for the UK arising from the GSP's analysis of these case studies are summarised in the next chapter.

4. What are the lessons and implications for the UK?

As outlined in this short study, broad similarities in the ways that the UK's potential adversaries are conceptualising and implementing MDI or related thinking present some important lessons for the UK. Based on current understandings of evolving Russian, Chinese, Iranian and North Korean approaches, this chapter highlights the implications and considerations for the UK.

Given the limited timeframes and remit of this GSP study, considerations presented in this chapter are intended to inform DCDC and wider MOD thinking, but further analysis would be required to develop robust implications and deductions for the UK's future force.

4.1. Lessons and implications

Consideration of lessons learnt from selected international perspectives highlights the following:

There is an important difference between multi-domain doctrine and multi-domain posture, and the UK should seek to bridge that gap in its own approach to MDI. Neither Russia, China, Iran or North Korea have an explicit 'multi-domain' doctrine; however, it is possible to infer a multi-domain posture, or elements thereof, from their force configuration and investment priorities. Reconfiguring force structures to enable greater synergies across the domains – as well as investments in enablers such as space, cyber, EW and C2 systems – are important examples of how the UK's potential adversaries are taking practical steps to operationalise their own versions of multi-domain thinking. Some of China's and Russia's multi-domain aspirations do not yet fully translate into capability; however, ongoing procurement efforts and ambitious military reforms indicate a deliberate move towards MDI.

The UK should not project Western constructs onto adversary approaches to multi-domain thinking, but must understand them on their own terms if the UK is to effectively counter them. While multi-domain concepts have been advanced as a solution to challenges such as Chinese and Iranian A2AD or Russian 'hybrid' warfare, these perceived challenges are themselves Western constructs and not terms or strategies that feature in Chinese, Iranian or Russian thinking. While these heuristics provide a useful means for understanding and articulating the contemporary threat environment, projecting these Western concepts onto non-Western nations' actions may distract the UK from nuanced but important developments in the evolution or implementation of multi-domain thinking by its potential adversaries.[108] In the same way, it should be noted that potential adversaries do not necessarily understand the 'domains' – or indeed, 'war' – in the same way as the UK and its allies; which leads to the following, related conclusion:

[108] Thomas (2019).

Potential adversaries do not possess perfect knowledge of UK and Western concepts or intentions, raising the risk of unintended consequences if each side misreads the other's approach to MDI.[109] Russia, China, Iran and even highly centralised North Korea are not homogenous, monolithic actors, and there remains considerable internal debate over future doctrine and strategy. Nor are these actors fully rational or possessed of perfect self-knowledge, let alone an objective read on Western capabilities, competence and intentions. It is tempting to ascribe intentionality to an opponent's actions, while at the same time being painfully aware of the many internal squabbles, compromises and errors made on one's own side in implementing a particular concept, reform or course of action. Perceptions matter; failure to reflect on how the UK and allied approaches to MDI are understood, wrongly or rightly, by potential adversaries could undermine deterrence and strategic signalling, both in peacetime and in a crisis.[110]

The broader (political, economic, informational) aspects of MDI should not be underestimated. While recognising the importance of a 'narrow' understanding of MDI in order to focus the military aspects of its approach, it is important to recognise that the military aspects are only one of the levers of state power that adversaries are exploiting to seek an advantage over the West. In other words, the multi-domain thinking of the UK's potential adversaries acknowledges the value of non-military measures for achieving a desired effect in the military domain. In the Russian case, this is reflected in the unusual constellation of departments and agencies that fall within the defence establishment, including not only the traditional Armed Forces but also organisations responsible for humanitarian aid and other mandates that in the UK or US settings would be seen as non-defence, interagency matters. An important aspect of multi-domain competition is the ability to use levers of power across the military, political, economic and informational domains to shape the strategic environment; a notable deficiency in current Western thinking is a failure to fully appreciate this.[111] In this regard, the UK's MDI and Fusion Doctrine or 'integrated approach' should be treated as mutually supportive; both to effectively challenge the multi-domain strategies of its adversaries, but also to achieve similar multi-domain effects to shape the UK's strategic environment to its advantage and minimise the expenditure of military resources.

The new operating domains of space, cyberspace and EW offer new opportunities to probe, test, influence, disorientate and ultimately unravel adversaries in the early stages of conflict. The UK's adversaries have recognised these opportunities and have focused on harnessing new technologies to generate cross-domain synergies to achieve advantage in the early stages of conflict. While the importance of seizing advantage during the initial stages of conflict is not a new concept, advances in cyber, EW and information technologies have created new opportunities in this space, while also potentially accelerating or condensing the IPW. In its MDI approach, the UK could usefully set out its own methods for ensuring that it is able to secure an advantage during the initial stages of conflict and translate early tactical success into strategic advantage (i.e. with a clear theory of victory and clearly identified mechanisms for bringing about a political resolution on favourable terms); it could also take measures to ensure resilience against the use of such measures by adversaries.

[109] Kilcullen (2020).

[110] Lindsay & Gartzke (2020).

[111] Internal interview with RAND expert, 29 May 2020.

MDI is not a panacea and creates vulnerabilities that are explicitly recognised by UK adversaries. Closer integration comes with increased risk, and much greater potential consequences of disruption. Systems thinking is prominent within the approaches of both Russia and China, highlighting that both countries recognise the vulnerabilities of their adversaries' (i.e. the United States, UK and NATO) increasingly integrated, and therefore increasingly interdependent, C2 systems.[112] As China's 'systems confrontation' theory highlights, failure at a critical node within a cohesive system of systems would have a catastrophic and cascading impact on the UK's information and communications; the closer integration of systems between and across domains would magnify this effect. At the same time, China and Russia have their own vulnerabilities that the UK can also identify and exploit.[113] China recognises these vulnerabilities and is building independence, autonomy and resilience into its own force structures to mitigate them. Iran similarly seeks to enhance the resilience of its own 'system' to US attacks on its C2 by promoting passive and mosaic defence concepts.[114] To counter the deliberate advances in MDI by its adversaries, the UK could develop multi-domain counter-tactics; for example, by finding the interdependencies an adversary is leveraging in a multi-domain fight and using the convergence of military capabilities across the operating domains to exploit the vulnerabilities within that interdependency. At the same time, the UK could also consider how it can realise the benefits of MDI while minimising the vulnerabilities of integration and building resilience into its own force structures, systems and tactics.

Multi-domain activities can sometimes impede, rather than enhance, strategic objectives. An important consideration for the UK's MDI concept is the possible (and uncertain) implications for deterrence, crisis instability and escalation.[88] For example, cyberspace and the nuclear arena have notably opposite informational characteristics. Offensive cyber operations depend on stealth and deception to disable control systems, which has the potential to enhance the effectiveness of nuclear counterforce or damage limitation strategies. Yet this also can undermine the stability of nuclear deterrence, which depends on credible mutual information about the balance of power. Efforts to win the counterforce contest in the cyber domain thus make it more likely that deterrence will fail in the nuclear arena.[115] Embracing MDI should also come with careful consideration of how the adversary might interpret and respond to different signals, as well as how the UK can best choose between different courses of action to achieve an overall deterrence posture across domains.

Future realisation of multi-domain integration will look different depending on the adversary and operating environment in question.[116] Despite some common themes and similarities, the UK's potential adversaries differ in their understanding and practical implementation of MDI (for example, in terms of their capabilities or force structure). There are also important geographical differences to consider, at least for future conflicts occurring close to an adversary's homeland (given their limited capacity to project and sustain forces further afield).[117] For example, a confrontation close to Russia might be more land-focused, whereas a conflict in China's immediate neighbourhood would likely be centred in the air and maritime

[112] Zadalis (2018).

[113] Internal interview with RAND expert, 29 May 2020.

[114] McInnis (2017).

[115] Lindsay & Gartzke (2020).

[116] Internal interview with RAND expert, 1 June 2020.

[117] Connable et al. (2020).

domains.[118] Iran and North Korea would each bring their own challenges. There is therefore no 'one-size-fits-all' approach to MDI; effective MDI concepts should be inherently flexible and provide commanders with the array of capabilities that can be drawn upon across the domains to meet specific operational requirements. There is a difficult trade-off to be made between generating a universally applicable concept – of seeking to develop a concept of MDI that is all things in all places and at all times, but less coherent as a result – or a series of more narrowly defined concepts, tailored to specific operational scenarios (in the mould of how AirLand Battle was designed around Cold War scenarios for war in Central Europe), which may be less flexible to address any unexpected contingencies that arise.

To translate broad multi-domain concepts into meaningful principles that can be operationalised, high specificity is required to define the problem and the solution. Rather than simply generalising strategic effects, to achieve effective MDI in practice, the UK will need to articulate the problems at the tactical and operational levels to a high degree of specificity. This need for specificity has been recognised in the United States, and helps distinguish MDO or JADO from the previous MDB concept.[119] Similarly, it is important to focus not just on acquiring new high-end capabilities, but on operating concepts; namely, thinking about how to use and combine capabilities across the domains in innovative ways to solve the operational problem. This is a challenge that the United States faces – and something that Russia is clearly doing (as evidenced by its operations in Ukraine).

Effective multi-domain integration at the operational level will require new training and new ways of thinking. A vital enabler of MDI will be the education and development of UK defence personnel.[120] Future education and training could focus on making multi-domain thinking the 'standard', going beyond the current emphasis on jointness, so that UK forces are intellectually and culturally prepared to counter the multi-domain tactics of adversaries.[121] Drawing from examples of Russian Battalion Tactical Group (BTG) commanders in Ukraine, emphasis is placed on creativity and empowering commanders to draw upon multi-domain capabilities in innovative ways that are tailored to the operational requirements. Iran similarly seeks to encourage a creative and flexible approach in highly changeable circumstances as part of a mosaic defence.[122] The adversary's use of creativity in a multi-domain environment also serves to conceal their intended action until it is employed, at which point it becomes one of a series of dilemmas; the UK will need to consider how to manage the cognitive burden that this complexity (and attitude to uncertainty and tactical risk) places on commanders and planners.

Force restructuring and wider military reforms are important for putting MDI concepts into practice, and must be seen to be credible by both internal and external audiences. This may require trade-offs and divestments to remove redundancies and create a more streamlined and integrated force. Contemporary force structures may not be best suited to future multi-domain integration. The ambitious military reforms undertaken by Russia and China provide an example of MDI or analogous ideas in practice; both countries have sought to shift away from traditionally siloed force structures towards a modern force with greater

[118] Internal interview with RAND expert, 2 June 2020.

[119] Internal interview with RAND expert, 2 June 2020.

[120] Knighton (2019).

[121] Zadalis (2018).

[122] McInnis (2017).

interoperability and access to capabilities between Services. Though it has fewer resources, North Korea is reported to spend up to 10–20 per cent of its military budget on cyber warfare and has invested heavily in information warfare capabilities more broadly. Such military reforms require trade-offs, such as the divestment of certain capabilities or, in the case of China, reductions in personnel numbers to offset modernisation costs. When considering the trade-offs that may be required to implement MDI, the UK must consider what level of cost and risk it is willing to accept, as well as what 'sacred cows' may need to be slain in order to make MDI a reality – not to mention a credible deterrent in the eyes of adversaries.

References

Adamsky, Dmitry. 2015. 'Cross-Domain Coercion: The Current Russian Art of Strategy'. Proliferation Papers 54, Institut Français des Relations Internationales (Ifri). As of 9 November 2021: https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

———. 2019. 'Russian Lessons Learned from the Operation in Syria'. In G.E. Howard & M. Czekaj (eds), *Russia's Military Strategy and Doctrine*, Washington DC: The Jamestown Foundation.

Air Power Development Centre. 2018. 'Multi-Domain Integration'. *Pathfinder: Air Power Development Centre Bulletin*, 322. November. As of 9 November 2021: https://nla.gov.au/nla.obj-2262659101/view

Ajili, Hadi and Mahsa Rouhi. 2019. 'Iran's Military Strategy'. *Survival*, 61:6, 139–152. As of 9 November 2021: https://doi.org/10.1080/00396338.2019.1688575

Ashby, Mark, Caolionn O'Connell, Edward Geist, Jair Aguirre, Christian Curriden and Jon Fujiwara. 2021. *Defense Acquisition in Russia and China*. Santa Monica, Calif.: RAND Corporation. RR-A113-1. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RRA113-1.html

Barabanov, Mikhail, Konstantin Makienko and Ruslan Pukhov. 2012. 'Military Reform: Toward the New Look of the Russian Army'. Moscow: Valdai Discussion Club. July. As of 9 November 2021: https://valdaiclub.com/a/reports/military_reform_toward_the_new_look_of_the_russian_army/

Bartles, Charles K. 2016. 'Getting Gerasimov Right'. *Military Review*. January–February. As of 9 November 2021: https://community.apan.org/cfs-file/__key/docpreview-s/00-00-00-11-18/20151229-Bartles-_2D00_-Getting-Gerasimov-Right.pdf

Beauchamp-Mustafaga, Nathan. 2019. 'Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations'. *China Brief*, 19:16. 6 September. As of 9 November 2021: https://jamestown.org/program/cognitive-domain-operations-the-plas-new-holistic-concept-for-influence-operations/

Bender, Bryan. 2016. 'The Secret US Army Study That Targets Moscow'. *POLITICO*. 14 April. As of 9 November 2021: https://www.politico.com/magazine/story/2016/04/moscow-pentagon-us-secret-study-213811

Blagden, David. 2020. 'Deterring Cyber Coercion: The Exaggerated Problem of Attribution'. *Survival*, 62:1, 131–148. As of 9 November 2021: https://doi.org/10.1080/00396338.2020.1715072

Bodner, Matthew. 2018. 'As Trump Pushes for Separate Space Force, Russia Moves Fast the Other Way'. *Defense News*. 21 June. As of 9 November 2021:

https://www.defensenews.com/global/europe/2018/06/21/as-trump-pushes-for-separate-space-force-russia-moves-fast-the-other-way/

Bonds, Timothy M., Joel B. Predd, Timothy R. Heath, Michael S. Chase, Michael Johnson, Michael J. Lostumbo, James Bonomo, Muharrem Mane and Paul S. Steinberg. 2017. *What Role Can Land-Based, Multi-Domain Anti-Access/Area Denial Forces Play in Deterring or Defeating Aggression?* Santa Monica, Calif.: RAND Corporation. RR-1280-A. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR1820.html

Boston, Scott and Dara Massicot. 2017. *The Russian Way of Warfare – A Primer*. Santa Monica, Calif.: RAND Corporation. PE-231-A. As of 9 November 2021: https://www.rand.org/pubs/perspectives/PE231.html

Boyd, Dallas, Jeffrey G. Lewis and Joshua H. Pollack. 2010. 'Advanced Technology Acquisition Strategies of the People's Republic of China'. Defense Threat Reduction Agency. As of 9 November 2021: https://fas.org/irp/agency/dod/dtra/strategies.pdf

Burke, Edmund J., Kristen Gunness, Cortez A. Cooper III and Mark Cozad. 2020. *People's Liberation Army Operational Concepts*. Santa Monica, Calif.: RAND Corporation. RR-1394-1. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RRA394-1.html

Cabinet Office. 2021. 'Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy'. 16 March. As of 1 October 2021: https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

Carter, Nicholas. 2019. 'New UK Strategic Command to Drive Integration for Multi-Domain Effect'. *SC Magazine UK*. 5 December. As of 9 November 2021: https://www.scmagazineuk.com/new-uk-strategic-command-drive-integration-multi-domain-effect/article/1667949

Charap, Samuel, Dar Massicot, Miranda Priebe, Alyssa Demus, Clint Reach, Mark Stalczynski, Eugeniu Han and Lynn E. Davis. 2021. *Russian Grand Strategy: Rhetoric and Reality*. Santa Monica, Calif.: RAND Corporation. RR-4238-A. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR4238.html

Chekov, Alexander D., Anna V. Makarycheva, Anastasia M. Solomentseva, Maxim A. Suchkov and Andrey A. Sushentsov. 2019. 'War of the Future: A View from Russia'. *Survival*, 61:6, 25–48. As of 9 November 2021: https://doi.org/10.1080/00396338.2019.1688563

Clare, Phil. 2020. 'The Answer is Multi Domain Operations – Now What's the Question?'. *Wavell Room*. 13 February. As of 9 November 2021: https://wavellroom.com/2020/02/13/the-answer-is-multi-domain-operations-now-whats-the-question/

Cleary, Mark. 2020. 'Taking the High Ground: the 6555th's role in Space through 1970'. FAS. As of 22 June 2020: https://fas.org/spp/military/program/6555th/6555c4-1.htm

Congressional Research Service. 2021. 'Joint All-Domain Command and Control (JADC2)'. As of 9 November 2021: https://sgp.fas.org/crs/natsec/IF11493.pdf

Connable, Ben, Abby Doll, Alyssa Demus, Dara Massicot, Clint Reach, Anthony Atler, William Mackenzie, Matthew Povlock and Lauren Skrabala. 2020. *Russia's Limit of Advance: Analysis of Russian Ground Force Deployment Capabilities and Limitations*. Santa Monica, Calif.: RAND Corporation. RR-2563-A. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR2563.html

Connolly, Richard and Mathieu Boulègue. 2018. 'Russia's New State Armament Programme: Implications for the Russian Armed Forces and Military Capabilities to 2027'. London: The Royal Institute of International Affairs (Chatham House). As of 9 November 2021: https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf

Cordesman, Anthony H., Ashley Hess and Nicholas S. Yarosh. 2013. *Chinese Military Modernization and Force Development: A Western Perspective*. Washington DC: Center for Strategic and International Studies (CSIS). As of 9 November 2021: https://books.google.co.uk/books?id=ZYDyAwAAQBAJ&dq=china+central+military+commission+integration+acquisition&source=gbs_navlinks_s

Costello, John and Joe McReynolds. 2018. *China's Strategic Support Force: A Force for a New Era*. China Strategic Perspectives 13. Institute for National Strategic Studies (INSS), National Defense University. As of 9 November 2021: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf

Cozad, Mark R. 2016. *PLA Joint Training and Implications for Future Expeditionary Capabilities*. Santa Monica, Calif.: RAND Corporation, CT-451. As of 9 November 2021: https://www.rand.org/pubs/testimonies/CT451.html

Curtis, Andrew. 2020. 'The UK's Integrated Review: A Return to the Phoney War'. *RUSI Commentary*. May 7. As of 9 November 2021: https://rusi.org/commentary/uks-integrated-review-return-phoney-war

Czulda, Robert. 2016. 'The Defensive Dimension of Iran's Military Doctrine: How Would They Fight?'. *Middle East Policy Council Journal*, XXIII, Spring, 1. As of 9 November 2021: https://onlinelibrary.wiley.com/doi/full/10.1111/MEPO.12176

Defense Intelligence Agency (DIA). 2019a. 'China Military Power: Modernizing a Force to Fight and Win'. DIA-02-1706-065. As of 9 November 2021: https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/China_Military_Power_FINAL_5MB_20190103.pdf

———. 2019b. 'Iran Military Power: Ensuring Regime Survival and Securing Regional Dominance'. DIA-Q-00055-A. As of 9 November 2021: https://www.hsdl.org/?abstract&did=831646

Deptula, David A. and Heather Penney. 2019. 'Mosaic Warfare'. *Air Force Magazine*. 1 November. As of 9 November 2021: https://www.airforcemag.com/article/mosaic-warfare/

Development, Concepts and Doctrine Centre (DCDC). 2010. *Joint Doctrine Publication 04: Understanding and Decision-making.* As of 9 November 2021:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf

———. 2015. *Strategic Trends Programme: Future Operating Environment 2035*. As of 9 November 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646821/20151203-FOE_35_final_v29_web.pdf

———. 2017. *Joint Concept Note 1/17: Future Force Concept*. As of 9 November 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf

Donnelly, Jared and Jon Farley. 2018. 'Defining the "Domain" in Multi-Domain'. *OTH: Multi-Domain Operations and Strategy*. 17 September. As of 9 November 2021: https://othjournal.com/2018/09/17/defining-the-domain-in-multi-domain/

Engstrom, Jeffrey. 2018. *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*. Santa Monica, Calif.: RAND Corporation, RR-1708-OSD. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR1708.html

Erickson, Andrew. 2019. 'Full Text of 2019 Defense White Paper: "China's National Defense in the New Era" (English & Chinese Versions)'. 24 July. As of 9 November 2021, available at: http://www.andrewerickson.com/2019/07/full-text-of-defense-white-paper-chinas-national-defense-in-the-new-era-english-chinese-versions/

Fabian, Sandor. 2019. 'The Russian Hybrid Warfare Strategy – Neither Russian nor Strategy'. *Defense & Security Analysis*, 35:3, 308–325. As of 9 November 2021: https://doi.org/10.1080/14751798.2019.1640424

Finkelstein, Claire Oakes and Kevin Govern. 2015. 'Introduction: Cyber and the Changing Face of War'. Penn Law: Legal Scholarship Repository. As of 22 June 2020: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2567&context=faculty_scholarship

Freedberg, Sydney J. 2018. 'Army Multi-Domain Update: New HQs, Grey Zones & The Art of the Unfeasible'. *Breaking Defense*. 7 December. As of 9 November 2021: https://breakingdefense.com/2018/12/army-multi-domain-update-new-hqs-grey-zones-the-art-of-the-unfeasible/

Freedman, Guy. 2017. 'Iranian Approach to Deterrence: Theory and Practice'. *Comparative Strategy*, 36:5, 400–412. As of 9 November 2021: https://doi.org/10.1080/01495933.2017.1379831

Friedman, Uri. 2020. 'The Blueprint Iran Could Follow After Soleimani's Death'. *The Atlantic*. 4 January. As of 9 November 2021: https://www.theatlantic.com/politics/archive/2020/01/what-iranian-way-war-looks-like/604438/

Galeotti, Mark. 2016. 'Hybrid, Ambiguous and Non-Linear? How New is Russia's "New Way of War"?'. *Small Wars & Insurgencies*, 27:2, 282–301. As of 9 November 2021: https://doi.org/10.1080/09592318.2015.1129170

Gibson, Richard W. 2019. 'Multi-Domain Operations and Counter-Space'. NATO Joint Air Power Competence Centre, courtesy of *Small Wars Journal*. As of 9 November 2021: https://www.japcc.org/multi-domain-operations-and-counter-space/

Giles, Keir. 2019. *Moscow Rules*. Chatham House Insights Series.

Glanz, James and Thomas Nilsen. 2020. 'A Deep-Diving Sub. A Deadly Fire. And Russia's Secret Undersea Agenda'. *The New York Times*. 21 April. As of 9 November 2021: https://www.nytimes.com/2020/04/20/world/europe/russian-submarine-fire-losharik.html

Goldstein, Lyle J. 2021. 'The One Flaw in China's Military Rise: No Combat Experience'. *The National Interest*. As of 9 November 2021: https://nationalinterest.org/blog/reboot/one-flaw-chinas-military-rise-no-combat-experience-181909

Gouré, Dan. 2019. 'A New Joint Doctrine for an Era of Multi-Domain Operations'. *RealClear Defense*. 24 May. As of 9 November 2021: https://www.realcleardefense.com/articles/2019/05/24/a_new_joint_doctrine_for_an_era_of_multi-domain_operations_114450.html

Griesemer, Thomas S. 2018. 'Russian Military Reorganization: A Step Towards Multi-Domain Operations'. *OTH: Multi-Domain Operations & Strategy*. 19 November. As of 9 November 2021: https://othjournal.com/2018/11/19/russian-military-reorganization-a-step-toward-multi-domain-operations/

Grossman, Derek. 2019. *Envisioning a 'World-Class' PLA: Implications for the United States and the Indo-Pacific*. Santa Monica, Calif.: RAND Corporation, CT-514. As of 9 November 2021: https://www.rand.org/pubs/testimonies/CT514.html

Hackett, James and Mark Fitzpatrick (eds). 2018. 'The Conventional Military Balance on the Korean Peninsula'. International Institute for Strategic Studies (IISS). As of 9 November 2021: https://www.iiss.org/blogs/research-paper/2018/06/military-balance-korean-peninsula

Hadi, Sayed Ali. 2020. 'Cross-Domain Deterrence – A Critical Appraisal'. Centre for Strategic and Contemporary Research. 6 March. As of 9 November 2021: https://cscr.pk/explore/themes/defense-security/cross-domain-deterrence-a-critical-appraisal/

Heath, Timothy R. and Andrew S. Erickson. 2017. 'Is China Pursuing Counter-Intervention?', *The Washington Quarterly*, 38:3, 143–156. As of 9 November 2021: https://www.rand.org/pubs/external_publications/EP67350.html

Heath, Timothy R., Kristen Gunness and Cortez A. Cooper. 2016. *The PLA and China's Rejuvenation: National Security and Military Strategies, Deterrence Concepts and Combat Capabilities*. Santa Monica, Calif.: RAND Corporation. RR-1402-OSD. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR1402.html

Hoffman, Frank. 2007. *Conflict in the 21st Century: The Rise of Hybrid War*. Arlington, VA: Potomac Institute for Policy Studies.

Hoffman, Frank and Michael C. Davies. 2013. 'Joint Force 2020 and The Human Domain: Time for A New Conceptual Framework?'. *Small Wars Journal*. As of 9 November 2021:

https://smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework

Howard, Glen E. and Matthew Czekaj (eds). 2019. *Russia's Military Strategy and Doctrine*. Washington DC: The Jamestown Foundation. As of 9 November 2021: https://jamestown.org/product/russias-military-strategy-and-doctrine/

Huang, Cary. 2019. 'If China thinks it's overtaking the US any time soon, here's a wake-up call'. *South China Morning Post*. As of 29 June 2020: https://www.scmp.com/week-asia/opinion/article/3006892/if-china-thinks-its-overtaking-us-any-time-soon-heres-wake-call

IHS Jane's. 2020a. 'China – Defence Budget Overview'. *Jane's Sentinel Security Assessment – China and Northeast Asia*. 22 January. As of 9 November 2021 [subscription required]: https://janes.ihs.com/Janes/Display/chins090-cna

———. 2020b. 'China – Armed Forces'. *Jane's Sentinel Security Assessment – China and Northeast Asia.* 22 January. As of 6 2020 June [subscription required]: https://janes.ihs.com/Janes/Display/CHINS100-CNA

Ilhan, Bekir. 2020. 'China's Evolving Military Doctrine After the Cold War'. Foundation for Political, Economic and Social Research (SETA). January. As of 9 November 2021: https://setav.org/en/assets/uploads/2020/02/A56En.pdf

Johnson, Dave. 2018. *Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle*. Santa Monica, Calif.: RAND Corporation. PE-301-A/AF. As of 9 November 2021: https://www.rand.org/pubs/perspectives/PE301.html

———. 2019. 'Review of Speech by General Gerasimov at the Russian Academy of Military Science'. *Russian Studies Series 4/19*, NATO Defence College. As of 9 November 2021: http://www.ndc.nato.int/research/research.php?icode=585

Johnson, James S. 2018. 'China's Vision of the Future Network-Centric Battlefield: Cyber, Space and Electromagnetic Asymmetric Challenges to the United States'. *Comparative Strategy*, 37:5, 373–390. As of 9 November 2021: https://doi.org/10.1080/01495933.2018.1526563

Kania, Elsa and John Costello. 2017. 'China's Quest for Informatization Drives PLA Reforms', *The Diplomat*. 4 March. As of 9 November 2021: https://thediplomat.com/2017/03/chinas-quest-for-informatization-drives-pla-reforms/

———. 2018. 'The Strategic Support Force and the Future of Chinese Information Operations'. *The Cyber Defense Review*. Spring. As of 9 November 2021: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/The%20Strategic%20Support%20Force_Kania_Costello.pdf

Kania, Elsa and Lorand Laskai. 2021. 'Myths and Realities of China's Military-Civil Fusion Strategy'. The Center for a New American Security. As of 9 November 2021: https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy

Kilcullen, David. 2020. *The Dragons and the Snakes: How the Rest Learned to Fight the West*. Glasgow, UK: Bell & Bain Ltd.

Kim Min-Seok. 2020. 'The State of the North Korean Military'. Carnegie Endowment for International Peace. 18 March. As of 9 November 2021: https://carnegieendowment.org/2020/03/18/state-of-north-korean-military-pub-81232

King, Scott and Dennis B. Boykin. 2019. 'Distinctly Different Doctrine: Why Multi-Domain Operations Isn't AirLand Battle 2.0'. Association of the United States Army (AUSA). 20 February. As of 9 November 2021: https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isn%E2%80%99t-airland-battle-20

Knighton, Richard. 2019. 'Lord Trenchard Memorial Lecture 2019'. Royal United Services Institute (RUSI). 18 November. As of 9 November 2021: https://www.youtube.com/watch?v=VH-HmmayaIw

Kofman, Michael. 2019. 'It's Time to Talk About A2/AD: Rethinking the Russian Military Challenge'. *War on the Rocks*. 5 September. As of 9 November 2021: https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/

Kucharski, Lesley. 2018. 'Russian Multi-Domain Strategy against NATO: Information Confrontation and US Forward-Deployed Nuclear Weapons in Europe'. Lawrence Livermore National Laboratory (LLNL). As of 9 November 2021: https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf

Lacey, James. 2020. 'Battle of the Bastions'. *War on the Rocks*. 9 January. As of 9 November 2021: https://warontherocks.com/2020/01/battle-of-the-bastions/

Lindsay, Jon R. and Erik Gartzke (eds). 2019. *Cross-Domain Deterrence*. Oxford: Oxford University Press.

———. 2020. 'Politics By Many Other Means: The Comparative Strategic Advantages of Operational Domains'. *Journal of Strategic Studies*. As of 9 November 2021: https://doi.org/10.1080/01402390.2020.1768372

Majumdar, Dave. 2014. 'US Navy Impressed with New Russian Attack Boat'. *USNI News*. 28 October. As of 9 November 2021: https://news.usni.org/2014/10/28/u-s-navy-impressed-new-russian-attack-boat

Mallory, King. 2018. *New Challenges in Cross-Domain Deterrence*. Santa Monica, Calif.: RAND Corporation. PE-259-OSD. As of 9 November 2021: https://www.rand.org/pubs/perspectives/PE259.html

Massicot, Dara. 2019. 'Anticipating a New Russian Military Doctrine in 2020: What It Might Contain and Why It Matters'. *War on the Rocks*. 9 September. As of 9 November 2021: https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/

McCauley, Kevin. 2019. '"Triad" Military Education and Training Reforms: The PLA's Cultivation of Talent for Integrated Joint Operations'. *The Jamestown Foundation*. As of 9 November 2021:

https://jamestown.org/program/triad-military-education-and-training-reforms-the-plas-cultivation-of-talent-for-integrated-joint-operations/

McDermott, Roger. 2019a. 'Deciphering the Lessons Learned by the Russian Armed Forces in Ukraine, 2014–2017'. In G.E. Howard & M. Czekaj (eds), *Russia's Military Strategy and Doctrine*, Washington DC: The Jamestown Foundation.

———. 2019b. 'Russian Military Introduces New Automated Command-and-Control Systems'. *Eurasia Daily Monitor*, 16:86. 11 June. As of 9 November 2021: https://jamestown.org/program/russian-military-introduces-new-automated-command-and-control-systems/

McInnis, J. Matthew. 2017. 'Iranian Concepts of Warfare: Understanding Teheran's Evolving Military Doctrines'. American Enterprise Institute. February. As of 9 November 2021: https://www.aei.org/research-products/report/iranian-concepts-of-warfare-understanding-tehrans-evolving-military-doctrines/

NATO Command and Control Centre of Excellence (C2COE). 2021. 'Multi-Domain Command and Control: Providing a Working Description of the Term Multi-Domain C2 (MDC2)'. As of 9 November 2021: https://c2coe.org/wp-content/uploads/Library%20Documents/Study/20210430%20MDC2%20Long%201.0.pdf

Office of the Secretary of Defense. 2019. 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019'. May. As of 9 November 2021: https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf

Palazzo, Albert and David P. McLain III. 2016. 'Multi-Domain Battle A New Concept for Land Forces'. *War on the Rocks*. 15 September. As of 9 November 2021: https://warontherocks.com/2016/09/multi-domain-battle-a-new-concept-for-land-forces/

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven S. Davenport, Isaac R. Porsche III and Joel Harding. 2018. *Lessons from Others for Future US Army Operations in and through the Information Environment: Case Studies.* Santa Monica, Calif.: RAND Corporation. RR-1925/2-A. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR1925z2.html

Pollpeter, Kevin L., Michael S. Chase and Eric Heginbotham. 2017. *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations*. Santa Monica, Calif.: RAND Corporation. RR-2058-AF. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR2058.html

Qiao Liang and Wang Xiangsui. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House.

Qiu, Mingda. 2015. 'China's Science of Military Strategy: Cross-Domain Concepts in the 2013 Edition'. CDD Working Paper. La Jolla, Calif.: UC San Diego. September. As of 9 November 2021: http://deterrence.ucsd.edu/_files/Chinas%20Science%20of%20Military%20Strategy%20Cross-Domain%20Concepts%20in%20the%202013%20Edition%20Qiu2015.pdf

Radin, Andrew, Lynn E. Davis, Edward Geist, Eugeniu Han, Dara Massicot, Matthew Povlock, Clint Reach, Scott Boston, Samuel Charap, William Mackenzie, Katya Migacheva, Trevor Johnston and Austin Long. 2019. *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for US-Russia Competition*. Santa Monica, Calif.: RAND Corporation. RR-3099-A. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR3099.html

Russian Federation. 2014. *The Military Doctrine of the Russian Federation* [Translation from Russian]. 25 December. As of 9 November 2021: https://www.rusemb.org.uk/press/2029

Scobell, Andrew, David Lai and Roy Kamphausen (eds). 2011. *Chinese Lessons from Other People's Wars*. Carlisle, PA: Strategic Studies Institute, U.S. Army War College.

Scouras, James, Edward Smyth and Thomas Mahnken. 2017. *Cross-Domain Deterrence in US–China Strategy: Workshop Proceedings*. The John Hopkins University Applied Physics Laboratory. As of 9 November 2021: https://www.jhuapl.edu/Content/documents/CrossDomainWeb.pdf

Shlapak, David A. and Michael Johnson. 2016. *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics*. Santa Monica, Calif.: RAND Corporation. RR-1253-A. As of 9 November 2021: https://www.rand.org/pubs/research_reports/RR1253.html

Shou Xiaosong. 2013. *The Science of Military Strategy*. Beijing: Military Science Press.

Smith, Grant J. 2019. 'Multi-Domain Operations: Everyone's Doing It, Just Not Together'. *OTH: Multi-Domain Operations & Strategy*. 24 June. As of 9 November 2021: https://othjournal.com/2019/06/24/multi-domain-operations-everyones-doing-it-just-not-together/

Spears, Will. 2019. 'A Sailor's Take on Multi-Domain Operations'. *War on the Rocks*. 21 May. As of 9 November 2021: https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/

Spirtas, Michael. 2018. 'Towards One Understanding of Multiple Domains'. *The RAND Blog*. 2 May. As of 9 November 2021: https://www.rand.org/blog/2018/05/toward-one-understanding-of-multiple-domains.html

Sprang, Ronald. 2018. 'Russia in Ukraine 2013–2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO and Media'. *Small Wars Journal*. As of 9 November 2021: https://smallwarsjournal.com/jrnl/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and

Sukman, Dan and Charles Davis. 2020. 'Divided We Fall: How the US Force is Losing Its Joint Advantage over China and Russia'. *Military Review*. March–April. As of 9 November 2021: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2020/Sukman-Divided/

Tabatai, Ariane M. 2019. 'Syria Changed the Iranian Way of War'. *The RAND Blog* and *Foreign Affairs*. 16 August. As of 9 November 2021: https://www.rand.org/blog/2019/08/syria-changed-the-iranian-way-of-war.html

Tasic, Mirko. 2019. 'Exploring North Korea's Asymmetric Military Strategy'. *Naval War College Review*, 72:4 (Autumn), 53–72. As of 9 November 2021: https://www.jstor.org/stable/10.2307/26775519

Taylor, Curt and Larry Kay. 2019. 'Putting the Enemy Between a Rock and a Hard Place: Multi-Domain Operations in Practice'. Modern Warfare Institute. 27 August. As of 9 November 2021: https://mwi.usma.edu/putting-enemy-rock-hard-place-multi-domain-operations-practice/

The State Council Information Office of the People's Republic of China. 2015. 'China's Military Strategy'. As of 9 November 2021: http://www.scio.gov.cn/zfbps/ndhf/2015/Document/1435159/1435159.htm

Thomas, Timothy. 2015. *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*. Fort Leavenworth, Kansas: Foreign Military Studies Office.

———. 2016. 'The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation and New-Type Thinking'. *The Journal of Slavic Military Studies*, 29:4, 554–575. As of 9 November 2021: https://doi.org/10.1080/13518046.2016.1232541

———. 2019. 'Russian Military Thought: Concepts and Elements'. MITRE Corporation. August. As of 9 November 2021: https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf

Udesen, Kristian. 2018. 'The Multi-Domain Battle: Implications for the Canadian Army'. Canadian Forces College. As of 9 November 2021: https://www.cfc.forces.gc.ca/259/290/405/286/udesen.pdf

UK Ministry of Defence (MOD). 2019a. 'Joint Doctrine Publication 0-01.1: UK Terminology Supplement to NATOTerm'. Edition A. As of 9 November 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773707/20190121-doctrine_uk_terminology_JDP_0_01_1_2019_1_.pdf

———. 2019b. 'Allied Joint Doctrine for the Planning of Operations (UK Joint Doctrine) Allied Joint Publication-5'. May. As of 9 November 2021: https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations

———. 2020a. 'Integrated Operating Concept'. As of 9 November 2021: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025

———. 2020b. 'Multi-Domain Integration (JCN 1/20)'. As of 9 November 2021: https://www.gov.uk/government/publications/multi-domain-integration-jcn-120

———. 2021a. 'Defence Experimentation for Force Development Handbook'. As of 9 November 2021: https://www.gov.uk/government/publications/defence-experimentation-for-force-development-handbook

———. 2021b. 'Defence in a Competitive Age'. 22 March. As of 1 October 2021: https://www.gov.uk/government/publications/defence-in-a-competitive-age

US Air Force (USAF). 2020. 'Air Force Doctrine Note 1-20: USAF Role in Joint All-Domain Operations'. As of 9 November 2021:

https://www.doctrine.af.mil/Portals/61/documents/Notes/Joint%20All-Domain%20Operations%20Doctrine--CSAF%20signed.pdf

US Army Training and Doctrine Command (TRADOC). 2015. 'Threat Tactics Report: North Korea'. October. Version 1.1. As of 9 November 2021: https://publicintelligence.net/usarmy-north-korea-tactics/

———. 2018. 'The US Army in Multi-Domain Operations 2028'. 6 December. As of 9 November 2021: https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf

US Department of Defense (DOD). 2012a. 'Capstone Concept for Joint Operations: Joint Force 2020'. As of 9 November 2021: http://www.ndu.edu/Portals/59/Documents/Incoming/ccjo_2012.pdf

———. 2012b. 'Joint Operational Access Concept (JOAC)'. 17 January. As of 9 November 2021: https://dod.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf

US Joint Staff. 2018. 'Memorandum for: Military Education Coordination Council Principals + Capstone Director'. 27 August. As of 9 November 2021: https://publicintelligence.net/jcs-china-system-attack/

Watling, Jack and Daniel Roper. 2019. 'European Allies in US Multi-Domain Operations. Occasional Paper'. Royal United Services Institute (RUSI). October. As of 9 November 2021: https://rusi.org/explore-our-research/publications/occasional-papers/european-allies-us-multi-domain-operations

Wehrey, Frederic, David E. Thaler, Nora Bensahel, Kim Cragin, Jerrold D. Green, Dalia Dassa Kaye, Nadia Oweidat and Jennifer Li. 2009. *Dangerous But Not Omnipotent: Exploring the Reach and Limitations of Iranian Power in the Middle East*. Santa Monica, Calif.: RAND Corporation. MG-781-AF. As of 9 November 2021: https://www.rand.org/pubs/monographs/MG781.html

Westerland, Fredrik and Susanne Oxenstierna (eds). 2019. *Russian Military Capability in a Ten-Year Perspective – 2019*. Swedish Defence Research Agency (FOI). As of 9 November 2021: https://www.researchgate.net/publication/337948965_Russian_Military_Capability_in_a_Ten-Year_Perspective_-_2019

Whisler, Greg. 2020. 'Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts and Service Main Commands (Part Two)'. *The Journal of Slavic Military Studies*, 33:1, 89–112. As of 9 November 2021: https://doi.org/10.1080/13518046.2020.1723227

Wuthnow, Joel and Phillip C. Saunders. 2017. 'Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges and Implications'. China Strategic Perspectives 10. Institute for National Strategic Studies (INSS), National Defense University. As of 9 November 2021: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-10.pdf

Wuthnow, Joel. 2019. 'China's "New" Academy of Military Science: A Revolution in Theoretical Affairs?'. *The Jamestown Foundation*. As of 9 November 2021: https://jamestown.org/program/chinas-new-academy-of-military-science-a-revolution-in-theoretical-affairs/

Yossef, Amr. 2019. 'Upgrading Iran's Military Doctrine: An Offensive "Forward Defense"'. Middle East Institute (MEI). 10 December. As of 9 November 2021: https://www.mei.edu/publications/upgrading-irans-military-doctrine-offensive-forward-defense

Zadalis, Tim. 2018. 'Multi-Domain Command and Control: Maintaining our Asymmetric Advantage'. NATO Joint Air Power Competence Centre (JAPCC). As of 9 November 2021: https://www.japcc.org/multi-domain-command-and-control/

Zhang, Ying and Chris Marquis. 2015. 'Achieving China's Next stage of "Catching Up"'. As of 9 November 2021: https://ecommons.cornell.edu/bitstream/handle/1813/40207/Achieving_Chinas_next_stage_of_Final.pdf;sequence=4

Annex A. Case study: Russian Federation

A.1. Summary of Russia's approach

A.1.1. Russia is refining its own variants of MDI concepts and putting theory into practice through military reforms, capability development and operations

Russia's doctrine, recent military reforms and operations indicate that Russia is leveraging multi-domain concepts to pursue asymmetric 'new-type' and systems warfare through tactics such as 'reflexive control' and disorganisation. This strategy focuses on the use of information to control adversary behaviour and shape the strategic environment in Russia's favour, as well as exploiting an adversary's weaknesses to achieve maximum effect with minimal expenditure of Russia's own constrained resources. The importance of creative thought is also emphasised, as well as the ability to achieve information advantage in the initial period of conflict; the information environment (information-technological and information-psychological) appears to be viewed as underpinning and integrating all other operational domains (land, air, sea, space, cyber and electromagnetic environment), and is therefore critical for achieving asymmetric advantage and Russian success at the tactical, operational and strategic levels.

A.1.2. Russia adopts a broad understanding of warfare, looking beyond the military domain to pursue asymmetric strategies outside of the conventional battlefield

It is also important to recognise that Russia's approach to MDI – in the narrower sense of conventional military combat operations – sits within a broader overarching understanding of global strategic competition and of the changing nature of warfare.[123] This includes but is not limited to:

- The perception that the international order is transitioning from a US-led unipolar system to a polycentric world, where other regional leaders like Russia and China have a greater role to play in balancing and stabilising the international order.
- A desire to establish and lead the post-Soviet Eurasian region in this new international order.
- A view that the West, led by the United States, supports and engages in certain aggressive behaviours to foster unrest and destabilise the Russian regime.
- An understanding that internal and external threats are becoming increasingly integrated.

[123] Kilcullen (2020).

- A firm belief in the need for Russia to maintain a strong and flexible military to defend its national interests against numerous and increasingly integrated threats, at home and abroad.[124]

In Western studies of Russian military thought, Russia's approach is variously described through terms such as 'hybrid', 'non-linear', 'no-contact', 'next-generation' or 'liminal' warfare, or as 'the Gerasimov doctrine' – a reference to a famous set of writings published by Russia's Chief of General Staff of the Armed Forces, Army General Valeriy Gerasimov, in 2013.[125] Gerasimov noted the increasing significance of asymmetric and indirect operations for modern military success. He stressed the necessity of creating a 'holistic theory of asymmetric operations', and that Russia's approach to future competition and warfighting must include asymmetric and indirect actions. This includes non-military methods such as political pressure, economic sanctions, blockades of maritime, air, and land LOCs, and the use of international peacekeeping contingents under the pretext of human rights and humanitarian operations.[126]

It is important to note that the Western portrayal of General Gerasimov's various writings and remarks is often not recognised by Russians themselves.[127] There is a live debate as to the extent to which General Gerasimov is leading, as opposed to being led by, conceptual development within the Russian Armed Forces; similarly, many argue that his conceptualisation of modern operations above and below the threshold of armed conflict (the famed 'hybrid warfare') is less a roadmap for Russia to follow and more a description of how Russia perceives the West to be operating against it.[128]

These caveats aside, in preparing Russia for future complex war, Gerasimov has repeatedly emphasised that a whole-of-government approach and MDI will be critical in high-intensity conflict. In line with General Gerasimov's vision, Russia is intentionally moving towards its own interpretations of what the United States might term 'multi-domain', while also incorporating elements of a 'comprehensive approach'.[129] This concept of 'hybrid' and 'non-linear' methods represents the 'broader' aspects of Russia's strategic thinking, which entails creating its own favourable strategic conditions by employing a combination of its levers of power, both military and non-military (e.g. economic, political, diplomatic, information, etc.). At the same time, this approach places a premium on using a mix of overt, ambiguous and covert action, as well as strategic signalling, with the aim of achieving Russia's strategic objectives while controlling the escalation ladder and avoiding crossing those thresholds that might trigger an unwanted armed conflict with superior NATO forces on unfavourable terms (i.e. 'liminal warfare').[130]

[124] Charap et al. (2021).

[125] Chekov et al. (2019).

[126] Thomas (2019).

[127] Chekov et al. (2019).

[128] Thomas (2015).

[129] Griesemer (2018).

[130] Kilcullen (2020).

A.1.3. Russian approaches to MDI in both a broad (competition) and narrow (conflict) sense represent adaptations to Russia's perceived strengths and weaknesses

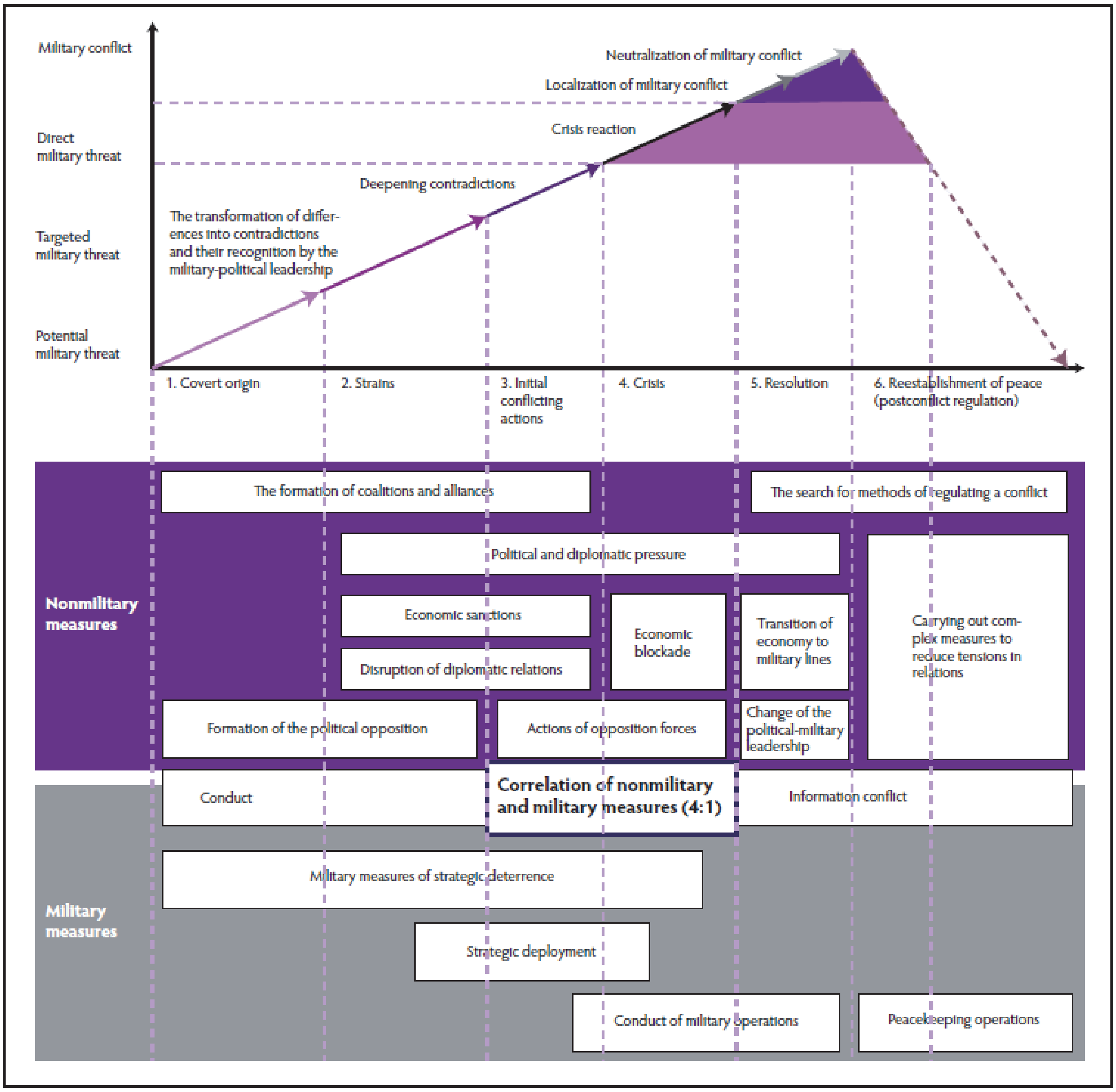
Crucially, when considering the extent to which MDI concepts map across to Russian thinking, it is important to note that while 'the West considers these non-military measures to be ways of *avoiding* war, Russia considers them *part of* war'.[131] General Gerasimov even goes so far as to estimate their relative importance, suggesting that 'war is now conducted by a roughly 4:1 ratio of non-military and military measures' (see Figure 4 below).[132] This broader understanding is grounded in longstanding Russian and Soviet-era conceptions of the nature of competition and of warfare – in particular, the haunting experience of repeated costly invasion from the West (in 1812, 1854, 1914 and 1941); the awareness of the importance of political (revolutionary) struggle; and the recognition of an imperative to promote security at home by generating a buffer around Russia, through territorial control if possible, or through interference in other countries' lands and societies if not.[133]

[131] Bartles (2016), cited in Kilcullen (2020).

[132] Bartles (2016, 34).

[133] Giles (2019), quoted in Kilcullen (2020).

Figure 4. Russian conceptualisation of the complexity of modern warfare by General Gerasimov


Military conflict
Direct military threat
Targeted military threat
Potential military threat
Neutralization of military conflict
Localization of military conflict
Crisis reaction
Deepening contradictions
The transformation of differences into contradictions and their recognition by the military-political leadership
1. Covert origin
2. Strains
3. Initial conflicting actions
4. Crisis
5. Resolution
6. Reestablishment of peace (postconflict regulation)
Nonmilitary measures
The formation of coalitions and alliances
The search for methods of regulating a conflict
Political and diplomatic pressure
Economic sanctions
Disruption of diplomatic relations
Economic blockade
Transition of economy to military lines
Carrying out complex measures to reduce tensions in relations
Formation of the political opposition
Actions of opposition forces
Change of the political-military leadership
Conduct
Correlation of nonmilitary and military measures (4:1)
Information conflict
Military measures
Military measures of strategic deterrence
Strategic deployment
Conduct of military operations
Peacekeeping operations

Source: Bartles (2016, 35).

This broader understanding also represents a necessary response to Russia's vulnerable strategic position since the chaotic and humiliating collapse of the Soviet Union in 1991 and the subsequent political, military and economic ascendancy of the United States (and NATO) in the 1990s and 2000s. The contemporary Russian military's embrace of 'hybrid', 'non-linear' or 'liminal warfare' – seeking to avoid the need for conflict by achieving Russian goals in the competition or shaping phase – can be 'best understood as a reaction to Western dominance, since the Cold War, of a narrowly defined form of symmetrical, force-on-force conflict'.[134] At the tactical level, Russian thinking emphasises the importance of models and formulae for the 'correlation of forces' in determining outcomes, and recognises the qualitative advantages that US

[134] Kilcullen (2020, 119).

and NATO forces are likely to enjoy in any direct confrontation. As such, 'at the operational and strategic levels, a much different approach is needed'.[135]

While offering an asymmetric counter to NATO's battlefield dominance in 'network-centric warfare', Russia's 'non-linear' or 'liminal' strategy of deploying covert, ambiguous and unconventional means is not without its own risks and limitations, nor is it expected to be effective forever. Both Russian and Western literature talks of a finite time period within which Moscow can secure its interests (whether the interests of the Russian state and people, or of the ruling regime) before its relative strength peaks and Russia's global competitiveness is once again eroded by both structural (e.g. demographic decline, economic stagnation) and externally imposed (e.g. financial sanctions) constraints:

> [Russia's approach] is an adaptive response to this dominance, shaped by an environment of pervasive electronic surveillance, a social media landscape that makes true clandestine or deniable covert operations increasingly hard to pull off, and tightening political and legal constraints on democratic governments, which need time and proof before they act. As such, liminal warfare is a survival mechanism for a power that lacks the capacity to compete directly with the West and faces a limited window of opportunity to carve out trade-space for its future interests while rebuilding its conventional capabilities.[136]

A.2. How does Russia think about domains and how, if at all, does it conceptualise MDI?

A.2.1. Russia's approach to thinking about domains and multi-domain integration does not map neatly against Western frameworks, though this is too often overlooked

Much as Russia's approach to strategic competition and more expansive definition of warfare is not a straightforward translation across to Western conceptual frameworks, the Russian military also adopts its own nuanced line on the notion of domains.

Certainly, the Russian Armed Forces operate and seek to develop capabilities across air, land, sea, space, cyber and the electromagnetic spectrum, while also recognising the importance of the information or human domains in both competition and conflict. The interlinkages between these domains are therefore an important subject of debate on Russia's own variations of what Western defence planners might term joint and multi-domain concepts.[137] While Russia does not have a formally articulated MDO or MDI concept, Russian thinking on related ideas can be found in its formal military doctrine. The term 'cross-domain' is also commonly found in literature discussing contemporary Russian military strategy, though often with a focus on the combination of conventional forces with unconventional (nuclear) forces in an overall deterrence posture, going beyond just the integration of air, land, sea and other dimensions.[138]

[135] Bartles (2016, 35).

[136] Bartles (2016, 119–120).

[137] Griesemer (2018).

[138] Adamsky (2015).

While these various physical and virtual domains are certainly all recognised as spaces within which the Russian Armed Forces can expect to conduct operations, that does not necessarily mean that the concept of 'domains' as understood by NATO militaries carries the same importance or currency:

> … [T]he Russian General Staff does not see the world in terms of domains; for example, Russia has integrated aerospace defence as everything from low-altitude air defence to space and anti-satellite capabilities. In the Russian military these functions combine electronic warfare, cyberwarfare, counter-space, along with air defence units and the air force. Therefore, the Russian goal would be not to deny specific domains, but rather to destroy the adversary's ability to function as a military system… The Russian General Staff sees the world in terms of theatres of operations, strategic directions, correlations, and asymmetries. What matters at the operational and strategic level is correlation of forces and means, not where the assets are physically located or which service has them… Incidentally, this is also why Russia is unlikely to be deterred in a specific domain, since deterrence exists in the mind of the adversary and not in a domain per se, especially when the adversary doesn't see the world through the US domain kaleidoscope.[139]

Instead, Russian military literature often frames discussions of the contemporary or future battlefield in terms of 'systems thinking': developing a 'theory of war that posits the adversary as a system with key sub-systems or nodes', whereby the goal for Russia is to 'look past the [adversary's] force and attain strategic effects by simultaneously targeting key military, supporting or decision-making functions'.[140] This recognises the success of the model of network-centric, precision warfare employed by the United States and its allies since the First Gulf War in 1991, as well as the need for Russia to focus not on tactical outcomes against NATO forces but rather on defeating its adversary at the operational and strategic levels by using a combination of military and non-military levers to influence the adversary's thinking in a direction aligned with Moscow's interest. Given that Russia assumes that any major conflict with the United States and NATO would be a defensive war close to Russia's borders, its strategy and operating concepts assume that the asymmetry of interests would see Russia stand firm – and therefore prevail – assuming it could break the Alliance's will to fight by exerting targeted pressure on the overall 'system' through a mix of kinetic and non-kinetic means.[141]

A.2.2. Even when thinking in the narrower sense of MDI for conventional military operations, Russia charts a course based on its ground-centric forces and setting

Even when focusing more narrowly on conventional military forces, how Russia thinks about integrating the different domains within its joint force has a character distinct from Western multi-domain concepts. This reflects both conceptual differences as well as the practicalities of Russian force structures.

Since the First Gulf War, the larger NATO militaries have focused heavily on the use of air- and to a lesser extent ship- or submarine-launched stand-off weapons to provide firepower to the joint force, offsetting a lack of mass (and enabling 'peace dividend' cuts in troops numbers) through effective intelligence,

[139] Kofman (2019).

[140] Kofman (2019).

[141] Kofman (2019).

surveillance, target acquisition and reconnaissance (ISTAR) and use of precision guided munitions (PGMs). As a result, the bulk of firepower is brought to bear when operating as a joint force, emphasising a need to develop multi-domain concepts. By contrast, the Russian Armed Forces rely heavily on tube artillery and multiple launch rocket systems (MLRS) for massed long-range fires, as well as ground-launched ballistic missile systems for deep strike.[142] This heightened emphasis on the ground force means that missions which are necessarily 'multi-domain' and joint for the United States or UK might be conducted solely by one service (and in one domain) in the Russian context.

Similarly, the unusual constellation of different services, departments and agencies that are organised under the banner of Russian defence means the Russian Armed Forces can call on non-military levers that would in a Western setting require interagency cooperation outside of the defence ministry:

> While the Russian military has the traditional armed forces with army, air force, and naval components, Moscow's military efforts can also incorporate other non-traditional militarised forces such as the Federal Security Service, the Interior Ministry, and the Ministry for Emergency Situations. This arrangement follows a different paradigm and is not well understood by many in the US military. Under this structure, the Russian military can directly leverage non-traditional forces and capabilities in circumstances that would require the US military to be subordinated under another interagency department. For example, the Ministry for Emergency Situations, a component of the Russian military, is the lead for foreign humanitarian assistance, whereby any US military involvement in the same would be under the auspices of the US Agency for International Development. This broad range of forces enables Russia's military to conduct joint military operations against adversaries across a broad spectrum of activities and well below the threshold of armed conflict.[143]

Russian theory and practice of what the United States would term MDI are also informed by geographical realities, and again do not necessarily map neatly to externally imposed Western conceptual frameworks.[144] One significant example is the idea of A2AD or 'counter-intervention', a notion originally developed to describe China's pursuit of integrated and layered stand-off capabilities, primarily in the air and maritime domains, to push US forces back beyond the island chains of the Western Pacific.[145]

While it is certainly true that Russia has invested heavily in its own integrated air defence systems (IADS), long-range precision strike and other capabilities, applying the lens of A2AD – a concept originating in Western minds and not in any Russian strategy or doctrinal documents – in the North-Eastern European setting produces a much greater emphasis on the land domain.[146] Understanding the differing drivers and barriers to operationalising MDI in this setting is important not only to understanding how Russia is and is not thinking about integration across multiple domains, but also to ensure that any Western concept of

[142] Radin et al. (2019).

[143] Sukman & Davis (2020).

[144] Thomas (2019); Kofman (2020).

[145] Heath & Erickson (2017).

[146] Bonds et al. (2017).

multi-domain operations developed for a particular adversary and context (e.g. defeating China in the air and at sea) is transferrable and applicable in any potential future conflict with Russia.[147]

A.2.3. Looking to the future, Russia is developing its theory and practice of integrated operations across multiple domains through several interrelated concepts

Confronted with a changing strategic and battlefield environment, the Russian military continues to modernise its forces, capabilities and operating concepts.[148] The overarching guidance and impetus for a growing focus on MDI is provided by Russia's 2014 Military Doctrine. This notes that contemporary conflicts are characterised by[149]:

- The integrated use of force and information and other non-military measures;
- The use of information management systems; and
- The ability to impose a simultaneous effect on the enemy to the full depth of his territory in global information space.

This necessitates an emphasis on emerging threats and opportunities arising from the information, cyber, electronic and space domains. In March 2018, General Gerasimov identified the need for Russia to prepare for complex warfare by leveraging multiple domains, stating: 'Each military conflict has its own distinctive features… besides [the] traditional spheres of armed struggle, the information sphere and space will be actively involved'. He also highlighted the need for continuing adaptation to modern and future war:

> The content of military operations is changing. Their spatial scope is growing, and their intensity and dynamism are increasing. Time parameters of the preparation and conduct of operations are shortening. There is a transition from successive concentrated actions to continuous distributed actions conducted simultaneously in all spheres of opposition as well as in remote [theatres of military operations].[150]

The following year, in 2019, General Gerasimov set out four directions for the development of future Russian military strategy that illustrated the growing shift towards (a Russian interpretation of) multi-domain thinking underpinned by information superiority:

1. Creating and developing a unified system of integrated forces and assets of reconnaissance, engagement, C2 and fire control based on state-of-the-art information and telecommunications technologies.
2. Promoting the use of military robotic complexes, especially unmanned aerial vehicles (UAVs), in line also with wider Russian efforts to develop strategic advantage through AI.

[147] Russia is 'a continental land power in a decidedly different geographical theatre and with a tradition of military thought distinct from China's… [A2AD] is not a concept in Russian military thought and there is no Russian strategy bearing that name… [Approaching Russian thinking on Russians' own terms is important, otherwise] the discourse turns into technology fetishism, and planners and strategists focus on procurement solutions to adversary capabilities rather than developing strategies to counter their operational concepts.' Kofman (2019).

[148] Radin et al. (2019).

[149] Thomas (2019).

[150] Griesemer (2018).

3. Countering adversary use of UAVs and PGMs, also involving a deciding role for EW forces and assets.
4. Increasing the combat might of the armed forces, determined by the numerical and qualitative composition of the force, its strength and outfitting, its morale and training, and its combat readiness and effectiveness.[151]

This increasing focus on MDI and information superiority is also reinforced through other related concepts that are prominent within Russian military theory and practice: namely, 'new-type warfare', 'information warfare', 'reflexive control' and 'disorganisation', which together aim to enable Russia to seize a decisive advantage in the shaping phase of any potential future conflict. The following sections discuss each of these in turn.

New-Type Warfare

Beneath the overarching strategic approach of 'non-linear' or 'liminal' warfare (see Section A.1.2), Russian strategic thinking in the narrower military sense is encapsulated in its writings on **New-Type Warfare**.

In 2015, General Lieutenant Andrey Kartapolov, then Chief of the Operations Directorate of the Russian General Staff, outlined the concept of 'new-type warfare' through asymmetric operations that maximise the exploitation of the cyber domain and information operations.[152] This concept perhaps most closely aligns with what is often referred to as 'hybrid warfare' in the West, a term that Russian authorities reject. New-type warfare is waged across multiple domains, including the physical and informational, under the aegis of Russia's nuclear capabilities, and seeks to manipulate the adversary's perception, influence its decision-making process and shape its strategic behaviour in favourable directions, while minimising the use and scale of kinetic force.[153] Kartapolov stated that unconventional ways and means are being developed to support military operations, which will exploit vulnerable areas that offer the best effect with minimal expenditure of Russia's own forces and resources.[154] These may include special forces operations, use of foreign agents and proxies and various forms of information effects, as well as political, economic and other non-military forms of activity. Doing so effectively requires integration of the political-military, political-psychological, and military-technical dimensions to ensure operational and strategic advantage.[155]

Some parallels can be drawn between Russia's new-type war and Western concepts of MDI/MDO, in terms of their stated aims of delivering effect through a cohesive system that is greater than the sum of its parts, as well as their emphasis on non-traditional or emerging arenas of competition and conflict. In particular, the exploitation of information and the cyber domain in new-type war is understood as allowing Russia to exercise 'reflexive control' (see below), control both strategic and operational tempo, and achieve cross-domain synergy and advantage. Russian military doctrine increasingly emphasises the role of cyber and information as important enablers, integrators and multipliers, helping to achieve cross-domain synergies.

[151] Thomas (2019).

[152] Sprang (2018).

[153] Adamsky (2015).

[154] Thomas (2019).

[155] Thomas (2019).

Crucially, they are viewed as a tool for exercising reflexive control and creating time, space and manoeuvre advantage for Russian forces. For example:

- **In the competition phase or initial period of a war**, cyber espionage can provide actionable intelligence on the planning operations of adversaries in other domains.
- **At the operational level**, cyber-attacks can disrupt or paralyse the joint C2 architecture of the adversary's networked forces.
- **At the strategic-political level**, coordinated information operations can inhibit the international community's understanding of the operational environment, creating decision paralysis or preventing a coordinated response among coalition allies.[156]

The recognition of cyberspace as a new operational domain has thereby provided Russia with new means to influence, disrupt and degrade the information and communications of the adversary to achieve effect within and across multiple domains.[157] This builds on longstanding Russian and Soviet concepts of deception, disinformation and political warfare, while providing new tools for the 21st century. Russia's new-type war therefore emphasises attaining information superiority as key to enabling indirect actions, and military and non-military measures. The importance of the space domain for achieving effect across the other military domains is also noted in Russian literature on new-type war. Observing that its potential adversaries (most notably the United States) accomplish their communications, navigation, reconnaissance, and all C2 of strategic nuclear, missile defence, and precision-guided munitions through space, Russian strategists recognise that a breakdown of these cohesive systems through the use of electronic and other asymmetric assets can largely reduce this advantage.[158]

This also aligns with the older Russian concept of **System Warfare**, which emerged in the 1990s and 2000s in response to observations of Western operations in the Gulf Wars and Kosovo, as well as informing the New Look reforms to Russia's beleaguered post-Soviet military. Russian strategists concluded that future wars would not be fought just force on force; this catalysed a revolution in Russian military thought and drove a shift in focus to system-on-system battles in space.[159] While there may be significant differences between the combat systems of opposing sides, Russia's system-on-system theory posits that the less developed system can succeed over a superior opponent if it possesses either greater organisational characteristics or greater functionality. These functions can be achieved via asymmetric or indirect means using signals, EW, or information and cyber means to undermine or disorganise such systems. System-on-system warfare, therefore, remains an important part of Russia's strategy for defeating a superior adversary through asymmetric means, exploiting capabilities in the space, cyber and electromagnetic domains.

[156] Sprang (2018).

[157] Kilcullen (2020).

[158] Thomas (2019).

[159] Thomas (2019).

Information Warfare

Within this new-type war, Russia's variations on multi-domain concepts are heavily centred on achieving asymmetric advantage by exploiting the information environment. At the same time, there is heavy concern that Russia's enemies, both foreign and domestic, might exploit this environment in order to sow dissent and chaos within Russia itself. This is a significant worry for the ruling regime, but also triggers painful memories for ordinary Russians of the divisions, upheaval and humiliation of the 1990s. There is hence a strong recognition in Russian military thinking that 'information warfare can make any state vulnerable to a revolutionary situation via an integrated use of the effects of various information resources and technologies',[160] and a desire to both counter hostile information operations within Russia while proactively striking at the will and cohesion of adversaries in their own societies, economies and governance systems.[161]

Russian understanding of information warfare has typically been divided into information-technical and information-psychological categories. Driven by Russia's technological advances and focus on achieving cross-domain synergies, these two aspects are now becoming increasingly integrated. For example, an information-technical cyber-attack against an adversary's banking sector could expose or manipulate data about the banking sector that causes information-psychological panic in the general population. Equally, the strategic disclosure of an information-technical achievement such as a status-6 nuclear torpedo could have a considerable impact on the information-psychological stability of a US coastal region that could be a hypothetical target of such a torpedo. In this regard, information-technical and information-psychological domains are viewed by Russian strategists as mutually supportive.

Reflexive Control

For information warfare to be successful, information superiority must be achieved. Russian information-technological operations therefore focus on the carriers of information – such as underwater cables and satellites – and EW means to degrade the C2 capabilities of foreign forces and undermine their societies. Russian doctrine also focuses on the ability to construct, rather than interrupt, information flows, and deceive an opponent with information specially developed for their consumption. This concept is referred to in Russia as the **Reflexive Control** of the adversary.

Reflexive control entails 'implementing measures and actions that incite the enemy to act in a corresponding way that is advantageous for our side…[making] it possible to change the enemy's goals and his methods of operation in favour of one's own forces'.[162] The aim is to induce the opponent to act in a way that benefits the proponent, for example by organising or manoeuvring in a certain way, or developing or employing certain weapons. In simple terms, it is a method of manipulating the adversary to create favourable conditions in order to accomplish an assigned mission. Russia may employ reflexive control from the tactical to the strategic levels; targeting may be as detailed as developing a psychological profile of specific officers in command positions and identifying pressure points (such as their family, social media or financial affairs).[163] Reflexive control can be leveraged across the military domains, exerting coercive pressure,

[160] Thomas (2019).

[161] Kilcullen (2020).

[162] Thomas (2019).

[163] Thomas (2019).

transmitting false information, influencing an opponent's decision-making algorithm, and achieving information and psychological effects. To be effective, a holistic idea of the armed struggle process in front of a commander must be viewed as an integrated system, where the creativity of a commander to adjust to this view of reality is essential to the successful use of reflexive control.[164]

Disorganisation

As already noted in Section A.2.2, there is no equivalent of the Western concept of A2AD in Russian military literature. However, there is a Russian term that describes how Russia may deny, or more likely delay, access to its territory; in particular, as a way to slow an inevitable US 'aerial blitzkrieg', impose costs and sow confusion,[165] and thereby create space and time for Russia to achieve its objectives quickly and force a political resolution on favourable terms.[166]

The Russian concept of **Disorganisation** describes a strategy for disrupting an adversary's C2, for example using radio-electronic combat (Radioelektronnaya Bor'ba or REB) capabilities. Disrupting adversary C2 is designed to impede the adversary's ability to coordinate and integrate the various aspects of their plans, including logistics, joint fire support, command over deployed troops, or any aspect of multi-domain coordination. This, in turn, should provide Russia with decision-making superiority and improved likelihood of victory. REB interventions, cyber effects and disinformation campaigns are all non-kinetic tools that can be employed in pursuit of disorganisation.[167] The Russian Armed Forces' extensive inventory of ballistic and cruise missile systems, tube artillery, MLRS and modern combat aircraft, and naval platforms and submarines also provides options for kinetic strikes to shape the deep battle or deny an adversary's use of air, land and sea LOCs. These do not only bring tactical benefits, but are rather understood as means of influencing the adversary's thinking at the strategic level: in this respect, 'the Russian General Staff has turned the Soviet Union's ideas into reality, developing recon-strike and recon-fire contours or loops, together with a long-range precision strike arsenal designed to deter or inflict unacceptable consequences, i.e. coerce the adversary.'[168]

While attempting to foment confusion or paralysis in the adversary's C2, Russian doctrine and training places considerable importance on creativity to enable Russia's own commanders to innovate and adapt to the unique requirements of any given operation. General Gerasimov has noted that the composition of strategy is not fixed but entirely flexible, and each situation has its own individual logic.[169] It therefore depends on the creative thought of commanders to best exploit the capabilities at their disposal in any given situation (in some respects an analogue to the Western notion of 'mission command', even within the structures of the historically more centralised, top-down Russian military).

[164] Thomas (2019).

[165] Kofman (2019).

[166] Shlapak & Johnson (2016).

[167] Thomas (2019).

[168] Kofman (2019).

[169] Thomas (2019).

Seizing Advantage in the Initial Period of War

An important consequence of thinking about 'reflexive control' or 'disorganisation' is that Russia's choices should remain concealed until they are utilised, with an array of missiles, satellites, underwater cables and electronic networks at hand to achieve rapid and devastating effect in a cross-domain way.[170] Indeed, Russian strategists, and Soviet leaders before them, have traditionally emphasised the importance of seizing advantage in the **Initial Period of War** (IPW). This concept is rooted in the notion that the readiness of the Armed Forces to fight can be the greatest determinant of success in an armed conflict. The emergence of cyber, EW, PGMs (even hypersonics) and automated control systems has magnified the importance of the IPW in Russian thinking. For example, protecting critical infrastructure from cyber-attacks (or targeting the critical infrastructure and systems of the adversary) may take precedence over other factors in the early stages of conflict. An example of Russian tactics for achieving IPW advantage could be to plant viruses in an adversary's systems during peacetime, disorganise these systems, then conduct large-scale information operations. These operations could also be conducted in conjunction with swift kinetic attacks in other domains to amplify effects across the domains and shape the early phases of a conflict, ideally to bring it to a quick resolution in Russia's favour before the need for protracted bloodshed on the battlefield.[171]

While the scenario-planning assumptions underpinning Russian military thinking focus on a defensive war with NATO close to Russia's borders, this does not mean that Russia views warfare as defence-dominant:

> The Russian General Staff does not see warfare as defence-dominant, and expects offensive operations to inflict critical damage, resulting in attrition and disorganization. Echeloned defence, as good as it looks on paper, by itself is a recipe for losing without offensive operations throughout the theatre, including the enemy homeland. As a consequence, one can detect a Russian preference for pre-emption and prevention in a threatened period of war in order to seize the initiative, rather than depending on layered defence. For example in a recent speech Gen. Valery Gerasimov, Russia's chief of General Staff, stated, 'The basis of "our response" is the "active defence strategy," which, given the defensive nature of the Russian Military Doctrine, provides for a set of measures to proactively neutralize threats to the security of the state.' In this context he emphasized initiative and pre-emption, adding, 'We must act quickly so as to pre-empt the enemy with our preventive measures, promptly identify his vulnerabilities, and create threats of unacceptable damage to it. This ensures that the strategic initiative is captured and maintained.'… Note the emphasis of pre-emption is not interdiction, but neutralisation, and inflicting unacceptable damage.[172]

Achieving this swift and decisive action in the IPW requires effective coordination of both military and non-military levers, integrating Russian operations in all theatres and all domains to achieve the overarching objective of a rapid dislocation and destruction of the adversary's C2 networks in the IPW and corresponding erosion of their capacity and will to sustain the fight.

[170] Thomas (2019).

[171] Thomas (2019).

[172] Kofman (2019).

A.3. What has driven or is driving the development of MDI concepts by the Russian Federation?

A.3.1. Russian leaders follow NATO – and especially US – concepts and capability development efforts closely, both as a source of learning and alarm

As outlined in the previous sections, the evolution of Russian military concepts has been driven in large part by a perceived threat from the West and a need to prepare for future complex warfare; leveraging cross-domain synergies is viewed as a means for achieving this.[173] The Russian strategic community has for example developed its concept of new-type war in response to what it understands to be a hybrid campaign directed by the West at Russia. In a 2019 speech, General Gerasimov noted that Russia's adversaries will orchestrate indirect actions to destabilise Russia internally while simultaneously conducting military operations and inflicting precision strikes on critically important targets.[174]

A.3.2. Contemporary Russian military thinking also draws on its rich inheritance from its Soviet predecessor, while updating these concepts to reflect new technology

Though Russian defence concepts have evolved due to a mix of internal adaptation and changes in the external environment over the last three decades, there are some enduring similarities between contemporary doctrine and the way that both strategic thinking and the operational art were expressed in the Soviet era. This includes both general trends and specific processes that have carried over from the Soviet era to the Russian way of configuring and managing threats and thought.[175]

Some of the main continuities between Soviet and modern Russian thinking are presented in Box 3.

Box 3. Comparison of Soviet and Russian military thinking

Fear of encirclement: Soviet leadership expressed concern over capitalist encirclement. Today's Russian leaders fear NATO encirclement.

Seizing advantage in the IPW: In the Soviet era, mobilisation priorities and deployment schedules were emphasised as a means for taking advantage in the IPW. Today, Russian thinking on the IPW is focused on cyber capabilities, such as disrupting the adversary's digital infrastructure to destroy their state control facilities.

Recon-fires and the importance of the deep battle: Studies of deep strikes in the Soviet era included ways of using aviation and special forces to strike deep into an opponent's territory and strike at command posts. Russia's modern concept of deep strikes includes cyber deep strikes to disrupt or destroy stock markets, while hypersonic weapons are designed to strike high-value targets on the other side of the globe.

Source: Thomas (2019).

The general concepts outlined above are also heavily impacted by technological developments and recent military experiences (see Section A.3.3 below), and thus continue to evolve rapidly; previous concepts such as annihilation, attrition and manoeuvre are all dramatically affected today by the new power and speed

[173] Griesemer (2018).

[174] Adamsky (2015).

[175] Thomas (2019).

enabled by modern technologies. The potential speed and simultaneity of manoeuvre and destruction across the military domains is where contemporary Russian thought differs from its Soviet predecessors.[176] Technology has driven a new impetus and immediacy to military thought; for example, today the IPW may last only a matter of seconds or minutes if the cyber-enabled destruction of an opponent's infrastructure and C2 is achieved. Cyber capabilities have extended the reach of Russian strategy to a global scale; new reconnaissance capabilities of UAVs and satellites have increased the speed and influence of operational decision; and EW now enables the disorganisation of an adversary's C2 facilities. The immediate consequences of the use of technologies, therefore, are their impact on the speed of decision making and the vast scale of territory to which such thinking can be applied; this has also driven the emergence of more cross-domain thinking and a focus on pursuing synergies across the new and traditional domains. Moreover, technology no longer influences only tactics; it also influences Russian strategy.[177]

A.3.3. Russia has also demonstrated a capacity to identify and operationalise the lessons learned from experiences in Chechnya, Georgia, Ukraine and Syria

As well as observing evolving Western approaches to network-centric warfare, the Russian military has also learned useful, if also painful, lessons from its own battlefield experiences in recent decades.[178] These include humiliations at the hands of Chechnyan insurgents at the former Red Army's lowest ebb in the 1990s, as well as recognition of the litany of tactical shortcomings demonstrated in the 2008 Georgian War.[179] Despite reforms to promote the professionalisation and modernisation of the Russian Armed Forces after they were effectively hollowed out in the years after the Cold War, Russia entered the Georgian conflict, the Ukrainian civil war and the Syrian civil war feeling comparatively weak and under-equipped. Under Gerasimov and others there has been a deeply felt lack of capability vis-a-vis the United States and NATO, and so a premium was set on developing asymmetric tactics and capabilities that would offset Western advantages.[180]

Accordingly, the Russians experimented with new ways of war in those theatres. Russian military thought has benefited from the conduct of serious lessons-learned analyses of combat operations in Syria, as well as Chechnya and Ukraine. These recent combat experiences have driven the understanding of strategic information confrontation, and have influenced the development of both the theory and practice of disorganisation. For example, Russian combat experiences in Chechnya and against the Islamic State (IS) in Syria highlighted that disorganising the opponent's C2 at the initial stage of combat operations can accelerate the attainment of tasks and goals; EW and aviation assets were identified as the primary means for conducting this disorganisation.[181] Experiences facing state militaries across the battlefield in Ukraine and elsewhere also brought five key lessons about what to expect from future warfare[182]:

[176] Thomas (2019).

[177] Thomas (2019).

[178] Chekov et al. (2019).

[179] Kilcullen (2020).

[180] Bender (2016).

[181] Thomas (2019).

[182] Chekov et al. (2019).

1. States will increasingly implement clandestine, deniable actions, including through use of proxies, in order to avoid 'the complications associated with direct collision of powers'.
2. 'The time to prepare for a military operation has significantly decreased, whereas the need for quick and intelligent decision-making has grown', reinforcing the requirement for reconnaissance-fire complexes to provide for 'swift and continuous strikes on the adversary', as well as emphasising the need for force mobility, dispersed operations and access to a range of non-kinetic effects.
3. The increasing reach and precision of guided munitions, backed by more accurate and selective targeting, 'significantly extends the traditional borders of operational theatres to encompass not only military facilities, but also objects of economic significance that may be thousands of kilometres away from an immediate war zone'.
4. 'Crises can be expected to emerge simultaneously in several theatres', necessitating development of rapid reaction forces in all armed services to respond to threats and opportunities that emerge.
5. Given all of the above, there is a need to create windows of advantage in time, space and manoeuvre, including through forward deployment of ISTAR and strike assets, and investment in automated C2 systems to reduce the time between initial reconnaissance and target engagement.

Importantly, such lessons do not appear to be falling on deaf ears. International observers of Russia's operational experience in recent conflicts suggest that the Armed Forces' learning process appears to be tolerant of risk and failure, and has shown conceptual flexibility and dynamism, and an overall willingness to adapt.[183] Further examples of the practical application of MDI concepts are provided below.

A.4. How do Russia's concepts of MDI manifest in practice?

A.4.1. Russia continues to implement major reforms, equipment and research programmes to modernise its forces, but important barriers to MDI remain

The Russian military's ambition and willingness to learn from experience and translate new conceptual thinking into practice is reflected in its ongoing reforms, which are modernising and professionalising the Armed Forces to prepare for complex warfare and embrace aspects of MDI. At the same time, significant capability shortfalls and other challenges remain, including an uncertain economic base for defence investment, widespread corruption and a fragile defence industry and technology sector, which are hampered by international sanctions. This is reflected in Russian perceptions of an ongoing race to enhance its cross-domain capabilities and exploit a window of opportunity to secure Russia's (and the regime's) interests by the late 2020s, before Russia's competitive position falls back relative to an already dominant US or a rapidly rising and ambitious China (see Annex B for more on the PLA's own modernisation).[184]

Force structure

The restructuring of Russia's military over the past 12 years highlights its deliberate efforts to create a more cohesive, integrated force. Beginning in 2008, Russia's military reorganisation not only eliminated redundancies and increased the lethality and efficiency of its Soviet-era force, but also focused on developing

[183] Adamsky, cited in Howard & Czekaj (2019, 381).

[184] Kilcullen (2020).

organisations, equipment and tactics that were designed to synchronise operations across the domains. Russia's military reorganisation, combined with the concepts set out within its military doctrine (see Section A.2) illustrates that Russia is intentionally moving towards a form of MDI in both theory and practice.[185]

At the centre of Russia's reorganisation was its primary fighting unit, the Battalion Tactical Group (BTG). Russia's new integrated approach to warfare seeks to provide BTG commanders with capabilities across the domains, enabling them to execute operations in a multi-domain fashion. This has included the integration into the BTG of surface-to-air missiles, UAVs and EW capabilities – key enablers that were traditionally siloed and held at higher echelons. Rather than being limited to certain capabilities within an inflexible force structure, under the new configuration of the Armed Forces, BTG commanders select the key enablers to incorporate into their unit to achieve a specific operational effect. This empowers the BTG commander to use their own creativity and initiative to harness capabilities that span the multi-domain environment. Therefore, not only does the organisational structure and equipment exist to enable multi-domain operations in the BTG, but BTG tactics also support large-scale multi-domain operations. In this regard, the BTG has been configured as an inherently multi-domain force.[186]

Recent restructuring at higher levels within the Russian military also reflects a growing recognition of the need for integration, and with it, rationalisation. Between 2007 and 2012, a succession of reforms has reapportioned C2 responsibilities between the General Staff, military districts and service Main Commands. The latter were 'relegated largely to "train and equip" roles, while the military districts became truly "joint" commands, and the General Staff became the authority for all operational and strategic planning'.[187] These reforms have been followed up by the establishment of the Northern Fleet Joint Strategic Command as a single multi-domain command for all combined and regional forces in the High North, and reorganisation of the other military districts as organisational-strategic commands (OSKs). At the highest levels, Russia has invested in a National Defence Control Centre (NDCC) to provide a fortified physical site and associated integrated information infrastructure for national C2 in times of crisis.

The establishment of the NDCC is also part of a larger set of reforms that are aimed at enabling the mobilisation[188] of internal security troops (the National Guard) in time of crisis or war, and improving their coordination with the military forces, to respond to the integration of internal and external threats. Other changes made to facilitate the greater coordination of military forces and internal security troops include updates to laws and policies for improving whole-of-government crisis response, legal authorisation for the National Guard to support military operations overseas, and command adjustments at the regional and municipal levels.[189] However, it should be noted that as of October 2021, there is no firm evidence that

[185] Griesemer (2018).

[186] Griesemer (2018).

[187] Whisler (2020).

[188] State mobilisation (or *mobilizatsiya*) can be defined as 'a complex of state measures for activating the resources, strengths, and capabilities for the achievement of military-political goals'. The 2015 Law On Mobilisation, and the National Defence Plan 2016–2020, set the framework for state mobilisation. See: Charap et al. (2021).

[189] Charap et al. (2021).

these legal and administrative steps have translated into the more effective practical integration of military and internal security forces.[190]

There have also been reforms to improve integration between domains by reorganising each of the individual services in the Russian Armed Forces. In 2015, for example, the Russian space force was merged with the air force to create the branch now known as the Russian Aerospace Forces. The Russian Aerospace Forces is a three-branch service that combines elements of the space force, air force, and air and missile defence forces under a single command; this consolidation was driven by Russia's understanding that the space domain is increasingly integrated with the other domains, for example with space assets as critical enablers of operations in other domains. The intelligence, surveillance and reconnaissance (ISR) capabilities needed for anti-satellite (ASAT) missions, air defence and missile defence are closely interconnected and multirole. For example, long-range radars can be used to track missiles, control airspace and track satellites in orbit. This restructuring therefore enables the Russian military to harness greater efficiencies and synergies between operations in these domains.[191]

The Russian military now includes several subunits that include information operations within their remit. This includes the Main (Intelligence) Directorate, the Main Directorate for the Development of Information and Telecommunications Technologies, and the Press Service and Information Directorate. In February 2017, the Russian Armed Forces was also reported to have established a dedicated information force, reflecting the significance that Russian strategists place on information operations and psychological warfare. Previous statements from Russian leadership also indicate that Russia's cyber forces amount to around 1,000 soldiers, and that the information space is now viewed as equally important as the land, sea and air domains.[192]

Capabilities and acquisition

Within Russian thinking, practical integration across the military domains requires:

- The development of information confrontation forces and assets.
- Upgraded information exchange systems that unify the Armed Forces information space with the wider Russian Federation information space.
- The integration of information-control systems with fire control systems and automated C2 systems at the strategic, operational-strategic, operations, operational-tactical and tactical levels.[193]

Recent modernisation and procurement efforts appear to reflect a recognition of these requirements, while also reflecting the enduring limitations on the financial and technical resources available to the Armed Forces, despite their privileged position and prioritisation by the ruling government. The essential capabilities of the Soviet Red Army were retained for 15 years after the collapse of the Soviet Union.[194] Since 2008, the Russian military has undertaken ambitious reforms to replace or modernise 70 per cent of its

[190] Charap et al. (2021).

[191] Bodner (2018).

[192] Thomas (2019).

[193] Thomas (2019).

[194] Barabanov et al. (2012).

military equipment by 2020, and overhaul the defence industrial base to support this.[195] Though severely limited by finances and developmental barriers (it has not made its original 2020 deadline, and its 2021 defence budget has plateaued), Russia maintains focused efforts to modernise its forces and equipment.

The 2014 Military Doctrine notes the importance of integrated weapons suites – which are able to conduct integrated operations in an information-critical environment – instead of the traditional 'simplicity + mass' formula of the Soviet years. This guidance states that 'the tasks of equipping the Armed Forces and other troops and… weapons' should include:

- **Improved means of information exchange** through the use of modern technologies and international standards, as well as a common information space of the Armed Forces, other troops and authorities as part of the information space of the Russian Federation.
- **Creation of new types of precision weapons** and the means to counter them; air and space defence systems communications; intelligence and control; EW; unmanned flying devices; modern transport aircraft; and personal protective equipment.
- **Creation of basic information management systems** and their integration with control systems and weapons complexes, as well as automated controls at the strategic, operational and tactical scale.[196]

This doctrinal statement appears to align with observed Russian acquisition activities. For example, in 2016 the Russian military completed a 'closed data transfer segment' internal communication system that is independent from the global Internet. It can only be accessed through special licensed computers using a dedicated Defence Ministry operating system. In May 2018, further investments had been made to 'provide for the creation of an integrated communications network for the needs of national defence, national security, and law enforcement'. This not only highlights Russian efforts to create more integrated communications systems, but also suggests the creation of a 'backup Internet' infrastructure in Russia, bolstering not only military but broader governmental and societal resilience against hostile information activities targeting Russia.[197] Russia's pursuit of sophisticated space-based capabilities also highlights a growing focus on that domain, and the exploitation of space assets to conduct reflexive control, disrupt information flows and undermine operations in other domains.[198]

These examples highlight ongoing Russian efforts to develop and acquire new capabilities that will enable the close integration of systems in space, cyber, EM and the traditional air, land and maritime domains in

[195] Massicot (2019).

[196] Russian Federation (2014, para 46).

[197] Thomas (2019).

[198] Russia's existing ASAT weaponry includes the Tirada-2S, which is designed to interfere with information flows and is capable of radio-electronic suppression or jamming or complete disabling of communication satellites. The Tirada is ground based and thought to receive target designation from Russia's Missile Attack Warning System. Similarly, the ASAT Kontakt missile can be launched from a MiG-31 aircraft; the S-500 Prometey air defence missile system is designed to intercept orbital vehicles; and the Nudol space missile is part of the A-235 missile defence system and capable of interceptions at ranges up to 1,500 kilometres. Russia has also developed 'inspection satellites' than can inspect other orbiting satellites to determine their function. They can therefore be used as reflexive control functions for purposes such as deterrence, for example by indicating that the function of an adversary satellite has been discovered and subsequently neutralised, when in fact they may not have been. See Thomas (2019).

support of disorganisation operations. Looking to the future, the State Armament Programme (GPV 2027) – approved in 2018 – forms the basis of Russia's defence procurement and military priorities until 2027. It is expected to build on the progress made under the previous programme, GPV 2020, and further strengthen and modernise the Russian Armed Forces to prepare for complex warfare across domains.[199]

Operations and practice

Recent Russian activities and military posturing suggest that Russian operations can include multi-domain linkages within the same physical domain. Russian maritime operations in the North Atlantic provide just one example of this. Open-source evidence suggests that the Main Intelligence Directorate (GRU) has developed deep-diving submarines that would be capable of accessing underwater cables that provide Internet connections between states divided by water.[200] The Barents Sea is also known to be an important Russian SSBN bastion, while modern SSNs and SSGNs[201] are reported to be one of the more competitive areas of Russia's conventional military technology, and thus one of the best prospects for achieving conventional military coercion against NATO maritime forces.[202] Therefore, it is entirely possible that on any given day, Russia could be integrating cyber, conventional and nuclear operations all within the same physical (maritime) domain, or even within the same North Atlantic theatre.[203]

Open-source information on Russian operations in Ukraine similarly provide many practical examples of the strategy of multi-domain coercion, imposing costs in one domain to achieve deterrent effect in another.

[199] Connolly & Boulègue (2018).

[200] Glanz & Nilsen (2020).

[201] SSBN refers to the US Navy and NATO hull classification for a nuclear-powered ballistic missile submarine; the classification SSN refers to a nuclear-powered attack submarine; and SSGN refers to a nuclear-powered guided missile submarine (equipped with conventional cruise missiles but not nuclear-armed ballistic missiles).

[202] Majumdar (2014); Lacey (2020).

[203] Thomas (2019).

Box 4. Case study: Russian multi-domain operations in Ukraine

Russian operations in Ukraine displayed the characteristics of multi-domain warfare. In the Battle of Zelenopillya (2014), a single Russian BTG commander is known to have deployed organically held weapons spanning the domains against Ukrainian forces. What made this operation distinctive was Russia's concerted use of organic UAVs, cyber capabilities and ground forces under a single battalion commander to accomplish a combined effect. The Russian forces first executed cyber-attacks to disrupt Ukrainian communications and confuse decision making. While Ukrainian C2 was suppressed, the *Orlan 10* UAV conducted detailed target acquisition of the Ukrainian position, followed by a devastating strike by long-range rocket and artillery to destroy the Ukrainian unit.[204] These tactics were repeated in subsequent confrontations involving different BTGs, including at the Battle of Ilovaisk (2014), Battle of Donetsk Airport (2014–2015) and the Battle of Debal'tseve (2015).[205]

The integration of Surface-to-Air Missiles (SAMs) and UAVs into the BTG highlights identified synergies between the land and air domains. Furthermore, the EW capabilities of ground-based jammers in addition to EW capabilities embedded into UAVs illustrated interdependencies between the land and EM spectrum, in addition to with the air domain.[206] In these confrontations, the use of the cyber domain created early windows of opportunity for success, and the simultaneous execution of offensive and defensive tasks across strategic and operational levels, and other domains.[207]

These examples of multi-domain warfare at the BTG level in Ukraine appear to be part of a bigger effort that illustrates Russia's exploitation of high-technology assets for modern warfare across the domains, especially linked to force enablers and multipliers.[208] Notably, these examples highlight how Russia has begun to operationalise its own multi-domain concepts through new-type war to achieve 'time, space and operational advantage'.[209]

A.5. What does the current literature suggest about the future developments and approaches to MDI by Russia (e.g. out to 2025, 2030, 2040)?

A.5.1. Russia remains beset by structural challenges and shortcomings, but continues to adapt in pursuit of advantage across military and non-military domains

Examination of Russian doctrine and activities reveals an evolution in military thinking that is encapsulated by its new-type war, which focuses on asymmetric methods for exploiting and integrating capabilities across the domains to achieve information superiority, disrupt the C2 of opponents and challenge militarily superior adversaries. The recurrent use of multi-domain warfare in Ukraine across multiple BTGs operating in separate areas (see Box 4) highlights that Russia has begun to operationalise its own unique variation on multi-domain concepts, and suggests that this is a developed tactic the Russian forces will continue to use

[204] Griesemer (2018).

[205] Sprang (2018).

[206] Griesemer (2018).

[207] Sprang (2018).

[208] McDermott, cited in Howard & Czekaj (2019).

[209] Sprang (2018).

in future confrontations.[210] It is expected that Russian military thinking will continue to evolve; new concepts, tactics and methods are continuously developed, drawn from lessons learned in Syria, Ukraine, and in dealing with the Arctic, as well as being driven by technological developments, observations of Western (and emerging Chinese) approaches and a desire to exploit the opportunities that these present.[211] Particular attention is placed by Western analysts on Russia's strong desire to achieve information superiority in the IPW; its attempts to manipulate the adversary's perceived reality and obstruct or distort information flow; and the use of new technologies and tactics in one domain to meet its objectives in another. Russia's continued consolidation and reinterpretation of established Soviet strategic and operational concepts to address new domains and new technologies is expected to provide a model for further conceptual development in the future.[212]

[210] Griesemer (2018).

[211] Thomas (2016); Griesemer (2018).

[212] Griesemer (2018).

Annex B. Case study: People's Republic of China

B.1. Summary of China's approach

B.1.1. Today the PLA envisages future warfighting as a multi-domain confrontation between 'systems of systems', but China seeks to avoid needing to fight by integrating all levers of power to gain dominance in the competition phase

When conceptualising China's approach to MDI or related concepts, it is useful to distinguish between its 'broad' (geopolitical and strategic competition) and 'narrow' (military operational) concepts[213]:

- **A broad understanding** of China's multi-domain concepts considers the use of all non-military (economic, political and informational) means to shape the strategic environment in China's favour, with the aim of achieving A2AD, but also ensuring that they will never need to get to the point of full-scale conflict that would necessitate systems destruction.
- **In narrow terms,** China's multi-domain thinking is characterised by its understanding of the networked, information-dependent context in which any future high-end war (e.g. with the United States) will be fought, and its focus on disrupting or destroying the adversary's 'system of systems'.

China's evolving strategic concepts are characterised by a multitude of layers of multi-domain thinking, which are broadly defined and all designed to affect future military engagement, but with various degrees of removal from the actual battlespace. They are also informed by the historical evolution of the PLA as the armed wing of the Chinese Communist Party (CCP) – rather than as an institution of the state – and its focus for many decades on political warfare, guerrilla warfare and internal repression. This ensures a distinct Chinese approach in both theory and practice, while also taking lessons from Western (primarily US) concepts of modern warfare, as demonstrated in operations from 1991 onwards.[214]

B.1.2. China's broad understanding of strategic competition is reflected in theories of 'Unrestricted Warfare', as well as its 'Three Warfares' doctrine

In the broadest sense, China understands the current state of global competition – and especially its contest for primacy with the United States – as a continuous effort to bring all available military and non-military levers to bear in pursuit of its strategic objectives, as demonstrated by its Military-Civil Fusion (MCF) strategy. This bears some similarities with Western notions of a whole-of-government or comprehensive

[213] Internal interviews with RAND expert, 29 May 2020.

[214] J.S. Johnson (2018).

approach, though the unique structures of the Chinese state ensure a unique approach 'with Chinese characteristics'. This includes, but is not limited to:

- A long-term perspective to strategy making and implementation, unencumbered by the short-termism and electoral cycles of democratic politics.
- A multipronged strategy to influence in its favour the rules, standards, norms and institutions that regulate the post-world war international system and global governance.
- A mercantilist approach employing Chinese economic clout and the CCP's close relationship with state-owned enterprises (SOE) to buy up strategic assets – most notably by investing in major infrastructure projects in both developing and advanced economies, including through its flagship Belt and Road Initiative (BRI) – that contribute to political and commercial leverage overseas.
- Heavy investment in technological and industrial development and promotion of a dominant market share in the supply of key enabling technologies and raw materials (e.g. rare earth minerals) to make China a crucial player in global supply chains.
- A concerted campaign of technology transfer, including both legal means and illegal cyber or industrial espionage, to acquire and steal intellectual property from other nations and their governments, businesses and universities.
- Mobilisation of the Chinese diaspora to gain support for its policies and control opponents.
- Imposition of legal and technology-enabled mechanisms to control dissent at home and abroad among its diaspora.
- Use of a set of technological, media, educational and cultural tools for exerting influence on foreign individuals and shaping a pro-China narrative.

This overarching approach to strategic competition is reflected in the **Three Warfares** doctrine that China adopted in 2003.[215] This focuses on the need to develop and employ capabilities for 'psychological warfare, public opinion warfare and legal warfare ("lawfare")'[216], moving beyond the traditional military domains of land, sea and air to pursue advantage in the information and cognitive domains.

In several respects, this doctrine built on the tenets of **Unrestricted Warfare**. This was put forward in 1999 in a short treatise published by Qiao Liang and Wang Xiangsui, senior colonels in the PLA air and ground forces respectively. While never officially endorsed, it has been extensively discussed and debated by analysts who follow Chinese military developments in the West; it is itself evidence of the capacity for lively internal debate over conceptual issues within the PLA (despite the centralised and politicised culture of that organisation). This concept of warfare broadens the definition of war far beyond the battlefield, articulating a modern Chinese perspective on war that is, instead, unrestricted. In this respect, China's 'vision of security has expanded to include virtually all policy domains'.[217] It theorises that war is no longer about 'using armed force to compel the enemy to submit to one's will'; instead, 'non-war actions may be the new factors

[215] Office of the Secretary of Defense (2019).

[216] Office of the Secretary of Defense (2019).

[217] Heath et al. (2016, 10).

constituting future warfare' as a continuous effort that involves 'using all means... military and non-military, and lethal and non-lethal… to compel the enemy to accept one's interest'.[218]

Table 1 provides examples of the many and varied military, 'trans-military' and 'non-military' forms of warfare that are conceptualised within this Chinese 'unrestricted warfare' framework.

Table 1. Overview of military, trans-military and non-military methods of unrestricted warfare

Military	Trans-Military	Non-Military
• Nuclear warfare • Conventional warfare • Biochemical warfare • Space warfare • Tactical warfare • Electronic warfare	• Diplomatic warfare • Network warfare • Intelligence warfare • Psychological warfare • Guerrilla warfare • Terrorist warfare • Virtual warfare (deterrence)	• Financial warfare • Trade warfare • Resources warfare • Ecological warfare • Economic aid warfare • Regulatory warfare • Smuggling warfare • Drug warfare • Sanction warfare • Media warfare • Ideological warfare

Source: Kilcullen (2020, 206), adapted from Qiao Liang and Wang Xiangsui (1999, 146).

B.1.3. In parallel, China is preparing for the future high-end fight, based around concepts of 'informatised warfare' and multi-domain 'systems confrontation'

In a competition for advantage, there is nothing new in trying to nullify or avoid an opponent's strengths (e.g. US military dominance) by adopting an asymmetric strategy that exploits their comparative weaknesses in other areas (e.g. the reliance of the US military on local allies for basing in the Indo-Pacific, encouraging China to seek to undermine the United States' partnership through economic, diplomatic and other means).[219] However, David Kilcullen argues that China's contemporary approach constitutes a more nuanced and difficult challenge for the West, reflecting 'not actually avoidance but rather a combination strategy.'[220]

On the one hand, China's unconventional and unrestricted approach, using all levers of power to position itself for advantage below the threshold of armed conflict, severely tests the bandwidth of Western governments to track, understand and respond to Beijing's concerted campaign of strategic competition in all sectors and on all fronts. This approach seeks to exploit an area of (perceived) weakness for democratic governance and open, liberal societies in the United States and Europe. At the same time, the PLA's ongoing efforts to prepare for future multi-domain conflict present a pacing threat to the United States and NATO's military dominance, meaning the West is also distracted by the need to defend a diminishing lead in the area of its relative strength:

> Chinese conventional military modernisation… challenges the United States directly in its sweet spot, forcing American planners [and their allies, e.g. the UK]

[218] Qiao & Xiangsui (1999), translated in Kilcullen (2020, 201–202).

[219] J.S. Johnson (2018).

[220] Kilcullen (2020, 208)

> to keep developing conventional concepts and capabilities, and encouraging the United States to keep sinking money into costly weapons and high-end platforms to support an exquisitely expensive warfighting style… This combination strategy encourag[es] the United States to double down on conventional capacity while simultaneously developing alternative, asymmetric options.[221]

This dual challenge from Chinese conceptual thinking combines the 'broad' and 'narrow' understandings of multi-domain, both above and below the threshold between competition and armed conflict. To focus this case study on those aspects that are most relevant to the UK's own emerging MDI concepts, the following sections focus primarily on the 'narrow' dimension of China's MDI – specifically, its understanding and exploitation of 'system of systems', the informatisation of conflict, and the means by which it is seeking to operationalise the new space, cyber and electromagnetic domains.

B.2. How does the People's Republic of China think about domains and how, if at all, does it conceptualise multi-domain integration?

B.2.1. Chinese literature recognises the growing importance of cyber, space and the electromagnetic environment, as well as the cognitive domain

The terms 'multi-domain operations' or 'multi-domain integration' are not included in modern Chinese military doctrine. However, since the 1990s the PLA has considered joint operations as the 'basic form' of war, and identifies a requirement for joint operations within and across the traditional domains of land, sea and air, as well as cyber, space and the electromagnetic environment.[222] As noted in the Science of Military Strategy published in 2013, the PLA also emphasises deeper integration across all levels of command including the strategic, operational and tactical levels.[223] Hence, the PLA appears to be seeking to develop increasingly integrated systems and force structures that can conduct operations in all these domains and at all levels to combine a range of kinetic and non-kinetic effects.[224]

PLA literature suggests that China's understanding of the military domains encompasses the traditional domains of air, sea and land, as well as increasing recognition of the space,[225] cyber and electromagnetic domains.[226] As noted in China's 2013 Science of Military Strategy, 'the emergence of new deterrence forces, based on new technology such as information, cyberspace, space and new-material technologies, is revolutionarily changing the mechanism, method and area of [military] operation'.[227] Recent PLA doctrine also places considerable emphasis on the 'cognitive' domain; cognitive domain operations seek to use information to influence the cognitive functions of the adversary, whether in terms of peacetime public

[221] Kilcullen (2020, 208–209). NB: the addition of a reference to the UK is by the RAND authors.

[222] Burke et al. (2020).

[223] Burke et al (2020).

[224] Internal interview with RAND expert, 2 June 2020.

[225] China officially designated space a new domain in its 2015 Defense White Paper. For more information, see: Office of the Secretary of Defense (2019).

[226] Beauchamp-Mustafaga (2019).

[227] Shou (2013), quoted in Qiu (2015).

opinion or governmental or military decision-making in conflict. This reflects the growing centrality of information to Chinese warfighting, as well as an emphasis on the human, moral and political components of warfare inherited from the Mao-era focus on revolutionary 'people's war'.[228]

B.2.2. The PLA focuses on military operations under informatised conditions, seeking to confront, disrupt and ultimately prevail over an adversary's system of systems

Today, new Chinese doctrinal concepts are developing that are designed to reflect and support the increasingly cross-domain nature of military operations. Most important to the PLA's theory and practice of 'integrated joint operations' are the notions of 'informatisation' and 'systems confrontation',[229] which share many central characteristics of what the West might describe as multi-domain concepts.[230]

Informatised warfare

At the centre of China's understanding of its strategic environment is the concept of **Informatised Warfare** (and increasingly **Intelligentised Warfare**)[231]; namely, the notion that superior command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities are paramount to military effectiveness. The PLA uses this term to describe the process of 'acquiring, transmitting, processing and using information to conduct joint military operations across the domains of land, sea, air, space, cyberspace and the electromagnetic spectrum during a conflict', utilising 'near-real-time shared awareness of the battlefield in enabling quick, unified effort to seize tactical opportunities'.[232]

This ability to transmit, process and receive information is seen as a vital enabler of everything the PLA wants to achieve;[233] informatisation therefore lies at the heart of China's military doctrine. The conduct of war under informatisation conditions requires an array of fully integrated technological, doctrinal, operational and organisational capabilities.[234] It requires reliable secure communication and imaging satellites; advanced navigation systems; a range of imaging, communication, radar and EW systems; and developing the PLA's capabilities for 'C2, comprehensive support, multidimensional protection, joint firepower strike and battlefield manoeuvre'.[235]

At the same time, the adversary's ability to employ sensing capabilities to provide situational awareness and targeting data for its own networked forces must be disrupted or denied. In the context of conflict in an informatised environment, the PLA has for example emphasised the necessity of 'destroying, damaging, and interfering with the enemy's reconnaissance and communications satellites', suggesting that space-based

[228] Shou (2013), quoted in Qiu (2015).

[229] Cozad (2016).

[230] Scouras et al. (2017).

[231] China's concept of informatised warfare is currently evolving into a new, closely related concept of 'intelligentised warfare', catalysed by the advent of AI/ML, advanced data analytics and cloud computing. Intelligentised warfare seeks to leverage the opportunities of disruptive technologies to enable human-computer hybrid operations in support of an evolved systems-of-systems approach to armed conflict. See: Burke et al. (2020).

[232] DIA (2019a).

[233] Kania & Costello (2017).

[234] Costello & McReynolds (2018).

[235] DIA (2019a).

systems would likely be among the targets of attacks designed to 'blind and deafen the enemy' in a systems confrontation. China has correspondingly developed a counter-space strategy that aims to create a denied, degraded and disrupted space operations environment (D3SOE) against advanced adversaries in future conflicts, for example through the use of ASAT weapons.[236]

Within the PLA's overarching concept of informatised warfare, the cyber and electronic domains can be understood as critical integrators and enablers of kinetic operations in the other domains, as well as being platforms for influence operations under China's Three Warfares strategy.[237] The PLA has adopted a formal information warfare strategy known as **Integrated Network Electronic Warfare (INEW)**, which requires a fully networked digital architecture capable of coordinating military operations in all domains and across the electronic spectrum.[238] INEW stipulates the integrated use of EW, computer network operations (CNO), and limited kinetic strikes against key C4ISR and computer nodes to disrupt the adversary's battlefield network information systems. This strategy is also closely aligned with the PLA's doctrine for the conduct of warfare for limited objectives under informatised conditions, as well as its concept of 'information blockade' or 'information dominance'.[239] Exploiting the interdependencies between the space, cyber and electromagnetic domains, and their integration with the traditional domains of land, sea and air, is embodied within China's related concept of a confrontation between 'systems of systems'.

China's theory of 'systems confrontation'

The PLA's prominent theory of war and (military) victory is referred to as **'Systems Confrontation'**. In the existing literature, this is often used interchangeably with related terms such as 'systems attack' and 'systems sabotage warfare'.[240] This concept is based on the perception that modern military forces are greater than the sum of their individual parts (e.g. armoured vehicles, naval platforms, aircraft, etc.).[241] The PLA conceptualises modern military forces as 'systems of systems' that are stronger, more capable and efficient than their constituent parts would be in isolation, as they are networked together through communications and information systems architecture. The PLA's understanding of modern and future warfare, therefore, is one of competition between these rival 'systems of systems', rather than between distinct units, platform-to-platform or between individual opposing military services. PLA doctrine indicates that China believes that whichever side has a more networked, integrated and cohesive force will have shorter Observe, Orient, Decide, Act (OODA) loops, operate more efficiently, and ultimately have a better probability of victory. This concept indicates the existence (or active pursuit of) fully integrated activities across the electromagnetic spectrum and all domains within China's military, as well as explicit recognition of the inherently integrated, cross-domain operating concepts of Western militaries.[242]

[236] Gibson (2019).

[237] Office of the Secretary of Defense (2019).

[238] Scouras et al. (2017).

[239] Office of the Secretary of Defense (2019).

[240] Scouras et al. (2017); US Joint Staff (2018).

[241] Johnson (2018).

[242] Scouras et al. (2017).

Based on this principle, systems confrontation is China's 'basic operational method' of warfare that seeks to overcome advanced adversaries by systematically targeting the linkages and nodes that hold an advanced network-centric force together as a cohesive whole.[243] This theory of victory is emphasised in China's 2019 Defence White Paper, which states that the PLA's 'integrated combat forces… [are to be] employed to prevail in system-vs-system operations featuring information dominance, precision strikes, and joint operations'.[244] In practice, 'systems warfare' entails thoroughly degrading the C4ISR capability of the adversary and thoroughly fragmenting its 'system of systems' into isolated component parts, to the point that the adversary lacks either the capability or the will to counter Chinese operations.[245]

Systems attacks are designed to facilitate follow-on operations; once systems attacks have fragmented the adversary's systems so that it can no longer operate as a cohesive force, this creates a favourable environment for the PLA to commit its own intact networked force to combat, continuing to carry out supplemental attacks to ensure the adversary's system does not recover while launching kinetic attacks against the adversary's aircraft, ships, submarines and long-range strike platforms. Placing system attacks first in this sequence enables the PLA to gain an advantage in the early stages of conflict and ultimately achieve greater effect against an advanced adversary, with lower risk to its forces or mission.[246]

China's theory of systems attack and its intended sequencing are described in detail in Box 5.

[243] US Joint Staff (2018).

[244] Engstrom (2018); Erickson (2019).

[245] Scouras et al. (2017).

[246] US Joint Staff (2018).

Box 5. China's theory of victory: systems confrontation / systems attack

1. **Create the Conditions for Winning the War:** The first step of systems attack is to disrupt the essential links and nodes that promote system cohesion, in order to create confusion, degrade communications and disorient leadership. PLA literature calls for targeted strikes designed to prevent or disrupt the flow of information within the adversary's operational system.[247] Rather than focusing on attrition, attacks will take place across all domains to degrade the system as a whole.

2. **Fragment the Force:** The second step involves degrading the adversary's data-flows and C2. The PLA emphasises degrading or denying an adversary's use of information in the early stages of conflict, and with greater intensity throughout the conflict. This is envisaged to entail using kinetic and non-kinetic operations to target an adversary's data links, communications, military networks and information systems architecture early in the conflict. Degrading adversary communications thus amplifies the effects of parallel missile and air strikes against C2 nodes, including command centres, flagships and military and civilian leadership.

3. **Blind the Enemy:** The third step entails denying adversary ISR and Early Warning. PLA literature indicates that China will seek to degrade adversary decision-making and awareness by targeting its ISR and early warning capabilities, including key space-based data collection systems, theatre ISR platforms, intelligence centres and satellites.

4. **Own the Initiative:** The fourth step focuses on infiltrating and disrupting the adversary's OODA loop, or 'reconnaissance-control-attack-evaluation' process.[248] This is intended to seize first-mover advantage by initiating conflict when the adversary is not prepared, and to disrupt the time sequence or tempo of the adversary's operational architecture. The PLA will seek to maintain battlefield initiative by forcing adversaries into a reactive cycle, driven by a rapid tempo of unexpected long-range strikes, asymmetric attacks and harassing attacks.

5. **More Return on Investment:** The final step entails the use of precision strikes to achieve 'outsized' effects.[249] This would be achieved through highly targeted precision strikes against key links and nodes to achieve a significant effect on the overall stability and effectiveness of adversary forces. These kinetic precision strikes would be accompanied by non-kinetic attacks against adversary networks, datalinks and information systems, which prevent the adversary from preparing or recovering and thus magnify the effect of kinetic strikes. This concept is also often referred to as 'target-centric warfare', 'key target warfare' or 'trump card and data link-centric warfare'.[250]

Source: RAND Europe analysis.

As highlighted in Box 5, China's theory of systems confrontation is characterised by the use of integrated kinetic and non-kinetic operations across all domains, operating in parallel to amplify effect while degrading the adversary's own communications and information systems, ultimately eroding their will to fight.

[247] Engstrom (2018).

[248] Engstrom (2018).

[249] US Joint Staff (2018).

[250] Burke et al. (2020).

B.2.3. Contemporary Chinese theory and practice for future high-end warfighting shares parallels with Western thinking, but is tailored to China's unique context

The PLA's related concepts of systems confrontation and informatised warfare, and its emphasis on exploiting opportunities in the space, cyber and EM domains to achieve information advantage across the domains, reveal China's pursuit of a superior ability to sense, understand and subsequently orchestrate effects across the operational domains, with information and communications as the key integrators. Therefore, while Chinese doctrine does not contain any explicit reference to MDI per se, notable parallels can be drawn with the UK and US concepts. China's approach does not necessarily mirror that of the United States; instead, it appears to be developing its own multi-domain concepts that take into account its own military culture and history, and its technical capabilities (and capability gaps). While the space and cyber domains are viewed in a similar manner (in terms of their use for C2 and obtaining information on potential targets), Chinese doctrine arguably places greater emphasis than US doctrine on the role of information, which it views as critical for shaping the strategic environment in its own favour, gaining advantage against a militarily superior adversary in the early stages of conflict, maintaining this advantage thereafter, and ultimately *winning* contemporary wars (as presented in the PLA's 2013 concept of 'Winning Informatised Local Wars').[251]

B.3. What has driven or is driving the development of MDI concepts by the People's Republic of China?

B.3.1. Contemporary Chinese thinking is informed both by internal factors as well as lessons derived from US-led military operations since the First Gulf War

China's modern military doctrine has evolved in line with the expansion of its political ambitions at the regional and international levels.[252] This has resulted in a shift from a purely (active) defensive stance envisaging a total war, to a more offensive stance envisaging limited war in the periphery.[253] China is understood to be starting from the position of a perceived threat from the United States and a recognition of the need to counter this threat and succeed in a potential military confrontation with a more militarily capable aggressor. Taiwan is a particularly significant concern for China; while the PLA outmatches Taiwan in practically every aspect of its military capabilities, China is concerned by the presence of US military assets in the region, including the possibility of the United States intervening in any conflict with Taiwan. Other potential flashpoints include contested islands in the South and East China seas. Much of China's modernisation and its underpinning concepts have thus been aimed at preparing for a potential military confrontation with the United States.[254] As described above, 'systems thinking' is central to China's approach to defeating an advanced adversary. There are also important inheritances from historical and

[251] Internal interview with RAND expert, 1 June 2020; Burke et al. (2020).

[252] Ilhan (2020).

[253] Ilhan (2020).

[254] IHS Jane's (2020a).

modern Chinese theorists (e.g. Sun Tzu, the Confucian tradition, or the revolutionary-era writings of Mao Zedong and others).

Contemporary Chinese thinking of MDI is also influenced by its perception of the expansion of the physical and non-physical domains of war (the *war space*) from multi-dimensional to full-dimensional, incorporating the cyber and space domains. As a PLA major general has noted, 'conventional time-space constraints on military operations [are] dwindling' and 'operations relying on specific battlefield space and specific branch of the military at a specific time will be replaced with integrated joint operations taking place over a broad range of space and time with highly integrated forces'.[255]

At the same time, much of China's contemporary thinking on the future of multi-domain concepts appears to be drawn directly from lessons learned from Western experiences, developing its own concepts in response based on its own military culture, geostrategic position and technical capabilities.[256] China's realisation of systems thinking and informatisation has been reached after observing two decades of US post-Cold War operations and the revolutionary impact of information systems in these contexts.[257] With the PLA not having conducted a large-scale ground offensive since its lacklustre showing in the Sino-Vietnamese War of 1979,[258, 259] and having never fought a major maritime engagement or aerial campaign,[260] China has instead relied heavily on drawing 'lessons from other people's wars', principally those of the United States.[261] At the end of the 20th Century, China observed and absorbed lessons from the First Gulf War, which in its view demonstrated the emergence of 'networked' precision strike capabilities and warfare under informatised conditions.[262] This, along with the subsequent US bombing of the Chinese embassy in Belgrade (1999) and the PLA's perceived powerlessness during the third Taiwan Straits crisis

[255] Burke et al. (2020).

[256] Internal interview with RAND expert, 1 June 2020.

[257] Engstrom (2018).

[258] Heavy losses sustained when using crude human-wave tactics, with little in the way of air or naval support, against less numerous but better equipped, organised and experienced Vietnamese forces led China to recognise the severe difficulties that a PLA geared towards guerrilla warfare and internal suppression would have against a competent opponent. Chinese President Deng Xiaoping subsequently abandoned the Mao-era 'people's war' to place greater emphasis on technology and professionalisation of the PLA as part of 'people's war under modern conditions'. This involved a new doctrine of limited local war and reforms to create a smaller, more professional and well-equipped PLA as one of the priority areas within Deng's wider 'Four Modernisations', with broader economic reforms fuelling increased investment.

[259] Although the PLA has not been engaged in a major conflict since 1979, China has continued to acquire limited operational experience through increased engagement in peacekeeping operations since the turn of the century.

[260] Western commentators often emphasise the PLA's lack of experience in modern warfare as a weakness in Chinese military modernisation efforts. Chinese authorities have also acknowledged the potential negative impact of the lack of real combat experience on their combat power, referring to a 'peace disease'. However, it should be noted that some factions of the PLA do not think that the lack of real combat experience undermines their potential military advantage and combat power. For them, combat experience is not the only determining factor of military advantage. Moreover, the value of recent combat experience may not carry over to future conflicts due to the changing character of war. See: Goldstein (2021).

[261] Scobell et al. (2011).

[262] Johnson, J. (2018); Burke et al. (2020).

(1995–1996) and Hainan incident (2001), not only alarmed the Chinese leadership, but also prompted a fundamental upheaval in thinking on the strategic and tactical roles of information in warfare.[263]

B.3.2. Geostrategic considerations and China's growing political ambitions have also given impetus to an increasing focus by the PLA on more offensive operations

From the First Gulf War, China deduced that the effective integration of information and weapons systems by networked joint forces could grant overwhelming military superiority.[264] To this end, the PLA recognised the need to adopt operational concepts that are now referred to as 'network-centric warfare', including the operational use of space-based C4ISR and precision-guided munitions (PGMs). First under Jiang Zemin, and then through sustained investment under Hu Jintao, China embraced the concept of a 'revolution in military affairs with Chinese characteristics' to try and develop its own equivalent capabilities, both to emulate the United States' role globally as well as to counter and deny US operations in China's near-abroad.[265]

At the same time, the PLA assessed that the US military's use of these technologies created fundamental dependencies, especially on vulnerable space infrastructure, that could be exploited in wartime like 'an electronic Maginot Line'.[266] The theorists of 'unrestricted warfare' also predicted that the US military's preoccupation with reinforcing its conventional dominance by further perfecting network-centric warfare might blind it to its vulnerabilities against adversaries employing more unconventional ways and means (as borne out by the swift defeat of the Iraqi military in 2003 and the subsequent quagmire of insurgency).[267]

China also recognises the challenges and opportunities offered by its geography and its large population, encouraging an approach that seeks to push hostile US forces back beyond the first, second and third island chains to prevent them bringing networked sensors or effectors – the same weapons used to such effect against Iraq in 1991 and with further refinement in 2003 – to bear while the PLA secured objectives closer to the Chinese mainland.

This line of thinking ultimately paved the way for China's systems confrontation strategy, which seeks to apply asymmetric information countermeasures against critical nodes in space, cyberspace and the EM domains.[268] The capability and force structure requirements of system confrontation are actively driving PLA reform, acquisitions, training and doctrine that are preparing China for integrated operations in informatised conflicts against an advanced adversary.[269] The PLA has thus been evolving its doctrine to align with its greater levels of technical modernisation and military capability, in order to shift away from what

[263] Costello & McReynolds (2018).

[264] Cozad (2016).

[265] Kilcullen (2020, 195).

[266] Qiao & Wang (1999).

[267] Qiao & Wang (1999).

[268] Costello & McReynolds (2018).

[269] US Joint Staff (2018).

has historically been a defensive stance. This shift has been driven by the perceived need to undertake offensive operations against a capable adversary and achieve first-mover advantage. [270]

B.4. How do China's concepts of MDI manifest in practice?

B.4.1. Modernisation of the PLA remains an incomplete and ongoing effort, but there is evidence of progress in operationalising China's own multi-domain concepts

The PLA remains a large but comparatively poorly equipped force by NATO standards, with a mix of capable modern platforms and much older, obsolescent systems. However, significant investment and a series of reform initiatives continue to enhance the professionalism of the PLA and replace its outdated equipment with the latest technologies. In parallel, a combination of foreign technology transfer (whether legal or through espionage and cyber theft of intellectual property) and domestic innovation are increasing the capacity of the Chinese defence industrial base to support the PLA's capability requirements in the context of informatised warfare.[271]

Reflecting China's long-term view on history and national strategy, there is a recognition from both the PLA and Chinese political leadership that completing this modernisation effort will take time. At the 19th Party Congress in 2017, President Xi Jinping set out a vision for the PLA having 'basically completed' its modernisation by 2035 and attaining the status of 'world-class forces' by 2050. Though vaguely defined, these goals can be understood as an ambitious roadmap for achieving parity with, if not leapfrogging, the US military by mid-century. Priorities include increasing the PLA's 'ability to conduct joint operations, improving China's power projection capabilities from a regional to a global level, and professionalising the PLA through strengthened oversight and discipline'.[272]

The evolution of systems thinking also heavily influences the PLA's current organising, equipping and training of its forces for future war-fighting contingencies; this is underpinned by significant emphasis on integration and informatisation across the military domains and services.[273] While China has set out some longer term concepts and stated ambitions, the degree to which this has been worked into practice remains, in places, unclear (at least from unclassified sources). However, the PLA's recent military reorganisation, capability development efforts and military exercises indicate that China is starting to become more coherent in its approach to, and operationalisation of, multi-domain concepts.

Force structure

China's evolving understanding of domains, and its approach to domain integration, is clearly evidenced through the military reform and restructuring pursued by the PLA in recent years. These reforms have been designed to enhance the PLA's ability to engage in integrated operations between theatres, arms, services and across the military domains.[274] On 1 February 2016, the PLA underwent a major restructuring to

[270] IHS Jane's (2020a).

[271] DIA (2019a).

[272] Grossman (2019).

[273] Engstrom (2018).

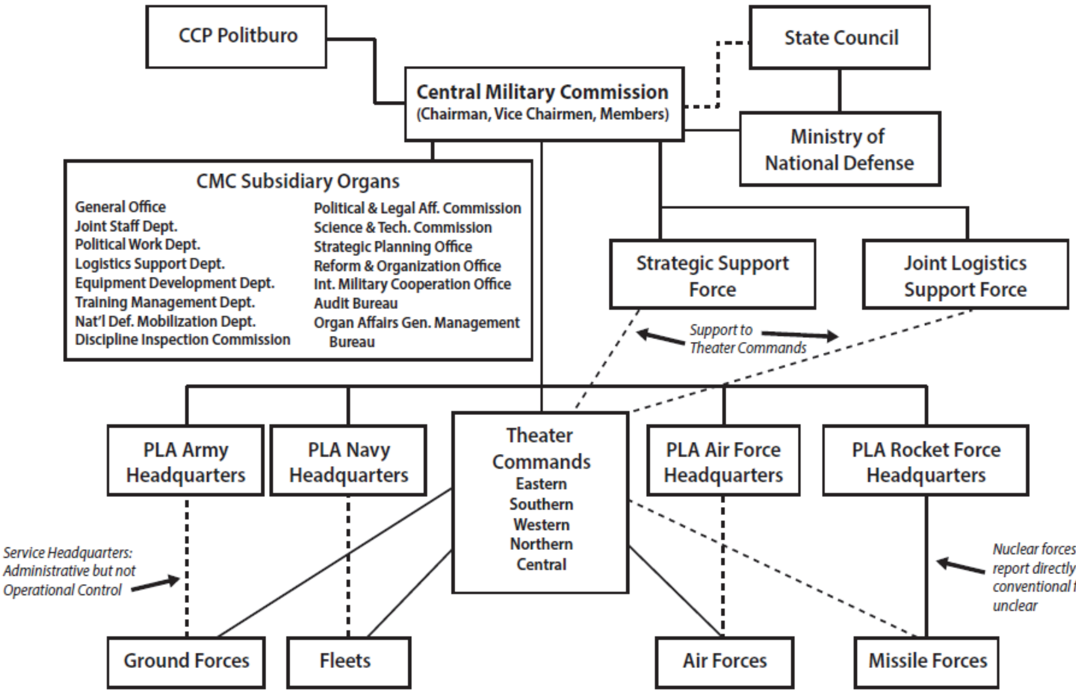
[274] Cozad (2016); Kania & Costello (2018); DIA (2019a).

enhance its ability to prepare and conduct joint operations across multiple domains, as well as tackle corruption, improve discipline, and enhance 'civil-military integration' with defence industry and research institutes[275, 276]:

- Four semi-autonomous general departments were disbanded and replaced by 15 rationalised new bodies within the Central Military Commission (CMC).
- Separate national and theatre-level ground-force headquarters were established for the first time, recognising that the general departments serving as PLA army headquarters and the seven military regions (MRs) had previously been overly focused on the ground force rather than joint operations.
- The seven MRs were replaced with five theatre commands (TCs – eastern, southern, western, central and northern) to lead joint and multi-domain operations in their respective regions.
- The dominance of the ground force within the PLA's structures was rebalanced and the responsibilities of service headquarters (for the PLA Army, PLA Navy, PLA Air Force and PLA Rocket Force, etc.) revised so that these would focus on organising, training and equipping forces, while the TCs focus on preparing and planning for joint combat operations.
- A new Strategic Support Force (SSF) focused on the information domain – including space, cyber and the EM spectrum – was established, along with a new Joint Logistics Support Force (JLSF).

The PLA's new structure after these reforms is outlined below in Figure 5.

Figure 5. PLA organisational structure after reforms to enhance readiness for informatised warfare


CCP Politburo
State Council
Central Military Commission
(Chairman, Vice Chairmen, Members)
Ministry of National Defense
CMC Subsidiary Organs
General Office
Joint Staff Dept.
Political Work Dept.
Logistics Support Dept.
Equipment Development Dept.
Training Management Dept.
Nat'l Def. Mobilization Dept.
Discipline Inspection Commission
Political & Legal Aff. Commission
Science & Tech. Commission
Strategic Planning Office
Reform & Organization Office
Int. Military Cooperation Office
Audit Bureau
Organ Affairs Gen. Management Bureau
Strategic Support Force
Joint Logistics Support Force
Support to Theater Commands
PLA Army Headquarters
PLA Navy Headquarters
Theater Commands
Eastern
Southern
Western
Northern
Central
PLA Air Force Headquarters
PLA Rocket Force Headquarters
Service Headquarters: Administrative but not Operational Control
Nuclear forces still report directly to CMC; conventional forces unclear
Ground Forces
Fleets
Air Forces
Missile Forces

Source: Wuthnow & Saunders (2017).

[275] Until the late 1980s, the PLA was historically and culturally an army-dominated institution. The air force (PLAAF) and Navy (PLAN) played limited supporting roles in the PLA's operations, including major conflicts (Ilhan 2020).

[276] Wuthnow & Saunders (2017).

This reorganisation is designed to move the PLA away from an army-centric force towards a joint command in which the military services are equally represented and integrated though digital and satellite-enabled C3I connectivity. This is reflected also in moves towards an integrated joint fires system, and backed by a joint acquisition enterprise to develop new capabilities and procure the necessary equipment.[277] Beyond the focus on combat forces, the establishment of the JLSF has consolidated logistics support under a joint function to support joint operations, common sustainment functions across the five services, and PLA operations overseas.[278] The prioritisation of interoperability among the PLA's capabilities is further evidenced by the establishment of a Joint Operations Command Centre under the CMC, which has a subordinate centre within each of the TCs.[279]

December 2015 marked the creation of the PLA's Strategic Support Force, several months prior to the wider PLA structuring.[280] The SSF was designed to enable the PLA to achieve dominance in the critical 'strategic commanding heights' of space, cyberspace, and the electromagnetic domain.[281] The SSF has also assimilated elements of the PLA's psychological and political warfare missions, as a result of a reorganisation of political warfare forces across the PLA. This may foretell a more operational role for Chinese psychological operations in the future.[282] The PLA's decision to build the SSF as a separate service rather than a joint force construct (such as US Strategic Command) was presumably driven by lessons learned from foreign militaries, and is designed to avoid redundancies in force development and counterproductive competition for funding and resources.[283] Rather than building the SSF from scratch, the PLA employed a modular approach to its formation by reorganising and subordinating existing organisations and their constituent parts, and redefining their command relationships, to reflect new conceptual paradigms.[284]

The operational aspects of China's informatisation unit were previously invested in the Information Assurance Base. This was responsible for information assurance and strategic information support, as well as playing a central role in the management of the PLA's Integrated Command Platform, which provides multiservice communications for joint operations.[285] Under the PLA restructuring, the functions of the Information Assurance Base were largely reallocated to the SSF. It is also thought that other specialised units, such as those concerned with EM spectrum management and computer network defence, may also have been transferred in order to integrate and support operations in the cyber and electromagnetic domains.[286]

[277] Sukman & Davis (2020).

[278] DIA (2019a).

[279] IHS Jane's (2020a).

[280] Pollpeter et al. (2017).

[281] Kania & Costello (2018).

[282] Costello & McReynolds (2018).

[283] Costello & McReynolds (2018).

[284] Costello & McReynolds (2018).

[285] DIA (2019a).

[286] Kania & Costello (2017).

The SSF is understood to have two primary roles[287]:

- **Strategic information support** entails centralising the collection and management of technical intelligence; providing strategic intelligence support to TCs; enabling PLA power projection and remote operations; and supporting strategic defence in the space and nuclear domains. The SSF's Space Systems Department (SSD) appears to have fused and centralised control over the majority of the PLA's space-based and space-related assets. Through these capabilities, the SSF has taken responsibility for strategic-level information support across the entire PLA, enhancing its ability to engage in integrated joint operations and remote operations. [288]
- **Strategic information operations** entail integrating multiple disciplines of information warfare into a unified force. This includes integrating cyber espionage and offence; consolidating information warfare campaign planning and force development; and unifying responsibilities for the C2 of information operations. Under its Network Systems Department, the SSF has also integrated the PLA's cyber, electronic and psychological warfare capabilities into a single force, potentially enabling it to exploit key synergies among operations in these domains. More broadly, the SSF coordinates the employment of space, cyber and EW to 'paralyse the enemy's operational system of systems' and 'sabotage the enemy's war command system of systems' in the initial stages of conflict.[289]

In this regard, the creation of the SSF represents a reconfiguration of force structure designed to integrate and operationalise the informatised and systems-of-systems concepts outlined in Section B.1. The establishment of the SSF reflects the PLA's recognition that establishing a domain-centric force for information warfare facilitates a level of unified planning, force development and integrated operations that would have been infeasible under the previous structure, in which information functions were siloed within the separate services.[290] This is a notable contrast with the restructuring of the PLA's conventional armed services toward force development and away from operations, which have been tasked to the TCs. This difference in approach between the services is cited as due to the unique requirements and tempo of the information domain, where the vulnerabilities and exploits necessary to deliver effect are identified, refined and deployed in a rapid, continuous loop throughout both peacetime and wartime.[291] However, the consolidation of information operations under the SSF could impede the development of space, cyber and EW capabilities necessary for tactical warfighting needs; it is unclear how the SSF will address conflicting or overlapping responsibilities between its space and cyber forces. Deficiencies in integration may impede the SSF's ability to integrate its in-house space and cyber missions as well as its coordination with the TCs.[292]

Beyond the establishment of the SSF, the PLA is also understood to be developing network-electronic capabilities within its national Joint Staff Department headquarters, as well as within new regional TCs. This indicates the emergence of a multi-level force structure configured for information operations and

[287] Costello & McReynolds (2018).

[288] Kania & Costello (2018).

[289] Kania & Costello (2018).

[290] Costello & McReynolds (2018).

[291] Costello & McReynolds (2018).

[292] Costello & McReynolds (2018).

designed to achieve military and non-military effect through and across the domains.[293] These developments reflect the PLA's increasingly integrated approach to force structure and operations in the new critical space, cyber, electronic and cognitive domains. The operationalisation of this paradigm could enhance its ability to engage and succeed in the future 'informatised' wars the PLA anticipates.[294]

In July 2017, the PLA underwent a second set of structural reforms aimed at further enhancing its capabilities to conduct joint operations and wage informatised local wars. One particular area of focus of this second set of reforms was the reorganisation of the Chinese Academy of Military Science (AMS), which was tasked with producing doctrines and drafting defence white papers under the leadership of the CMC. The reorganisation of the AMS sought to merge six institutes with a focus on science and technology (S&T) that had previously been subordinate to the PLA's former general departments – including the System Engineering Institute and the National Defence S&T Innovation Institute – with other military political and war institutes, to embed high-tech at the heart of doctrinal work in order to operationalise the informatised concepts and accelerate the PLA's modernisation. A second area of focus for the second set of reforms was the consolidation of the War Research Institute, and creation within it of a new Joint Operations Lab to develop 'new models of simulating joint campaigns in computer-assisted wargames'.[295]

Certainly, some elements of PLA writings on systems attack remain aspirational; however the doctrine shows that the PLA is thinking seriously and realistically about how to defeat an advanced adversary.[296] While implementing the PLA's joint force objectives has so far been regarded as a slow process, it is likely to have accelerated with the creation of TCs in 2016. Evidence that enhancing joint operations in and across all domains is a genuine strategic priority for China is provided in the political and military leadership's willingness to implement sweeping changes to the PLA's structures and to invest heavily in other reforms to realise goals for a modernised force by 2035, and a world-class one by 2050.

Capabilities and acquisition

China's recent and ongoing procurement efforts similarly reflect a sustained and growing emphasis on the pursuit of informatisation, which requires the incorporation of information systems throughout the PLA. Recent procurement efforts have therefore centred on automatic command systems, strategic and tactical sensors, precision munitions and computer network attack capabilities.[297]

Procurement efforts for the ground forces have focused on transforming the service from a motorised to a mechanised force and significantly increasing its transport capabilities, as well as improving armoured, air defence, aviation, ground-air co-ordination, and cyber-attack and EW capabilities.[298] China is now understood to possess sophisticated capabilities including precision-strike systems, fourth- and fifth-generation fighters, and multiple short-range ballistic missile systems. The PLA has also fielded an

[293] IHS Jane's (2020a).

[294] Kania & Costello (2018).

[295] Wuthnow (2019).

[296] US Joint Staff (2018).

[297] IHS Jane's (2020a).

[298] IHS Jane's (2020a & 2020b).

assortment of anti-access systems across the domains including ASAT systems, anti-ship ballistic missiles (ASBMs), submarines, cruise missiles and mine-warfare forces intended to impede the operation of perceived adversaries around its periphery.[299] China remains focused on implementing new information technologies to upgrade older equipment, while disseminating new digital and satellite C3I connectivity throughout the military services.[300]

China also continues to invest in emerging and disruptive technologies, for example deploying hypersonic missiles such as the DZ-FZ (designated the WU-14 by the United States) and investing in directed energy systems. This reflects the wider emphasis placed by the PLA on developing highly secretive and transformative 'Assassin's Mace' capabilities that could potentially remain hidden until deployed to decisive advantage in a future conflict, similar to the US black programme to develop stealth in the 1970s and 1980s. PLA strategists similarly view the ability to utilise space-based assets and deny adversaries access to space as a critical enabler of informatised warfare, recognising also the United States' vulnerable dependencies in this domain.[301] Drawing on recent Western military engagements, PLA analysis of US and coalition military operations emphasised the importance of space-based operations for enabling informatised warfare.[302] Accordingly, the PLA is also acquiring a range of space and counter-space technologies.

China's recent and ongoing procurement efforts also reflect an increasing emphasis on military-civil fusion in Beijing's approach to MDI and warfare more broadly.[303] Whilst tighter linkages between civilian and military commercial and technology entities were already advocated as early as the 1980s under Deng Xiaoping (known at the time as 'military-civil integration'), it was not until recent years that efforts accelerated, were remodelled (with 'military-civil integration' becoming 'military-civil fusion') and became a national priority. The focus of Chinese MCF efforts in acquisition are in the areas of biology, big data, drones, robotics, launch vehicles, smallsats, space, cyberspace and maritime development.[304]

In pursuit of a more integrated and modernised force, China's recent modernisation efforts have required trade-offs in other areas; in particular, the PLA has made significant reductions in its personnel numbers to sustain and mitigate the financial impact of its modernisation process (even as China's economy continues to far outstrip GDP growth in Western nations). It is expected that China's modernisation requirements will require significant and continuous investment over the next decade, requiring reductions in personnel numbers and reallocation of resources towards more sophisticated, integrated technological capability and informatisation.[305] In addition, China is thought to pursue certain military technologies that can also benefit its civilian high-tech infrastructure,[306] in order to maximise its return on investment and benefit both its

[299] IHS Jane's (2020b).

[300] IHS Jane's (2020a).

[301] Cordesman et al. (2013).

[302] IHS Jane's (2020a).

[303] Ashby et al. (2021).

[304] Kania and Laskai (2021).

[305] IHS Jane's (2020a).

[306] Office of the Secretary of Defense (2019).

military and national economy, for example through enhanced 'civil-military integration' on research and development (R&D).[307]

Military exercises and operations

To accompany the PLA's modernisation efforts as well as the restructuring outlined above, the PLA has also implemented a range of personnel, education and training reforms, and recent exercises across the military services indicate a focus on greater connectivity and integration between services and across the domains.[308] The PLA has placed significant focus on improving joint forces interoperability, notably by deepening the Triad military education and training reform concept,[309] revising the professional military education system and providing more instruction on joint operations at the National Defence University (NDU) and the National University of Defence Technology (NUDT).[310] It also published an 'Outline of Training and Evaluation' in 2018 that emphasised the need for realistic joint training across all warfare domains against 'strong military opponents'.[311] Numerous military exercises demonstrate that this is an area where China has made significant strides.[312] For example:

- The SSF has actively sought to integrate into the joint operations systems by carrying out confrontational training in new domains.
- The Rocket Force has strengthened training for joint strikes, organised force-on-force evaluation-oriented training and training based on operational plans at brigade and regiment levels, and completed regular exercises, such as Heavenly Sword.
- The Air Force has held a series of regular system-versus-system exercises such as Red Sword.
- The newly established JLSF has aligned itself with the joint operations systems and conducted exercises such as Joint Logistics Mission 2018.[313]

As discussed in Section B.3, China developed its systems confrontation doctrine in large part by observing how the United States fights. China therefore expects that the United States will attempt to degrade the PLA's ability to operate as a coherent force and is training and equipping its forces to operate independently, autonomously and resiliently, with a considerable emphasis on operating in a complex electromagnetic environment.[314]

[307] Boyd et al. (2010).

[308] IHS Jane's (2020b).

[309] The 'Triad New Military Talent Education System of Systems', also known as Triad system, is composed of three components: institutional education, unit training and military professional education. Improvements to the Triad system mentioned in the 2015 China Defence White Paper seek to 'pool more talented people and cultivate more personnel who can meet the demands of informatised warfare', by fusing the three components of the Triad. See: The State Council Information Office of the People's Republic of China (2015).

[310] McCauley (2019); Wuthnow (2019).

[311] Office of the Secretary of Defense (2019).

[312] Cozad (2016).

[313] Erickson (2019).

[314] Gibson (2019).

B.5. What does the literature suggest about future developments and approaches to MDI by China (e.g. out to 2025, 2030, 2040)?

B.5.1. China's concept of systems attack is not yet fully reconciled with its current capabilities, but it is investing heavily to make its theory of victory a reality

The possible sequence of operations enabled by potential Chinese systems attacks would entail: achieving air superiority; using air superiority to seize maritime superiority and enable ground operations; then using maritime superiority to execute attacks from the sea to the land. While China's existing capabilities may enable it to execute the first part of this sequence, the latter part remains, for the moment, aspirational if confronting a determined US military. China does not currently possess ship-launched land attack cruise missiles, and its emerging aircraft carrier programme is not capable of conducting strike warfare. However, these sequences represent how the PLA explicitly wants to be able to conduct warfare, and its ongoing acquisitions and training reflect this ambition.

It is unclear when the PLA expects to achieve its desired level of dominance, or the 'ability to win informationised wars'. Some PLA sources expect that this may be achieved in the 2020s, but other sources indicate that this will not be feasible until President Xi's 2050 marker.[315] The establishment of the SSF is intended to optimise the PLA for future warfare, in which the PLA anticipates that the domains of space, cyberspace and the EM spectrum, along with the cognitive domain, will be crucial to victory.[316] In this regard, China's integrated, informatised multi-domain doctrine is reflected in its current acquisitions, capability development and training patterns, but in future it may be demonstrated in its operations.[317]

[315] IHS Jane's (2020a).

[316] Kania & Costello (2018).

[317] Gibson (2019).