Cyber Threats to NATO from a Multi-Domain Perspective

James Black
Research Leader
Defence, Security and Infrastructure
RAND Europe

Alice Lynch[1]
Former Security and Defence Analyst
RAND Europe

Abstract: This paper situates cyber threats within the wider context of a continued shift towards multi-domain concepts by NATO Allies and adversaries alike. These emerging concepts emphasise the importance of integration for achieving advantage; however, with greater connectivity and network-dependency comes greater potential vulnerability and consequences from disruption. This paper considers challenges associated with closer integration within and across military domains and examines how potential adversaries (Russia and China) are embracing variations on multi-domain and systems thinking and prioritising offensive cyber capabilities to exploit seams and vulnerabilities to disorientate, paralyse and demoralise NATO in any future conflict. Acknowledging that cyber attacks do not exist in a vacuum, this paper places discussions of cyber threats in the context of how the Alliance plans to operate, fight and win in future competition and conflict. In doing so, it highlights the adversary's perspective on how, when and why it might employ cyber capabilities to gain an advantage over NATO forces. The paper then considers the implications for NATO in terms of internal barriers, limitations and vulnerabilities that challenge the Alliance's ability to respond to these threats. Improved understanding of the interlinkages between these external threats and internal vulnerabilities is essential in achieving the genuine and wide-reaching transformation required for the Alliance to bolster its cohesion, improve its strategic resilience and ensure its ability to realise its ambitions in cyberspace and across all domains.

Keywords: *Cyber, multi-domain, cross-domain, concepts, Russia, China*

[1] Disclaimer: Alice Lynch has contributed to this paper in a personal capacity, and the analysis and views expressed therein do not necessarily reflect those of her current employer.

1. INTRODUCTION

Fully understanding future cyber threats to the North Atlantic Treaty Organisation (NATO) necessitates looking beyond trends in cyberspace and considering how these both shape and are shaped by threats in or across other operational domains. NATO, the US and other Allies are increasingly developing concepts, forces and capabilities that go beyond the traditional focus on 'joint' to embrace ambitious visions for future multi-domain operations (MDO). Adversaries are similarly developing and employing cyber capabilities against the Alliance not as part of some segregated cyberwar, but rather as critical integrators and enablers of their own variations on MDO and systems thinking.

This paper situates cyber threats in the wider context of this evolving MDO theory and practice. First, it introduces the logic and focus of emerging US and NATO concepts for multi-domain and how cyberspace fits within them. Second, it examines cyberspace's evolving role in the multi-domain thinking of Russia, China and, to a lesser extent, Iran and the Democratic People's Republic of Korea (DPRK), recognising that NATO can only truly mitigate threats if it understands potential adversaries in terms of both capability and intent. Lieutenant General Thomas J. Sharpy of Allied Command Transformation (ACT) warns that NATO otherwise risks MDO being the 'Sputnik moment of this generation', as adversaries increasingly combine cyber, space, electronic and information warfare capabilities to exploit seams in Alliance decision-making and joint operations (Sharpy, 2020). Third, this paper considers the internal challenges and vulnerabilities NATO faces in adapting to future cyber and multi-domain operations.

Collectively, the sections of this paper underscore the need for genuine and wide-reaching transformation if the Alliance is to bolster its cohesion, improve its strategic resilience and ensure its ability to compete in cyberspace and across all domains.

2. CYBER AS AN OPERATIONAL DOMAIN

NATO's contemporary strategic environment is characterised by continuous global competition, both above and below the threshold of armed conflict. Potential adversaries are closing the gap; NATO's competitive edge has been eroded in every military domain, across air, land, sea, space and cyberspace (Knighton, 2019). Rapid technological developments exploiting cyberspace and the electromagnetic spectrum (EMS) present the Alliance with new challenges as threats from increasingly sophisticated adversaries become more complex, destructive and unpredictable (Brent, 2019). Accordingly, the Allies have sought to operationalise cyberspace. At the 2016 Warsaw Summit, they formally recognised cyber as an operational domain, alongside air, land, maritime and, since 2019, space (NATO, 2020a; NATO, 2020b).[2] This was followed in 2018 by establishment of a Cyberspace Operations Centre (CyOC) as a new NATO theatre component command, with plans to reach full operating capability by 2023 (Brzozowksi, 2018; Brent, 2019). At the 2018 Brussels Summit, Allies issued a joint declaration that 'we must be able to operate as effectively in cyberspace as we do in the air, on land, and at sea to strengthen and support the Alliance's overall deterrence and defence posture' (NATO, 2018a).

Efforts to operationalise the cyber domain include recently published doctrine. *AJP-3.20 Allied Joint Publication Doctrine of Cyberspace Operations* sets out the principles by which joint cyber operations may be planned, executed and assessed (NATO, 2020c). This reflects a shift away from understanding cyber as an enabler of operations in other domains towards being a domain in its own right through which deterrence and coercion can be practised and decisive kinetic and non-kinetic effects delivered (Shea, 2018).[3] However, cyberspace does not exist in a vacuum. Viewing it as a solitary fifth domain risks underestimating the full implications of cyber threats' convergence with those emerging from other domains, thereby undermining the ability to deter and defend against adversaries exploiting seams and vulnerabilities within the increasingly interconnected systems, infrastructure and processes of NATO and individual Allies.

A. Situating the Cyber Domain within Multi-Domain Thinking

Technology is facilitating unprecedented integration across and between domains as military platforms and systems increasingly form part of a complex, networked ecosystem or system-of-systems' (NATO, 2018b).[4] Cyber-related developments are therefore increasingly understood in the context of interlinkages and 'convergence'[5] across domain boundaries, most prominently within emerging US concepts of MDO (TRADOC, 2018).

Much of today's multi-domain thinking can be traced back to concepts of AirLand Battle developed by the US Army in the 1970s and 1980s. AirLand Battle sought to deepen the coordination of manoeuvring land forces and airpower, leveraging satellite technology, theatre battle networks and precision-guided munitions to counter the Warsaw Pact's numerical superiority in the European theatre (Manea, 2018). Central to AirLand Battle were the

[2] Though NATO now formally recognises five operating domains, notably there is no commonly agreed upon definition of 'domain' within the Alliance. See: Donnelly & Farley, 2019.

[3] NATO does not intend to develop its own offensive cyber capabilities; however, individual Allies have agreed to integrate national capabilities into NATO missions. See: Tucker, 2019.

[4] Systems-of-systems are a 'set or arrangement of systems that results when independent…systems are integrated into a larger system that delivers unique capabilities.' See: DAU, 2020.

[5] Convergence can be defined as 'the integration of capabilities across domains, environments, and functions in time and physical space to achieve a purpose'. See: TRADOC, 2017.

concepts of ‘Integrated Battle’ and the ‘Extended Battlefield’. Integrated Battle stipulated that every asset of the air-ground team at a commander’s disposal should be employed together to defeat the opponent. Extended Battlefield involved attacking all echelons of the opponent’s formations simultaneously (Johnson 2018). AirLand Battle remained primarily focused on the air and land domains. ‘Cyberspace’ was not yet understood as a domain in its own right, although strong emphasis was placed on computer networks as an enabler and force multiplier for joint operations. Many of AirLand Battle’s core principles endured and evolved to guide the development of ‘network-centric warfare’ in the 1990s and 2000s, influencing current NATO doctrine on joint operations and, more recently, shaping the multi-domain thinking now so prominent in the US and increasingly among NATO Allies.

While MDO originates from US Army thinking, others have begun developing their own variations, including: the US Air Force’s Multi-Domain Command and Control; recent US joint terminology of Joint All-Domain Operations; Norway’s Holistic Operations; and the UK’s Multi-Domain Integration (Watling & Roper, 2019; Carter, 2019; Underwood, 2020). While these all refer to similar fundamental principles, NATO has no unifying definition of MDO and differences persist even between US service branches (Grest & Heren, 2019). This paper assumes a generic use of the term MDO to encompass these various still-evolving concepts and its use does not specifically endorse those of any single service or nation.

MDO is premised on the notion that deeper integration within and across domains will enable NATO to overcome adversary strategies and capabilities aimed at preventing access to theatres of operations and limiting freedom of manoeuvre, often referred to in the West—though not, notably, in Russian or Chinese literature —as Anti-Access/Area-Denial (A2/AD). Given technological developments and growing independencies across domains, previous concepts of ‘jointness’ are no longer seen as sufficient to address such threats or to reflect the importance of new cyber and space capabilities (Siegemund, 2018).

The primary purpose of MDO, therefore, is to prepare for future integrated operations across the full spectrum of conflict by removing the institutional segregation of military capabilities and elevating the role of service branches and domains typically thought of as support (Freedberg, 2018). In contrast with joint warfare which remains premised on separate domains in which operations are principally led by one service and where capabilities in one domain are used to support those in another, MDO presents a more ambitious vision genuinely agnostic of domain boundaries or traditional force structures (Perkins & Andera, 2018). Harnessing synergies across cyberspace, space and the EMS, MDO enables commanders to orchestrate and converge effects at the optimal tempo in windows of opportunity, thus ‘[presenting] the enemy with multiple dilemmas across multiple domains and in multiple locations’ (Feickert, 2020: p. 2). This emphasises integration as key to gaining an advantage in future conflicts in which adversaries contest

NATO in all domains with the convergence of networked sensors and effectors in different domains producing an overall effect greater than the sum of its parts (Lindsay & Gartzke, 2020; Siegmund, 2018).

B. Emerging Multi-Domain Concepts within NATO

While high-level principles of US MDO are maturing, the specifics of how to operationalise them remain a work-in-progress (Clare, 2020). Nonetheless, several other Allies have begun exploring similar concepts. The Tri-lateral Strategic Steering Group comprising the US, UK and France has investigated Multi-Domain Warfare (MDW) based on shared recognition that future adversaries will combine conventional, asymmetric and hybrid capabilities and tactics across all domains (Perkins & Olivieri, 2018). The UK's own Multi-Domain Integration (MDI) concept adopts a similar rationale to that of the US, aiming to 'achieve the seamless planning and execution of activities and effects across all domains at a pace and tempo that outstrips our adversaries' (Barry, 2020) to gain information advantage; key priorities being to extend joint operations into cyberspace and exploit data and networks more effectively.

NATO is also beginning to consider implications for implementing MDO at the Alliance level, especially around interoperability and command and control (C2). For example, the NATO Command and Control Centre of Excellence (NATO C2COE) has made MDO the focus of its annual seminar for 2020 (NATO C2COE, 2020b); while the Joint Air Power Competence Centre is investigating ramifications for C2 and future airpower (Harrigian, 2020). The NATO Science and Technology Organisation (STO) also has projects focused on agile multi-domain C2 and wargaming MDO in an A2/AD environment (NATO STO, 2018; NATO STO, 2020). Multi-domain thinking was also evident in Exercise *Trident Juncture 2018* (TRJE18), which incorporated a robust opposition space force order of battle and cyber capabilities in its scenario development. With experimentation efforts ongoing to develop a new *NATO Warfighting Capstone Concept* (NWCC) looking out to a 20-year horizon, Supreme Allied Commander Europe (SACEUR) has also stipulated that high-intensity, near peer-to-peer, multi-domain scenarios should be the main priorities for future NATO training, exercises and force development (NATO, 2020d; NATO2020e; Wijninga, 2019).

C. Recognising Cyberspace as Both an Opportunity and Risk for MDO

Networks enable collection, communication and consolidation of data across organisations, commands and domains; accordingly, cyberspace enables manoeuvre[6] across all domains (Conti & Raymond, 2017). It extends the reach of operations into the 'strategic support area' and the homeland, while offering alternatives to kinetic effects (TRADOC, 2018; Lindsay & Gartzke, 2020). Cyber operations also create windows of opportunity for action in other domains, providing commanders with a broader range of options

[5] Manoeuvre aims 'to gain positional advantage in respect to the adversary from which force can be threatened or applied [...] manoeuvre is the means by which a commander sets the terms in time and space, declines or joins combat or exploits emerging developments.' See: NATO, 2019b: p. 21).

to exploit adversaries' vulnerabilities as they emerge, rather than being restricted to siloed force constructs and physical sensors and effectors (Nakasone & Lewis, 2017; NATO, 2020c).

While employing cyber capabilities as an integrated part of MDO may enhance NATO's combat effectiveness, it may also create new vulnerabilities. These arise from dependency on connectivity and data within an increasingly complex system-of-systems (Joiner & Tutty, 2018). NATO's adversaries may identify and exploit existing vulnerabilities in military platforms and networks or create new ones through, for example, cyber espionage and the manipulation of technology supply chains and markets (Conti & Fanelli, 2019). These create windows of opportunity for adversaries to undermine NATO's cyber defences or to compromise the cybersecurity of governments, industry and critical national infrastructure, shaping political, strategic and operational outcomes across all domains through hostile action in cyberspace (Schneider, 2019).

Activities in cyberspace and the EMS are therefore key enablers for MDO, but also areas of risk. Effective integration within and across nations, services, commands and domains is impractical without secure and resilient lines of communication; in short, success within a multi-domain environment cannot be achieved without the interconnected networks and secure systems constituting the base of the cyber domain (Shea, 2018; Zadalis, 2018). There is also an increasing overlap between cyber threats and space. As C2 systems increasingly rely on space to gather and disseminate mission-critical data, any cyber, jamming, spoofing or physical attack on satellites or ground stations could have cascading effects across all domains and on strategic weapon systems and early warning (Unal, 2019).

D. Adversary Perspectives

NATO's adversaries have explicitly recognised the vulnerabilities inherent in the Alliance's growing dependence on networks, cyberspace, satellite technologies and the EMS. They now seek to exploit these vulnerabilities through their own variations on multi-domain concepts (Nakasone & Lewis, 2017; Schneider, 2019). NATO Allies are not alone in adopting a multi-domain understanding of the future battlespace. While not explicitly embracing the lexicon of US MDO, adversaries nonetheless express similar themes in their own languages. These emerging concepts are increasingly made manifest through joint operations, investment priorities and force and capability development initiatives. This section examines how selected non-NATO nations, principally Russia and China, are approaching multi-domain thinking in theory and in practice. It also considers how each is integrating the cyber domain into its systems thinking, providing an understanding of how cyber threats to NATO are evolving both in terms of hostile intent and capability.

1) Russian Federation

Cyberspace forms part of Russia's strategy of harnessing multi-domain synergies through its interrelated concepts of 'new-type war', 'reflexive control' and 'disorganisation', which together seek to create strategic conditions for prevailing over the US and NATO. Russian doctrine, activities, force structures and capability development efforts indicate that Moscow is refining and beginning to implement variations on multi-domain thinking. Observing the evolution of network-centric warfare within NATO since AirLand Battle, Russia is seeking to leverage synergies across physical and virtual domains to contest NATO above and below the threshold of armed conflict, creating favourable conditions to seize the advantage in the initial period of war (IPW) (Greisemer, 2018).[7] To achieve this, Russian doctrine emphasises exploiting new technologies and asymmetric means to counter perceived Western advantages, highlighting opportunities arising from cyberspace, alongside the electronic, information and space domains. This asymmetric thinking is expressed through Russia's concept of 'new-type war', which focuses on integration across domains to achieve information superiority and shape strategic conditions through 'reflexive control'.

Reflexive control is the practice of manipulating the adversary's perceptions and decision-making processes through the deliberate construction of information flows to deceive, persuade, coerce and otherwise influence the opponent (Adamsky, 2015). This seeks to exploit NATO's weaknesses with minimal use of kinetic force, achieving maximum effect with minimal use of Russia's resources (Galeotti, 2016). Reflexive control is employed in conjunction with the interrelated concept of 'disorganisation', a strategy of disrupting or degrading an opponent's C2 networks to hinder their ability to coordinate or integrate across multiple domains, thus providing Russia with decision advantage and increased likelihood of victory (Adamsky, 2015).

Cyberspace is viewed as an important enabler, integrator and multiplier. Within 'new-type war', the information domain and exploitation of cyberspace and the EMS are viewed as the means through which Russia can achieve cross-domain synergy and exercise reflexive control creating time, space and manoeuvre advantage for Russian forces while disorganising NATO. For example, during sub-threshold operations or in the IPW, cyber espionage can elicit valuable intelligence on adversary operations in other domains and during operations, targeted cyber attacks can disrupt the adversary's networked C2 systems. At the strategic level, cyber activities support information operations to confuse, influence or mislead target audiences and undermine NATO's cohesion and will-to-fight (Sprang, 2018). Cyberspace thereby provides new methods for disrupting and degrading NATO's networked information and communication systems to achieve Russia's operational and strategic objectives within and across multiple domains (Kilcullen, 2020).

Recent Battalion Tactical Group (BTG) operations in Ukraine provide practical examples of how Russia seeks to exploit cyberspace to operationalise

[7] Russia's IPW concept recognises readiness and will-to-fight as key determinants of conflict outcomes, with early, swift and devastating action potentially decisive. Today, Russian understanding of the IPW emphasises cyber-attacks and broader information operations to degrade the adversary's C2. See: Thomas, 2019.

its own variation on multi-domain concepts (Sprang, 2018). Within Russia's new integrated approach to warfare, BTG commanders are provided with capabilities across domains to achieve a specific operational effect. This includes enablers such as EMS capabilities, previously siloed within what used to be an inflexible force structure (Griesemer, 2018). In multiple confrontations with Ukrainian forces,[8] Russia deployed cyber capabilities in concert with other weapons spanning the domains including uncrewed aerial systems (UAS) and ground forces under a single battalion commander. To achieve a combined effect, Russian forces first disrupted Ukrainian communications and decision-making through targeted cyber-attacks and jamming. With Ukrainian C2 compromised, UAS conducted detailed reconnaissance and target acquisition against Ukrainian positions, enabling devastating long-range rocket and tube artillery strikes (Griesemer, 2018).

Russia has also made tactical use of cyber, electronic and information warfare alongside conventional forces to achieve multi-domain effects in Syria, both targeting pro-democracy, Kurdish and Islamic State fighters and interfering with the US-led coalition's operations in and around Syria (McLeary, 2018). The alleged use of cyber attacks and jamming of GPS signals during TRJE18 are further evidence of Russia's willingness to use offensive cyber and EW capabilities to disrupt NATO operations, with cascading effect across multiple domains (Tigner, 2018). Most recently, military exercises in the Central and Southern Military Districts as part of Kavaz 2020 have provided perhaps the most explicit public acknowledgement of Russia's ambition to implement its own variant on multi-domain concepts. One of 'the key features of the manoeuvres was to use [multi-domain] force groupings to commence and repel a 'global strike' from a simulated adversary' representing the US or NATO and to organise Russia's counter-action as a 'multi-sphere operation' (mnogosfernoy operatsii— seen by observers as "apparently the Russian General Staff's interpretation of the US term, 'multi-domain operations'") (McDermott, 2020).

These conceptual developments and real-world applications illustrate how Russian commanders increasingly use cyber-attacks to create windows of opportunity for success in the early stages of a conflict, while also enabling the execution of offensive tasks in other domains to achieve victory (Sprang, 2018).

2) *People's Republic of China*

China's strategic concepts are also increasingly characterised by joint and multi-domain thinking, the People's Liberation Army (PLA) understanding the future battlespace as an all-domain confrontation between networked, information-dependent systems-of-systems. Acknowledging increasing interdependencies within and between domains, the PLA aims to harness cyber capabilities to exploit seams and vulnerabilities within adversary networks. Chinese doctrine, therefore, centres on concepts of 'informatised warfare' and

[7] Including the battles of Zelenopillya (2014), Ilovaisk (2014), Donetsk Airport (2014-15), and Debal'tseve (2015). See: Sprang, 2018 and Griesemer, 2018.

multi-domain 'systems confrontation' designed to prepare for future conflict with a technologically advanced opponent (Engstrom, 2018; Kilcullen, 2020).

Parallels can be drawn with Western multi-domain thinking. 'Informatised warfare' recognises the growing information-dependency of military operations and seeks to acquire, transmit, process and use information to conduct cross-domain operations and seize tactical opportunities through an enhanced, shared awareness of the battlespace (DIA, 2019). 'Systems confrontation' or 'systems attack', known as China's 'basic operational method' of warfare, aims to defeat militarily superior opponents by exploiting vulnerabilities in their integrated, networked systems. This entails systematically targeting linkages and nodes that hold an advanced network-centric force together as a cohesive whole (US Joint Staff, 2018).

China is therefore seeking to use cyberspace and the EMS to disrupt and fracture the adversary's system-of-systems and achieve information and decision advantage over a paralysed, disoriented and demoralised US or NATO (Engstrom, 2018; Kilcullen, 2020). The PLA understands activities in cyberspace and the EMS as critical integrators and enablers of kinetic operations in physical domains and arenas for influence operations within informatised warfare (OSD, 2019). China's information warfare strategy, known as 'integrated network electronic warfare', entails the integrated use of cyber-attacks, electronic warfare (EW) and targeted kinetic strikes on critical nodes in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks; this must be underpinned by a fully networked digital architecture to integrate PLA joint operations across domains (Scouras, Smyth & Mahnken, 2017).

China's efforts to implement this vision are evidenced through the PLA's recent force restructuring. In December 2015, it formed the Strategic Support Force (SSF), with the stated purpose of improving the PLA's capacity for operating in the cyber, electromagnetic and space domains (Kania & Costello, 2018). One of the SSF's primary roles is strategic information operations—the integration and coordination of cyber-espionage and offence, space and EW within a unified force 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 (Costello & McReynolds, 2018: p. 2). China is similarly investing heavily in artificial intelligence (AI) to enable improved sensor and shooter integration, situational awareness and lethality, and more rapid and automated decision-making exploiting adversaries' OODA loops.[9] It seeks to move beyond 'informatised' to 'intelligentised' warfare in future (Bommakanti, 2020; Kania, 2020). Even in the context of sub-threshold operations, China's offensive cyber capabilities are being used both to compromise military and government networks directly and to target underlying supply chains and critical infrastructure (IISS, 2019).

[9] The OODA (observe-orient-decide-act) loop describes the iterative decision-making process of military commanders. See Zager & Zager, 2017.

Situated in a context of broader PLA restructuring, the SSF's establishment highlights China's efforts to operationalise cyberspace through increasingly integrated force structures capable of conducting operations across domains (Pollpeter et al., 2017; Costello & McReynolds, 2018). PLA modernisation remains an ongoing effort and its capabilities are not yet fully configured to deliver its stated strategy of 'systems attack' in a full-scale conflict (IHS Jane's, 2020). However, ongoing capability development and the recent overhaul of approaches to joint training and exercises indicate China is investing heavily in realising Xi Jinping's stated ambition of the PLA becoming a 'world-beating' all-domain force by 2049 (Cozad, 2016). Therefore, while China's systems-based, multi-domain understanding of cyberspace is currently reflected in doctrine and reform programmes, in the future it may be demonstrated through real-world operations (IHS Jane's, 2020).

3) Other Potential Adversaries

While their concepts and capabilities are less well-developed, smaller nations such as Iran and the DPRK are also investing heavily in cyberspace and exploring the effects on other domains. There is limited evidence of explicit multi-domain thinking within the current doctrine or activities of either country; however, both are seeking to enhance the use of cyber capabilities within their own joint operations. Iran's concepts of 'Retaliatory Deterrence' and 'Mosaic Warfare'[10] increasingly seek to exploit the cyber domain and encourage more deeply integrated joint operations, primarily aimed at deterring US-led intervention. Capitalising on opportunities presented by new technologies, Teheran is investing in cyber forces and capabilities to extend the reach of its deterrence strategy in conjunction with long-range ballistic and cruise missiles (McInnis, 2017; DIA, 2019). The DPRK is also pursuing an apparent shift towards warfighting beyond the traditional domains, viewing cross-domain integration and coordination of effects as a 'force multiplier' (Paul et al., 2018). This includes leveraging cyberspace and the EMS to defeat a militarily superior adversary by targeting vulnerabilities or dependencies within C2 networks to undermine cohesion within or between allied adversaries and erode their will to fight (Paul et al., 2018; Tasic, 2019).

3. Implications for NATO

Ongoing initiatives by Allies and adversaries alike emphasise the need to consider future threats in cyberspace and the EMS not in isolation but rather in terms of convergence with operations and vulnerabilities in other domains. At the Alliance level, these complex interlinkages present both opportunities and challenges for NATO. Novel technologies and concepts associated with cyberspace, space and information operations or activities in the EMS potentially offer new ways and means to understand, influence, deter and ultimately defeat adversaries through MDO. There are, however, considerable gaps between future ambitions and present realities. Addressing known shortfalls in cyber capabilities and MDO at the national level

[10] Not to be confused with the Defense Advanced Research Project Agency's emerging concept of Mosaic Warfare. See: Clark et al., 2020.

represents a significant, long-term and resource-intensive challenge. Integrating and cohering initiatives across an Alliance of 30 nations only increases the complexity of transformation 'exponentially' (Sharpy, 2020).

To address growing external threats posed by adversaries employing cyber-attacks as part of cross-domain manoeuvre, NATO must first understand its internal barriers, limitations and vulnerabilities regarding MDO. Only then can Allies agree a common approach to developing the future concepts, policies and permissions, C2, capabilities and innovation ecosystem required to compete in such a contested operational environment. The following sections address each of these themes in turn.

A. Conceptual Difficulties

NATO's challenges start with language (Heren, 2020; Reilly, 2020). There is no single definition of MDO employed consistently across the US services, let alone NATO (Donnelly & Farley, 2019; Smagh, 2020). According to Jeff Reilly of the US Air Command and Staff College, the ongoing revolution in the technology and threat environment 'mandates a greater investment of intellectual energy in the concept before it will be accepted by the military and defence communities within NATO' (Reilly, 2020: p. 2). This includes wargaming, modelling and simulation and experimentation to socialise, stress-test and refine MDO concepts (Zadalis, 2018).

Though arguably most mature in its thinking, the US is still working to build a common understanding of domains and of MDO, including why it is necessary, how it is novel or different from joint operations, and how to translate it into practice; including through a new Joint Warfighting Concept and related initiatives such as Joint All-Domain Command and Control (JADC2) capabilities (Grispen-Gelens, 2020). NATO remains even earlier in development: explicit MDO terminology such as convergence is largely absent from NATO doctrine, and has only recently begun featuring in national documents among European Allies such as France, Norway and the UK (Watling & Roper, 2019).

Whether 'multi-domain' is an enduring concept or simply the latest 'buzzword' in military thinking also remains to be seen. If the latter, there is a chance that US thinking may shift away from MDO before NATO has even begun to fully mature its own concept (Spirtas, 2018). As with many buzzwords, there is potential for conceptual confusion or for misappropriation of the latest fashionable concept to provide political and intellectual cover for enduring competition among individual service branches for new funding and responsibilities in emerging domains such as cyberspace and space (Grest & Heren, 2019).

NATO is evolving its understanding of multi-domain synergies while doctrine, policies, plans, C2 structures and capabilities for the cyber and space domains remain immature. The Allies approved a high-level Military Vision and Strategy on Cyberspace as a Domain of Operations in June 2018 (NATO, 2020b) and NATO only recently published the first edition of *AJP-*

3.20 Allied Joint Doctrine for Cyberspace Operations covering cyberspace operations in January 2020. Reservations lodged by Allies include US concerns about how NATO defines and understands domains and the information environment (NATO, 2020c). NATO is also busy operationalising the *Military Strategy* adopted in 2019, implementing readiness initiatives, developing theatre-wide strategies, and graduated response plans, and working up both the NWCC and a new *Concept for the Deterrence and Defence of the Euro-Atlantic Area* (NATO, 2019a; NATO, 2020f). With so many competing priorities already on the Alliance's agenda, finding the political, institutional and intellectual bandwidth needed to agree a common lexicon and concept of MDO—and cyberspace's role therein—is a challenge.

NATO faces another difficulty not shared by adversaries. While Russia and China can focus conceptual, force and capability development efforts on a specific foe (the US and NATO) and region (their near abroad), NATO must plan and prepare for wide-reaching scenarios. A multi-domain concept and set of forces configured to address Russia in northern and eastern Europe might be ill-suited to operating in the Mediterranean, countering Iran in the Gulf, or deterring China in the Indo-Pacific. One potential risk is a divergence between US efforts to design MDO and JADC2 networks primarily to address China and any NATO system-of-systems for MDO oriented towards Russia (Grispen-Gelens, 2020).

B. Policy Tensions

Policy differences exacerbate conceptual ones. Allies differ in their policy and legal constraints, strategic cultures, threat perception, resources, planning and budgetary cycles and forces (Sondhaus, 2006). While solidarity ultimately remains NATO's strongest asset, these differences create seams that adversaries can exploit. This is especially so with cyberspace, where there is more sensitivity and less commonality to emerging national approaches than in more established domains, and to MDO, which is inherently predicated on integration and interoperability (Sharpy, 2020).

Information sharing is especially problematic for the cyber dimension of MDO, with Allies reticent to share details of their capabilities across NATO given security concerns and political sensitivities. The issue of permissions is also a 'significant challenge in the development of cyber capabilities', especially where reconnaissance on Allied soil and networks is required to detect hostile cyber activity (Watling & Roper, 2019). Nations also have differing policy, legal and ethical stances on key technologies on which MDO relies. This includes the use of offensive cyber capabilities or basing of hypersonic missiles or long-range penetrating fires in Europe, which some fear could be destabilising and escalatory (Quintin & Vanholme, 2020). NATO similarly lacks a common approach to governance and use of AI, autonomy and automation, all envisaged as essential enablers for JADC2 (Williams, 2020). This affects the levels of autonomy (with the human in, on or out of the loop) used for sensor data fusion and decision-making, or to deliver effects using uncrewed platforms, automated cyber systems and human-machine teaming (Scharre, 2018).

In considering cooperation and burden-sharing, Allies face several dilemmas depending on their ambitions and resources for both cyberspace and MDO. The US must overcome domestic inter-service rivalries and decide how to integrate partners, including whether it can accept a multinational vision of MDO that is not imposed on smaller allies—or excludes them entirely, at NATO's expense—but rather is genuinely collaborative (Watling & Roper, 2019). Larger European nations face the dilemma of whether to buy into a US-led architecture and system-of-systems with implications for freedom of action, data-sharing and procurement choices, or shoulder the costs of sovereign or multinational alternatives.[11] They also face choices over how best to contribute to multinational MDO: whether to aspire to full-spectrum capabilities to allow sovereign action and offer redundancy to Allies' capabilities or to specialise in certain domains (e.g. cyber) to offer niche capability and buy leverage with the US and NATO by making themselves indispensable. Smaller nations must decide how to influence larger Allies and NATO, and what to do if they lack cyber capabilities (or others deemed central to MDO, e.g. long-range fires) or their forces are too small to operate or gain MDO experience at echelons above brigade (Watling & Roper, 2019).

The economic fallout of COVID-19 also raises renewed questions about affordability and the extent to which Allies are willing and able to invest in new cyber capabilities—though some may see these as cost-efficient alternatives to land, air or maritime forces—and how they time investments in ambitious transformation programmes such as MDO (Clark, 2020). Timing presents both threats and opportunities from a cyber perspective. Rapid, hasty transformation risks undermining NATO cohesion and interoperability or creating vulnerabilities in JADC2 systems with immature cyber defences (Donaldson & Sciarini, 2019b). Conversely, overly cautious change risks ceding ground to adversaries such as Russia and China which are investing heavily in asymmetric means, including offensive cyber capabilities, to gain an information advantage over NATO (Kilcullen, 2020).

The most likely outcome may be a variegated approach, with some Allies (including the US) taking the lead on conceptual and capability development for MDO, creating national or mini-lateral networks for JADC2, and then building up a looser degree of interoperability at NATO level (Watling & Roper, 2019).

C. Capability and Force Development Priorities

Assuming NATO can overcome conceptual and policy hurdles, significant effort will still be required to develop the necessary forces and capabilities across all domains, but perhaps especially for cyberspace.

Operationalising MDO demands a 'calibrated force posture' with multi-domain formations strategically positioned, held at readiness and able to de-

[11] E.g. development of a 'combat cloud' within the Franco-German Future Combat Air System. See: Airbus, 2020.

ploy over large distances, trained and equipped to operate across multiple contested domains (Grispen-Gelens, 2020). The vision is for different sensors and shooters to share and fuse data, build a common operating picture, inform rapid decision-making and deliver effects at a time and place of the commander's choosing and to do so agnostic of domains, nation, service or platform (Niewood, Grant & Lewis, 2019). Forces must operate at pace and against an adversary contesting all domains. This tempo necessitates moving beyond NATO's past focus on synchronisation of pre-planned effects in individual domains towards more agile targeting and more resilience against hostile attempts at 'disorganisation' or 'systems attack' (Thomas, 2019; Engstrom, 2018).

Linking all this together demands novel approaches to C4ISR, as reflected in investments in JADC2 (Harrigian, 2020). This US initiative leverages advances in information and communication technologies such as mesh networks, cloud and edge computing, open architectures, data analytics, AI and machine learning, autonomy and automation, software-defined systems, robotics, satellite communications and sophisticated cyber and EMS capabilities (Hitchens, 2019). Future JADC2 networks must be secure, robust, resilient, agile and more decentralised, with enough bandwidth to share data in a timely and secure manner despite cyber attacks, jamming, spoofing or physical destruction of communication nodes (Goldfein, 2017). Trust is also essential, handling data from different sources and at multiple security levels without making controls so arduous that users and devices cannot access the network (Donaldson & Sciarini, 2019a).

Reliance on connectivity makes cyberspace, space and the EMS the 'centre of gravity' for MDO (Hess et al., 2019). JADC2 introduces obvious challenges from a cyber threat perspective, both in terms of the attack surface for different threat vectors and the cascading effects from hostile cyber activity—though, of course, existing centralised C2 hubs also have their own vulnerabilities to cyber or physical attack (Hess et al., 2019). Improved cyber capabilities are not only needed to secure and enable operations in other domains (Reilly, 2020). Investments by Russia and China to contest cyberspace and the EMS may also limit the ability of NATO commanders to employ offensive cyber capabilities at a time and place that will 'converge' with effects through other domains. Securing networks against disruption is critical at the operational and strategic levels given requirements for reach-back to headquarters, especially constraining organisations responsible for delivering offensive cyber effects, since these are likely to be physically located in the homeland (Watling & Roper, 2019; Nettis, 2020).

D. Challenges for Command and Control

Any shift towards MDO also raises difficult questions about C2. NATO is arguably already challenged by seams when executing joint warfare, let alone a more ambitious vision of future JADC2 (Perkins & Olivieri, 2018; Zadalis, 2018). In broad terms, this could adopt a more hierarchical or de-centralised model, each with associated benefits, costs and risks (DCDC, 2015). The

NATO C2COE has launched an MDO C2 demonstrator to explore these issues, including how new technology might enable accelerated decision-making, reduced reliance on siloed physical command centres and a re-imagining of mission command for future MDO (NATO C2COE, 2020a).

Problematically, authorities associated with using cyber capabilities are typically held at the strategic and national level; how tactical or operational commanders might call upon cyber means as part of future MDO remains unclear (Nettis, 2020). Responsibilities for cyberspace also often fall at least partly to civilian agencies, adding the complexity of cross-government co-operation. The private sector's role developing and applying technologies in the cyber domain (and, increasingly, space) also necessitates that NATO work more closely with industry, academia and others than for land, maritime or air operations (Ablon et al., 2019). This presents operational, policy and legal difficulties for C2, and cybersecurity challenges associated with reliance on industry-owned networks, though Allies continue to evolve novel mechanisms for partnering with industry to address cyber threats (Carr, 2016).

There is also the question of tempo: how to synchronise operations in cyberspace with the delivery of effects in other domains (Reilly, 2020). Though cyber attacks might initiate in a moment, the underlying tools and exploits may take years to develop and the lead times and scale of their eventual effect may be difficult to predict or measure given the difficulties with battle damage assessment in cyberspace or the EMS (Patrikarakos, 2017; US Joint Staff, 2019). Similarly, commanders may lack awareness or understanding of available cyber instruments and their limitations and effects compared to more familiar weapons in the physical domains, limiting inclusion in joint planning and decision-making (Carbonell, 2017).

E. Innovation and Transformation

Finally, NATO also faces vulnerabilities and risks associated with the pace of tactical and technological innovation in both the cyber domain and MDO. These change not only the capabilities that NATO requires, but also how it develops, acquires, trains, fields, exercises and sustains them, necessitating transformation across all components of the DOTMLPF-I framework and all stages of the capability lifecycle.[12]

Developing new technology is necessary but insufficient to deliver the cyber, C4ISR and other capabilities needed to realise ambitions for MDO (Dwyer, 2020). Technical standards and a broader enterprise architecture approach to manage and coordinate are essential. Yet despite increasing automation, the human dimension also remains key (Carbonell, 2017). There are several unanswered questions to consider, answers to which will shape whether NATO or its adversaries gain advantage in cyberspace and future MDO: how to deliver multi-domain education, training and exercising, including

[12] Doctrine, organisation, training, materiel, leadership, personnel, facilities and interoperability (DOTMLPF-I) is the mnemonic aid used by NATO military planners to consider the issues and perspectives required to field a new capability.

through challenging scenarios that allow learning through failure and make cyberspace a key consideration for non-cyber audiences (Perkins & Olivieri, 2018); how to bring together disparate modelling and simulation initiatives, integrating synthetic environments for individual domains into a single integrated architecture[13] allowing realistic simulations of MDO and the cross-domain effects of cyber, electronic and information warfare (McArdle, 2019); how to build a multi-domain culture and mindset that overcomes traditional stovepipes, such as territoriality by individual services or command structures (Goldfein, 2017; Heren, 2020); and how to maintain a pipeline of relevant skills and expertise, both for cyber defence and multi-domain integration, and offer career paths for specialists (Ablon et al., 2019).

Ensuring NATO is resilient against fast-changing cyber and multi-domain threats also requires enhancing its agility and adaptability (Ozdemir, 2020). This includes reforming capability development processes to reduce lead times—especially important for cyber capabilities—and increasing organisations' capacity to identify disruptive innovations and absorb them at pace (Ablon et al., 2019). This necessitates models such as agile and spiral development or DevSecOps, genuine partnerships with industry and academia and increased end-user involvement in systems design (Harrigian, 2020; Sharpy, 2020). Realising such transformation requires changes across DOTMPLF-I, including strong and sustained leadership, appropriate and coordinated investment of resources and a different attitude towards risk in areas such as acquisition, training and experimentation to operationalise cyberspace as part of MDO (Niewood, Grant & Lewis, 2019).

ACT, the NATO Communications and Information Agency and individual Allies are already taking steps to address barriers to agile capability development and innovation. However, there remains more to do and change takes time (Grand & Gillis, 2020). Lessons learned from past programmes offer insights into what enables success, but also urge realism about how difficult and long a process it can be to implement reforms in complex military bureaucracies and multinational settings (Sharpy, 2020). Examples cited include the case of AirLand Battle, which for all its ambition could not eradicate the deep-seated differences between the US Army and US Air Force cultures and views on warfighting (Johnson, 2018); the development and promulgation of Link 16 across the Alliance, which has taken almost half a century to overcome both technical and cultural barriers to interoperability (Hura et al., 2000); or NATO's hard-fought efforts to enhance chemical, biological, radiological and nuclear capabilities since the 1990s (Ablon et al., 2019). Tellingly, militaries are still working to better integrate land, sea and airpower, suggesting it may take decades to fully understand the complex synergies with cyberspace, the EMS and space (Reilly, 2020).

[13] For example, UK Strategic Command has partnered with technology company Improbable to explore the feasibility of high-fidelity modelling and simulation of multi-domain operations through its Single Synthetic Environment (SSE) Technology Demonstrator, with the British Army also contracting Improbable to help develop its SSE roadmap. See Improbable, 2020.

4. Conclusion

In conclusion, cyber threats do not exist in a vacuum, nor are NATO's cyber operations divorced from developments on land, at sea, in the air or in space. According to emerging concepts in the US and other Allied nations, the future is 'multi, multi, multi' (Schanz, 2014: p. 40). This necessitates thinking beyond existing conceptual or institutional boundaries and understanding cyber developments in their wider context: multi-domain, multi-sensor, multi-shooter, multi-mission, multi-service and multi-national. This requires education, training and cultural reform to instil multi-domain thinking at all levels: from junior military personnel and international civilian staff up to the most senior political-military leaders.

Such thinking avoids the pitfalls of oversimplified analysis but, equally, brings the challenge of complexity. Fortunately, NATO is one of the great success stories of an organisation harmonising different perspectives, institutions, cultures, capabilities and effects in pursuit of a common goal; the Alliance is already a system-of-systems of a kind (Sharpy, 2020). However, it faces complex and fast-changing challenges as it evolves from an analogue to a digital alliance and begins to embrace cyberspace and MDO. These stem both from external adversaries such as the evolving theory and practice of disorganisation and reflexive control by Russia or systems attack by China, and internal barriers to NATO cohesion. Continuing to improve understanding of the interlinkages between these different threats and risks is essential to inform the transformation process needed to realise NATO's ambitions for the cyber domain and for multi-domain more broadly.

5. References

Ablon, L., Binnendijk, A., Hodgson, Q., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. (2008) *Operationalizing Cyberspace as a Military Domain: Lessons for NATO*. Santa Monica, CA: RAND Corporation, PE-329-NATO. [Accessed 13th August 2020]. Available from: https://www.rand.org/pubs/perspectives/PE329.html.

Adamsky, D. (2015) *Cross-Domain Coercion: The Current Russian Art of Strategy*. Proliferation Papers 54, Institut Français des Relations Internationales (Ifri). Available from: https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf [Accessed 12th August 2020].

Airbus. (2020) *Airbus and Thales Join Forces to Develop the Air Combat Could for Future Combat Air System*. Airbus, 19 February 2020. Available from: https://www.airbus.com/newsroom/news/en/2020/02/airbus-and-thales-join-forces-to-develop-the-air-combat-cloud-for-future-combat-air-system.html [Accessed 22nd September 2020].

Asian Military Review. (2020) *China Broadens Cyber Options*. Asian Military Review, 15 January 2020. Available from: https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/ [Accessed 24th September 2020].

Barry, B. (2020) *New UK Strategic Command Faces Early Challenges*. IISS Military Balance [online]. 19 June 2020. London: International Institute of Strategic Studies. Available from: https://www.iiss.org/blogs/military-balance/2020/06/uk-strategic-command-challenges-covid-19 [Accessed 13th August 2020].

Bommakanti, K. (2020) *AI in the Chinese Military: Current Initiatives and the Implications for India.* Occasional Paper [online], Observer Research Foundation. February 2020. Available from: https://www.orfonline.org/research/a-i-in-the-chinese-military-current-initiatives-and-the-implications-for-india-61253/ [Accessed 14th August 2020].

Brent, L. (2019) *NATO's Role in Cyberspace*. NATO Review [online]. 12 February 2019. Available from: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html [Accessed 11th August 2020].

Brzozowski, A. (2018) *NATO Sees New Cyber Command Centre by 2023 as Europe Readies for Cyber Threats.* Euractiv [online]. 17 October 2018. Available from: https://www.euractiv.com/section/defence-and-security/news/nato-sees-new-cyber-command-centre-by-2023-as-europe-readies-for-cyber-threats/ [Accessed 22nd October 2020].

Carbonell, J. (2017) *Getting off the Bench: Challenges to Integrating Cyber into Multi-Domain Operations.* OTH: Multi-Domain Operations & Strategy [online]. 1 June 2017. Available from: https://othjournal.com/2017/06/01/cyber-challenges-mdo/ [Accessed 12th August 2020].

Carr, M. (2016) Public-Private Partnerships in National Cyber-Security Strategies. *International Affairs.* 92 (1), 43-62. Available from: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf [Accessed 13th August 2020].

Carter, N. (2019) *New UK Strategic Command to Drive Integration for Multi-Domain Effect*. SC Magazine UK 5 December 2019. Available from: https://www.scmagazineuk.com/new-uk-strategic-command-drive-integration-multi-domain-effect/article/1667949 [Accessed 11th August 2020].

Clare, P. (2020) *The Answer is Multi-Domain Operations – Now What's the Question?* Wavell Room. 13 February 2020. Available from: https://wavellroom.com/2020/02/13/the-answer-is-multi-domain-operations-now-whats-the-question/ [Accessed 7th August 2020].

Clark, B. (2020) *JADC2 and AI Should Enable Post-Pandemic Military Creativity, Not Replace It.* Hudson Institute. 9 May 2020. Available from: https://www.hudson.org/research/16019-jadc2-and-ai-should-enable-post-pandemic-military-creativity-not-replace-it [Accessed 13th August 2020].

Clark, B., Patt, D., & Schramm, H. (2020) *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations.* Center for Strategic and Budgetary Assessments (CSBA), 11 February. Available from: https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations [Accessed 20th September 2020].

Conti, G. & Raymond, D. (2017) *On Cyber: Towards an Operational Art for Cyber Conflict.* Kopidion Press.

Conti, G. & Fanelli, R. (2019) 'How could they not: thinking like a state cyber threat actor'. *The Cyber Defense Review*. (4) 2, 49-64. Available from: https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/CDR%20V4N2-Fall%202019.pdf [Accessed 22nd September 2020].

Costello, J. & McReynolds, J. (2018) China's Strategic Support Force: A Force for a New Era. *China Strategic Perspectives 13* [online]. Institute for National Strategic Studies (INSS), National Defense University. Available from: https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf [Accessed 8th August 2020].

Cozad, M. (2016) *PLA Joint Training and Implications for Future Expeditionary Operations*. Santa Monica, CA: RAND Corporation, CT-451. Available from: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT451/RAND_CT451.pdf [Accessed 12th August 2020].

Development, Concepts and Doctrine Centre (DCDC). (2015) *Future Operating Environment 2035*. Strategic Trends Programme. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/646821/20151203-FOE_35_final_v29_web.pdf [Accessed 9th August 2020].

Development, Concepts and Doctrine Centre (DCDC). (2017) *Joint Concept Note 2/17 Future of Command and Control.* Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf [Accessed 11th August 2020].

Defense Acquisition University (DAU). (2020) Chapter 3: Systems Engineering. In: *US Defense Acquisition Guidebook.* Fort Belvoir, VA: USA. Available from: https://www.dau.edu/guidebooks/_layouts/15/WopiFrame.aspx?sourcedoc=/guidebooks/Shared%20Documents/Chapter%203%20Systems%20Engineering.pdf&action=default [Accessed 8th August 2020].

Defense Intelligence Agency (DIA). (2019) *China Military Power: Modernizing a Force to Fight and Win.* DIA-02-1706-065. Available from: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [Accessed 11th August 2020].

Donaldson, J. & Sciarini, C. (2019a) *Vulnerabilities of Multi-Domain Command and Control (Part 1).* OTH: Multi-Domain Operations & Strategy. 4 March 2019. Available from: https://othjournal.com/2019/03/04/vulnerabilities-of-multi-domain-command-and-control-part-1/ [Accessed 11th August 2020].

Donaldson, J. & Sciarini, C. (2019b) *Vulnerabilities of Multi-Domain Command and Control (Part 2)*. OTH: Multi-Domain Operations & Strategy. 6 March 2019. Available from: https://othjournal.com/2019/03/06/vulnerabilities-of-multi-domain-command-and-control-part-2/ [Accessed 11th August 2020].

Donnelly, J. & Farley, J. (2019) *Defining the 'Domain' in Multi-Domain*, in the Joint Air Power Competence Centre, Joint Air and Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future (2019): 7-11. Available from: https://www.japcc.org/defining-the-domain-in-multi-domain/ [Accessed 20th September 2020].

Dwyer, M. (2020) *Making the Most of the Air Force's Investment in Joint All Domain Command and Control*. Center for Strategic & International Studies (CSIS). 6 March 2020. Available from: https://www.csis.org/analysis/making-most-air-forces-investment-joint-all-domain-command-and-control [Accessed 11th August 2020].

Engstrom, J. (2018) *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare.* Santa Monica, CA: RAND Corporation, RR-1708-OSD. Available from: https://www.rand.org/pubs/research_reports/RR1708.html [Accessed 10th August 2020].

Feickert, A. (2020) *Defense Primer: Army Multi-Domain Operations (MDO)*. Briefing prepared by the Congressional Research Service. 19 January 2020. Available from: https://fas.org/sgp/crs/natsec/IF11409.pdf [Accessed 9th August 2020].

Freedberg, S. (2018) *Army Multi-Domain Update: New HQs, Grey Zones & The Art of the Unfeasible*. Breaking Defense. 7 December 2018. Available from: https://breakingdefense.com/2018/12/army-multi-domain-update-new-hqs-grey-zones-the-art-of-the-unfeasible/ [Accessed 13th August 2020].

Galeotti, M. (2016) ‘Hybrid, ambiguous, and non-linear? How new is Russia’s ‘new way of war’?’ *Small Wars and Insurgencies*. 27 (2). 21 March 2016. Available from: https://www.tandfonline.com/doi/abs/10.1080/09592318.2015.1129170 [Accessed 11th August 2020].

Goldfein, D. (2017) *Enhancing Multi-Domain Command and Control… Tying it All Together.* Washington, DC: United States Air Force. Available from: https://www.af.mil/Portals/1/documents/csaf/letter3/Enhancing_Multi-domain_CommandControl.pdf [Accessed 13th August 2020].

Grand, C. & Gillis, M. (2020) Alliance Capabilities at 70: Achieving Agility for an Uncertain Future. *NDC Policy Brief* No.1 January 2020. Available from: http://www.ndc.nato.int/download/downloads.php?icode=622 [Accessed 14th August 2020].

Grest, H. & Heren, H. (2019) *What is a Multi-Domain Operation?* in the Joint Air Power Competence Centre, Joint Air and Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future (2019): 1-3. Available from: https://www.japcc.org/what-is-a-multi-domain-operation/ [Accessed 20th September 2020].

Griesemer, T. (2018) *‘Russian Military Reorganization: A Step Towards Multi-Domain Operations’.* OTH: Multi-Domain Operations & Strategy, 11 November 2018. Available from: https://othjournal.com/2018/11/19/russian-military-reorganization-a-step-toward-multi-domain-operations/ [Accessed 11th August 2020].

Grispen-Gelens, C. (2020) *Cohesion Through Convergence?* Seminar MDO Read Ahead, NATO C2COE, 1 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-carlina-grispen-gelens-cohesion-through-convergence/ [Accessed 11th August 2020].

Harrigian, Jeffrey L. (2020) Shaping the Future Multi-Domain C2. *Joint Air Power Competence Centre (JAPCC) Journal.* 29 (1). Available from: https://www.japcc.org/shaping-the-future-multi-domain-c2/ [Accessed 12th August 2020].

Heren, H. (2020) ‘Multi-Domain Operations: Inconceivable!’. *Joint Air Power Competence Centre (JAPCC) Journal.* 29 (1). Available from: https://www.japcc.org/multi-domain-operations-inconceivable/ [Accessed 12th August 2020].

Hess, J, Kiser, A., Bouhafa, E.M., & Williams, S. (2019) *The Combat Cloud: Enabling Multidomain Command and Control across the Range of Military Operations.* Wright Flying Papers, Air Command and Staff College. February 2019. Available from: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/wf_0065_hess_combat_cloud.pdf [Accessed 14th August 2020].

Hitchens, T. (2019a) *Multi Domain drive NATO Industry to Craft New Air Power Interoperability.* Breaking Defense. 15 November 2019. Available from: https://breakingdefense.com/2019/11/multi-domain-drives-nato-industry-to-craft-new-air-power-interoperability/ [Accessed 12th August 2020].

Hitchens, T. (2019b). *OSD, Services Get First Look at Air Force Multi-Domain Chops.* Breaking Defense, 23 December 2019. Available from: https://breakingdefense.com/2019/12/osd-services-get-first-look-at-air-force-multi-domain-chops/ [Accessed 14th August 2020].

Hura, M., McLeod, G., Larson, E., Schneider, J., Gonzales, D., Norton, D., Jacobs, J., O’Connell, K., Little, W., Mesic, R., & Jamison, L. (2000) *Interoperability: A Continuing Challenge in Coalition Air Operations.* Santa Monica, CA: RAND Corporation, MR-1235-AF. Available from: https://www.rand.org/pubs/monograph_reports/MR1235.html [Accessed 21st September 2020].

IHS Jane’s. (2020) *China – Defence Budget Overview.* Jane’s Sentinel Security Assessment – China and Northeast Asia. 22 January 2020. Available from: https://janes.ihs.com/Janes/Display/chins090-cna [Accessed 9th August 2020].

Improbable. (2020) *Improbable Secures Pathfinder Technology Demonstrator Contract with British Army.* 6 August. Available from: https://improbable.io/blog/uk-army-cttp-sse [Accessed 13th August 2020].

International Institute for Strategic Studies (IISS). (2019) 'China's Cyber Power in a New Era' in *Asia Pacific Regional Security Assessment* 2019, IISS, May 2019. Available from: https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5 [Accessed 24th September 2020].

Johnson, D. (2018) *Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle.* Santa Monica, CA: RAND Corporation. PE-301-A/AF. Available from: https://www.rand.org/pubs/perspectives/PE301.html [Accessed 13th August 2020].

Joiner, K. & Tutty, M. (2018) 'A tale of two allied defence departments: new assurance initiatives for managing increasing system complexity, interconnectedness and vulnerability'. *Australian Journal of Multi-Disciplinary Engineering.* 14 (1). Available from: https://www.tandfonline.com/doi/full/10.1080/14488388.2018.1426407?casa_token=NQjkdhyasGUAAAAA%3AqkxJ_XQlQSkacMH0_TE13gLRUFzB7ANaj42zxuUeGRuun3WOYYC0ALeNRdui_BPgiuV8Rbpq31Y [Accessed 22nd September 2020].

Kania, E. & Costello, J. (2017) *China's Quest for Informatization Drives PLA Reforms.* The Diplomat, 4 March 2017. Available from: https://thediplomat.com/2017/03/chinas-quest-for-informatization-drives-pla-reforms/ [Accessed 10th August 2020].

Kania, E. (2020) *'AI Weapons' in China's Military Innovation.* The Brookings Institution in partnership with the Center for Security and Emerging Technology, April 2020. Available from: https://www.brookings.edu/research/ai-weapons-in-chinas-military-innovation/ [Accessed 14th August 2020].

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

Knighton, R. (2019) *Lord Trenchard Memorial Lecture 2019*. Royal United Services Institute (RUSI). November 18. Available from: https://rusi.org/event/lord-trenchard-memorial-lecture-2019 [Accessed 11th August 2020].

Lindsay, J. & Gartzke, E. (2020) Politics By Many Other Means: The Comparative Strategic Advantages of Operational Domains. *Journal of Strategic Studies*. Available from: https://doi.org/10.1080/01402390.2020.1768372 [Accessed 13th August 2020].

Manea, O. (2018) The Role of Offset Strategies in Restoring Conventional Deterrence. *Small Wars Journal*. Available from: https://smallwarsjournal.com/jrnl/art/role-offset-strategies-restoring-conventional-deterrence [Accessed 21st September 2020].

McArdle, J. (2019) *Victory Over and Across Domains: Training for Tomorrow's Battlefields.* Center for Strategic and Budgetary Assessments (CSBA), 25 January. Available from: https://csbaonline.org/research/publications/victory-over-and-across-domains-training-for-tomorrows-battlefields [Accessed 21st September 2020].

McDermott, R. (2020) Russian Armed Forces Test Multi-Domain Operations. *Eurasia Daily Monitor* [online]. 17 (123). Available from: https://jamestown.org/program/russian-armed-forces-test-multi-domain-operations/ [Accessed 21st September 2020].

McInnis, J. (2017) *Iranian Concepts of Warfare: Understanding Teheran's Evolving Military Doctrines*. American Enterprise Institute. February 2017. Available from: https://www.aei.org/research-products/report/iranian-concepts-of-warfare-understanding-tehrans-evolving-military-doctrines/ [Accessed 13th August 2020].

McLeary, P. (2018) ‘Russia Winning Info & Electronic War in Syria, US & UK Generals Warn’. *Breaking Defense* [online], 9 October. Available from: https://breakingdefense.com/2018/10/russia-winning-information-electronic-war-over-syria-us-uk-generals-warn/ [Accessed 20th September 2020].

Nakasone, P. & Lewis, C. (2017) Cyberspace in Multi-Domain Battle. *The Cyber Defense Review* [online]. 2 (1), 15-26. Available from: https://www.jstor.org/stable/10.2307/26267397 [Accessed 11th August 2020].

Nettis, K. (2020) *Multi-Domain Operations: Bridging the Gaps for Dominance.* Sixteenth Air Force. 16 March 2020. Available from: https://www.16af.af.mil/News/Article/2112873/multi-domain-operations-bridging-the-gaps-for-dominance/ [Accessed 13th August 2020].

Niewood, E., Grant, G., & Lewis, T. (2019) *A New Battle Command Architecture for Multi-Domain Operations: Countering Peer Adversary Power Projection.* The MITRE Center for Technology & National Security, December 2019. Available from: https://www.mitre.org/sites/default/files/publications/Joint-All-Domain-Command-Control.pdf [Accessed 13th August 2020].

North Atlantic Treaty Organisation (NATO). (2018a). *Brussels Summit Declaration*. 11 July 2020. Available from: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk [Accessed 23rd October 2020].

North Atlantic Treaty Organisation (NATO). (2018b). *Framework for Future Alliance Operations: 2018 Report*. Available from: https://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf [Accessed 23rd October 2020].

North Atlantic Treaty Organisation (NATO). (2019a) *NATO: Ready for the Future. Adapting the Alliance (2018-2019).* 29 November 2019. Available from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf [Accessed 12th August 2020].

North Atlantic Treaty Organisation (NATO). (2019b) *AJP-3 Allied Joint Doctrine for the Conduct of Operations*, Edition C Version 1, February 2019. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf [Accessed 24th September 2020].

North Atlantic Treaty Organisation (NATO). (2020a) *NATO’s approach to space*. Available from: https://www.nato.int/cps/en/natohq/topics_175419.htm [Accessed 13th August 2020].

North Atlantic Treaty Organisation (NATO). (2020b) *Cyber defence*. Available from: https://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed 13th August 2020].

North Atlantic Treaty Organisation (NATO). (2020c) *Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operation*. London: Ministry of Defence. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf [Accessed 11th August 2020].

North Atlantic Treaty Organisation (NATO). (2020d) *NATO Warfighting Capstone Concept Experiment Workshop.* Available from: https://www.act.nato.int/articles/nato-warfighting-capstone-concept-experiment-workshop [Accessed 22nd October 2020].

North Atlantic Treaty Organisation (NATO). (2020e) *Military Committee Visits Joint Warfare Centre; NATO Military Leaders Discuss Warfare Development.* Available from: https://www.act.nato.int/articles/mc-visits-jwc-discuss-warfare-development [Accessed 22nd October 2020].

North Atlantic Treaty Organisation (NATO). (2020f) *NATO Chiefs of Defence Assess Current Adaptation and Future Requirements.* Available from: https://www.nato.int/cps/en/natohq/news_172672.htm [Accessed 22nd October 2020].

NATO Command and Control Centre of Excellence (NATO C2COE). (2020a) *Multi-Domain Operations C2 Demonstrator, a collaboration between NATO C2COE and civil partners.* 16 April 2020. Available from: https://c2coe.org/2020/04/16/multi-domain-operations-c2-demonstrator-a-collaboration-between-nato-c2coe-and-civil-partners/ [Accessed 8th August 2020].

NATO Command and Control Centre of Excellence (NATO C2COE). (2020b) *Multi-Domain Operations: "Keys to Master Complexity"*. Available from: https://c2coe.org/seminar/ [Accessed 12th August 2020].

NATO Science and Technology Organisation (STO). (2018) *Agile Multi-Domain C2 of Socio-Technical Enterprises in Hybrid Operations*. Available from: https://www.sto.nato.int/SitePages/newsitem.aspx?ID=3578&IsDlg=1 [Accessed 22nd October 2020].

NATO Science and Technology Organisation (STO). (2020) *Wargaming Multi-Domain Operations in an A2/AD Environment.* Available from: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16876 [Accessed 22nd October 2020].

Office of the Secretary of Defense (OSD). (2019) *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019.* Available from: https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf [Accessed 13 August 2020].

Ozdemir, H. (2020) *Multi-Domain Operations from System Dynamics Perspective.* Seminar MDO Read Ahead, NATO C2COE. 10 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-dr-hilmi-ozdemir-multi-domain-operations-from-system-dynamics-perspective/ [Accessed 11th August 2020].

Paul, C., Clarke, C., Schwille, M., Hlavka, J., Brown, M., Davenport, S., Porsche III, I., & Harding, J. (2018) *Lessons from Others for Future US Army Operations in and through the Information Environment: Case Studies.* Santa Monica, CA: RAND Corporation. RR-1925/2-A. Available from: https://www.rand.org/pubs/research_reports/RR1925z2.html [Accessed 10th August 2020].

Perkins, W. & Olivieri, A. (2018) On Multi-Domain Operations. *Joint Air Power Competence Centre (JAPCC) Journal.* 26 (1). Available from: https://www.japcc.org/on-multi-domain-operations/ [Accessed 12th August 2020].

Pollpeter, K, Chase, M., & Heginbotham, E. (2017) *The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations.* Santa Monica, CA: RAND Corporation, RR-2058-AF. Available from: https://www.rand.org/pubs/research_reports/RR2058.html [Accessed 21st September 2020].

Quintin, A. & Vanholme, R. (2020) *Hypersonic Missiles and European Security: Challenges Ahead.* European Army Interoperability Centre (Finabel). 28 July 2020. Available from: https://finabel.org/hypersonic-missiles-and-european-security/ [Accessed 13th August 2020].

Reilly, J. (2020) *Creating Competitive Space Through a Framework of Joint All Domain Maneuver*. Seminar MDO Read Ahead, NATO C2COE. 23 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-dr-jeff-reilly-creating-competitive-space-through-a-framework-of-joint-all-domain-maneuver/ [Accessed 12th August 2020].

Schanz, M. (2014) *The Combat Cloud.* Air Force Magazine, July 2014. Available from: http://www.airforcemag.com/MagazineArchive/Magazine%20Documents/2014/July%202014/0714combatcloud.pdf [Accessed 12th August 2020].

Scharre, P. (2018) *Army of None: Autonomous Weapons and the Future of War.* London, UK: W.W. Norton & Company.

Schneider, J. (2019) The capability/vulnerability paradox and military revolutions: Implications for computing, cyber, and the onset of war. *Journal of Strategic Studies.* 42 (6), 841-863. Available from: https://www.tandfonline.com/

doi/abs/10.1080/01402390.2019.1627209 [Accessed 20th September 2020].

Scouras, J., Smyth, E., & Mahnken, T. (2017) *Cross-Domain Deterrence in US-China Strategy: Workshop Proceedings.* The John Hopkins University Applied Physics Laboratory. Originally published in 2014 and re-issued in 2017. Available from: https://www.jhuapl.edu/Content/documents/CrossDomainWeb.pdf [Accessed 11th August 2020].

Sharpy, T. (2020) *Multi-Domain Operations: The Future of Warfare*. Seminar MDO Read Ahead, NATO C2COE. 16 July 2020. Available from: http://c2coe.org/download/seminar-2020-read-ahead-lieutenant-general-sharpy-multi-domain-operations-the-future-of-warfare/ [Accessed 12th August 2020].

Shea, J. (2018) Cyberspace as a Domain of Operations: What is NATO's Vision and Strategy? *MCU Journal*. 9 (2), 133-150. Available from: https://doi.org/10.21140/mcuj.2018090208 [Accessed 10th August 2020].

Siegemund, M. (2018) *NATO Planning and Multi Domain Operations: A German Perspective.* OTH: Multi-Domain Operations & Strategy. 27 June 2018. Available from: https://othjournal.com/2018/06/27/nato-planning-and-multi-domain-operations-a-german-perspective/ [Accessed 9th August 2020].

Smagh, N. (2020) *Defense Capabilities: Joint All Domain Command and Control.* Briefing prepared by the Congressional Research Service. 6 April 2020. Available from: https://fas.org/sgp/crs/natsec/IF11493.pdf [Accessed 12th August 2020].

Sondhaus, L. (2006) *Strategic Culture and Ways of War.* Routledge Military Studies, Routledge.

Spirtas, M. (2018) *Towards one understanding of multiple domains.* RAND Corporation, 2 May 2018. Available from: https://www.rand.org/blog/2018/05/toward-one-understanding-of-multiple-domains.html [Accessed 24th September 2020].

Sprang, R. (2018) *Russia in Ukraine 2013-2016: The Application of New Type Warfare Maximizing the Exploitation of Cyber, IO and Media.* Small Wars Journal 11 September 2018. Available from: https://smallwarsjournal.com/jrnl/art/russia-ukraine-2013-2016-application-new-type-warfare-maximizing-exploitation-cyber-io-and [Accessed 9th August 2020].

Tasic, M. (2019). Exploring North Korea's Asymmetric Military Strategy. *Naval War College Review* [online]. 72 (4), 53-72. Available from: https://www.jstor.org/stable/10.2307/26775519 [Accessed 13th August 2020].

Thomas, T. (2019) *Russian Military Thought: Concepts and Elements.* MITRE Corporation. August 2019. Available from: https://www.mitre.org/sites/default/files/publications/pr-19-1004-russian-military-thought-concepts-elements.pdf [Accessed 13th August 2020].

Tigner, B. (2018) *Electronic jamming between Russia and NATO is par for the course in the future, but it has its risky limits.* Atlantic Council, 15 November 2018. Available from: https://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-in-the-future-but-it-has-its-risky-limits/ [Accessed 22nd September 2020].

Training and Doctrine Command (TRADOC). (2017) *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century* Version 1.0, December 2017. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf [Accessed 22nd September 2020].

Training and Doctrine Command (TRADOC). (2018) *The US Army in Multi-Domain Operations 2028.* TRADOC Pamphlet 525-3-1. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf [Accessed 10th August 2020].

Tucker, P.. (2019) *NATO Getting More Aggressive on Offensive Cyber.* Defense One, 24 May 2019. Available from: https://www.defenseone.com/technology/2019/05/nato-getting-more-aggressive-offensive-cyber/157270/ [Accessed 13th August 2020].

Underwood, K. (2020) *Army Shapes Joint All-Domain Operations.* AFCEA, 1 August 2020. Available from: https://www.afcea.org/content/army-shapes-joint-all-domain-operations [Accessed 14th August 2020].

US Joint Staff. (2018) *Memorandum for: Military Education Coordination Council Principals + Capstone Director.* Public Intelligence, 27 August 2018. Available from: https://publicintelligence.net/jcs-china-system-attack/ [Accessed 13th August 2020].

US Joint Staff. (2019) *Methodology for Combat Assessment.* CJCSI 3162.02. Washington, DC. 8 March 2019. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/cjcsi_3162_02.pdf?ver=2019-03-13-092459-350 [Accessed 14th August 2020].

Watling, J. & Roper, D. (2019) *European Allies in US Multi-Domain Operations.* Occasional Paper, Royal United Services Institute (RUSI). October 2019. Available from: https://rusi.org/sites/default/files/20190923_european_allies_in_us_multi-domain_operations_web.pdf [Accessed 13th August 2020].

Wijninga, E. (2018) *Training Joint Forces for Multi Domain Operations.* Conference read-ahead for the Joint Air & Space Power Conference 2019, Joint Air Power Competence Centre. Available from: https://www.japcc.org/training-joint-forces-for-multi-domain-operations/ [Accessed 22nd September 2020].

Williams, L. (2020) *JADC2 Tops Pentagon's Artificial Intelligence Efforts.* FCW, 9 July 2020. Available from: https://fcw.com/articles/2020/07/09/williams-jaic-ai.aspx [Accessed 13th August 2020].

Unal, B. (2019) *Cybersecurity of NATO's Space-Based Strategic Assets.* Chatham House, July 2019. Available from: https://www.chathamhouse.org/sites/default/files/2019-06-27-Space-Cybersecurity-2.pdf [Accessed 22nd September 2020].

Zadalis, T. (2018) Multi-Domain Command and Control: Maintaining Our Asymmetric Advantage. *Joint Air Power Competence Centre (JAPCC) Journal.* 26 (1). Available from: https://www.japcc.org/multi-domain-command-and-control/ [Accessed 13th August 2020].

Zager, R. & Zager, J. (2017) OODA Loops in Cyberspace: A New Cyber-Defense Model. *Small Wars Journal.* 21 October 2017. Available from: https://smallwarsjournal.com/jrnl/art/ooda-loops-cyberspace-new-cyber-defense-model [Accessed 2nd November 2020].