Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030

Franz-Stefan Gady
Research Fellow
Cyber, Space and Future Conflict Division
International Institute for Strategic Studies

Alexander Stronell
Research Assistant
Cyber, Space and Future Conflict Division
International Institute for Strategic Studies

Abstract: Synchronised kinetic and cyber operations across domains that present 'multiple dilemmas' are a fundamental tenet of multi-domain operations. Recent practice and study of the battlespace use of cyber capabilities in conjunction with kinetic operations, however, have shown the difficulties in creating joint effects due to insufficient synchronisation of operations or lack of coordination and control of cyber effects. This paper outlines three requirements needed to conduct integrated cyber and kinetic operations in a future high-intensity conflict involving NATO and a near-peer adversary: firstly, an internet of military things (IoMT) in conjunction with an artificial-intelligence (AI)-enabled command and control (C2) capability for integrated cyber and kinetic operations; secondly, multi-domain formations integrated with cyber commands or their respective organisational equivalents for coordinated theatre-wide cyber campaigns; and thirdly, a cyber mission command doctrine based on decentralised decision-making and decentralised execution to enable an accelerated operational pace. The analysis presents three comparative country studies— the US, UK and Germany— to assess the status of the integration of cyber capabilities into multi-domain warfighting concepts for high-intensity conflict in 2030. It also offers a preliminary set of recommendations on technical capabilities, new organisational structures and doctrinal changes required to facilitate the better integration of cyber with kinetic capabilities.

Keywords: *Offensive cyber operations, high-intensity warfare, multi-domain operations, internet of military things, mission command*

1. INTRODUCTION

Among NATO member states, the US has taken the lead in developing multi-domain operational concepts.[1] These are eventually expected to be adopted into formal doctrine in all military service branches and are built around synchronised combined arms operations across all five warfighting domains (including cyber and space); as well the electromagnetic spectrum. The US Army has designated its version of this new operational concept 'Multi-Domain Operations' (MDO) (TRADOC, 2018). The US Air Force, Navy, and Marine Corps are working on related concepts, and the Joint Chiefs of Staff are expected to publish a new overarching Joint Warfighting Concept for All-Domain Operations by the end of 2020 integrating the separate service approaches (Goure, 2019; Clark, 2020). The US' NATO allies, including the UK and Germany, have also begun the development of similar operational concepts (Kommando Heer, c.2017; Gerhartz, 2020).

Straddling all five warfighting domains,[2] cyberspace is not merely the connector of all systems, but also a weapons platform in itself, since cyberspace environments can be altered to allow for various vectors of attack on the adversary in ways that natural physical environments cannot. Synchronised kinetic and cyber operations across domains that present 'multiple dilemmas' are a fundamental tenet of multi-domain operations (Taylor & Kay, 2019).[3] Over the past decade, the US has pioneered the practical battlespace use of cyber capabilities in conjunction with kinetic operations, notably in operations conducted against Islamic State (also known as ISIL and ISIS). Though most details remain classified, US Cyber Command's Joint Task Force Ares (JTF-Ares), established in the first half of 2016, is known to have synchronised its capabilities with kinetic battlefield operations, most notably in Operation Glowing Symphony (OGS) (Martelle, 2018; Martelle, 2020), established to 'contest ISIL in the information domain'. Cyber Command has responsibility for coordinating its synchronisation with kinetic offensive operations conducted by other commands (US Cyber Command, 2016). Though characterised as a success, heavily redacted briefing documents suggest that significant challenges were encountered, and lessons learned in the deconfliction and engagement process. In particular, JTF-Ares cyberattack operators were required to undergo a further target vetting and deconfliction process after Combatant Command had formally designated a target for cyberattack, presumably complicating the engagement of time-sensitive targets (US Cyber Command, 2017; Martelle, 2020).

[1] No agreed definition of multi-domain operations among NATO member states exists. Multi-domain operations in this paper are defined as coordinated and synchronised combined arms operations across all warfighting domains and services at and above the tactical level that present multiple complementary threats to a great power adversary.

[2] No clear definition of domain exists among NATO member states (Townsend, 2019).

[3] For the sake of consistency, this paper will refer to all military operations built around synchronised combined arms operations across all five warfighting domains, the electromagnetic spectrum, and across service branches, as multi-domain operations and will use the MDO acronym only in reference to the US Army's narrower concept.

Several recent academic and military studies of the battlespace use of cyber capabilities in conjunction with kinetic operations demonstrate the difficulties associated with creating joint effects due to insufficient synchronisation of operations or lack of coordination and control of cyber effects (Metcalf & Barber, 2014; Kostyuk & Zhukov, 2017; Rothstein & Saltzman, 2019). A key challenge thus exists in the effective integration of conventional kinetic operations with cyber, space and information operations in the future battlespace. Further challenges identified as associated with multi-domain operations include the necessity of a secure and reliable cloud communication network; the need for highly trained personnel in command and control (C2); integration of allied capability; and stress exerted on the C2 structure (Rothstein & Saltzman, 2019).

Despite the apparent centrality of cyberspace to future high-intensity conflict, there has been little unclassified analysis of the specific technical, organisational and doctrinal requirements for the effective integration of cyber capabilities into multi-domain operations in future high-intensity warfighting scenarios (for some exceptions, see: Bonner, 2014; Reilly, 2016; McArdle, 2019; Rothstein & Saltzman, 2019). While literature exists exploring the organisational integration of offensive cyber capabilities (OIOCC) within national security structures (Smeets, 2018) and on kinetic and cyber operations in wartime (Kostyuk & Zhukov, 2017), the integration of kinetic and cyber strike capabilities for conventional warfighting has not formerly been addressed.

2. AIM

This paper will first analyse the conceptual origins of multi-domain operations before outlining the three requirements judged necessary for conducting integrated cyber and kinetic operations in a future high-intensity conflict involving NATO and a great power adversary in 2030: Firstly, an internet of military things (IoMT) in conjunction with an AI-enabled C2 capability for integrated cyber and kinetic operations; secondly, multi-domain formations integrated with cyber commands or their respective organisational equivalents for coordinated theatre-wide cyber campaigns; and thirdly, a cyber mission command doctrine based on decentralised decision-making and decentralised execution to enable an accelerated operational pace.

The analysis will then present three comparative country studies— the United States (US), United Kingdom (UK) and Germany—to assess the status of the integration of cyber capabilities based on the three identified requirements into multi-domain warfighting concepts for high-intensity conflict in 2030. These three countries were selected because they are among the largest military powers in the NATO alliance, and each publicly acknowledges the possession of offensive cyber capabilities. All three have also begun the development of operational concepts around or similar to multi-domain operations. The analysis will also offer recommendations on technical capabilities, new organisational structures, and doctrinal changes required to facilitate the better integration of cyber with kinetic capabilities. The paper will not attempt to present a comprehensive set of capability requirements, nor will it address future multi-domain operations in their entire range and scope. Rather, it will confine itself to some of the technical, organisational and doctrinal capabilities judged to be necessary for the opening stages of a conventional high-intensity conflict between peers and near-peers after the breakdown of deterrence, and exclude what the Joint Chiefs of Staff (2019) refer to as 'competition below armed conflict' (Morris et al., 2019).

3. MULTI-DOMAIN OPERATIONS AND CYBER

The historical origins of the multi-domain operations warfighting concept are rooted in the US Army's AirLand Battle doctrine, first introduced in 1982 (Skinner, 1988). This multi-dimensional doctrine, updated in 1986 and 1993, focused on integrated, joint air and ground manoeuvre supported by long-range precision-guided munitions to defeat Soviet forces in Central Europe. NATO adopted the tenets of AirLand Battle for its Follow-On-Forces Attack Concept. AirLand Battle was considered an important contributing factor in the overwhelming allied victory during Operation Desert Storm in 1991 (Paquin, 1999), which was, in turn, instrumental in shaping the Chinese People's Liberation Army's (PLA) perception of future warfighting, triggering doctrinal changes and a concerted modernisation effort (Defense Intelligence Agency, 2019). However, Russian and Chinese military reforms in the 2000s—particularly the PLA's adoption of the 'informationised warfare' concept and Anti-Access/Area Denial (A2/AD) systems, Russian military modernisation efforts, and subsequent Russian operations in Ukraine in 2014—convinced US military leaders that AirLand Battle doctrine was obsolete. In 2015, Deputy Secretary of Defense Robert Work tasked the US Army with the development of 'AirLand Battle 2.0', which served as the institutional impetus to develop first the Multi-Domain Battle (MDB) concept and, subsequently, the MDO concept (McCoy, 2017; Johnson, 2018).

The importance of MDO for future NATO warfighting is twofold. Firstly, as the most comprehensive and advanced multi-domain concept of all US service branches, it is expected to constitute the foundational element of the new Joint Warfighting Concept for All-Domain Operations (Hoehn, 2020). Secondly, it is expected to influence the development of operational concepts and doctrine around multi-domain operations of NATO allies, in a similar manner to the influence of AirLand Battle on the Follow-On-Forces Attack Concept in the 1980s, although there are numerous capability gaps and policy challenges that need to be addressed first (Watling & Roper, 2019). According to the concept note, MDO has been developed to solve the problem of 'multiple layers of stand-off in all domains—and, sea, air, space and cyberspace — to separate US forces and our allies in time, space and function in order to defeat us'. The solution to this is:

> the rapid and continuous integration [emphasis added] of all domains of warfare to deter and prevail as we compete short

> of armed conflict. If deterrence fails, Army formations, operating as part of the Joint Force, penetrate and disintegrate enemy anti-access and area denial systems; exploit the resulting freedom of manoeuvre to defeat enemy systems, formations and objectives and to achieve our own strategic objectives; and consolidate gains to force a return to competition on terms more favourable to the U.S., our allies and partners (TRADOC, 2018: p. i, iii).

The underlying idea of MDO is thus deeper integration of capabilities across domains (also referred to as 'cross-domain synergy') to achieve convergence of time, space and capabilities to conduct independent manoeuvre and employ cross-domain fires including integrated kinetic and cyber strikes (TRADOC, 2018; Judson, 2020). Put otherwise, MDO is intended to accelerate the closing of the US Armed Forces' kill-chain, while simultaneously breaking the enemy's (Brose, 2020). Operational speed is vital in that regard and can only be guaranteed through the effective integration of separate battle networks into a system of systems architecture. Such an architecture will require sophisticated cyber defence and also narrow AI-enabled C2 capabilities to coordinate, deconflict and synchronise military operations across domains; for example, a coordinated and synchronised attack against an adversary C2 node via cyberspace, air and the electromagnetic spectrum. Cyberspace would thus not only be the key enabling domain for coordination and integration operations, but also an attack vector. Notably, in the US Air Force's Doolittle Series wargames, the centre of gravity for multi-domain operations was identified as the ability to create accurate and shared battlespace awareness, which, according to the joint force commander in the exercise, depended principally on protecting intelligence gathering systems and maintaining the security of C2 networks, both of which are dependent on cyberspace as their connector and integrator (Rothstein & Saltzman, 2019).

4. THREE REQUIREMENTS FOR EFFECTIVE INTEGRATION OF CYBER OPERATIONS INTO MULTI-DOMAIN OPERATIONS

There are numerous technical, organisational and doctrinal requirements necessary for the effective integration of cyber capabilities into multi-domain operations in future high-intensity warfighting scenarios. This section analyses the three judged to be most essential: an IoMT for effective cyber C2; integrated multi-domain formations; and a mission command doctrine based on decentralised decision-making and execution. All three countries discussed in this paper— the US, UK and Germany— are each working on at least one of the three requirements.

A. Technological

At the technological level, an IoMT is desired in combination with an AI-enabled C2 capability that enables the integration and synchronisation of cyber and kinetic strike capabilities in multi-domain operations. An IoMT is a network or system of interconnected computing devices including sensors, weapons platforms, and data storage resources (Russell, Abdelzaher & Suri, 2019). It would thus theoretically collect and create vast amounts of shareable data, which could be turned into actionable intelligence for cyberattack packages. The IoMT would also enable the fast transfer of cyberattack packages to, for example, aircraft to target enemy air-gapped systems via the radio frequency (RF) spectrum (Theohary & Hoehn, 2019). The overall synchronisation and integration of operations in other domains would also require an AI-enabled C2 architecture also called an AI-enabled battle management system embedded within an IoMT capable of presenting a commander a real-time common operating picture that would include a cyber and electromagnetic picture. In essence, an AI-enabled battle management system in comparison to a conventional battle management system relies on machine-learning algorithms to process big data from multiple sources for C2 decision support in order to expedite the so-called dynamic observe, orient, decide, and act (DOODA) loop cycle (Schubert et al., 2018).

An IoMT paired with an AI-enabled C2 capability would thus fulfil a key requirement of multi-domain operations: information superiority in order to enable faster and more effective decision-making in the battlespace. As one analysis notes:

> Effective cross-domain data-driven decision-making relies on a precision balance between the right amount of information, the right amount of time and the correct ability to execute a choice. It is here where the [IoMT] complex system-of-systems can deliver benefit to all the phases of decision-making, regardless of context (Russell, Abdelzaher & Suri, 2019: p. 729).

An IoMT may also enable a faster closing of the cyber kill-chain. Using the seven phases of the Intrusion Kill-Chain Model, an IoMT would have its greatest utility in the reconnaissance phase or in the faster identification and selection of targets during multi-domain operations facilitated through a common cyber and electromagnetic picture (Hutchins, Cloppert & Amin, 2010). Nevertheless, there remain various technical and security challenges that need to be addressed before such a system can be operationalised, including cryptographic security and the power it consumes from devices (thereby reducing their lifespan) (Sfar et al., 2018; Eversden, 2020); military cloud computing architectures that may not meet the demand of real-time or near real-time battlefield awareness at the edge of a network, to which fog computing may present a solution (Butler, 2018); and the sheer scale of integration of large military formations (Kott, Swami & West, 2016).

B. Organisational

At the organisational level, the effective integration of kinetic and cyber strike capabilities in high-intensity warfighting scenarios will require the creation of multi-domain field formations which integrate battlespace intelligence, surveillance, reconnaissance (ISR) assets such as unmanned combat aerial vehicles or low-earth orbit satellites with electronic and cyber warfare capabilities. This facilitates synchronised cyber operations in the tactical battlespace, and also fulfils the requirement of spatial proximity for tactical cyber operations via the RF spectrum (Schulze, 2020a). Theatre-wide cyber operations would require a delineation between tactical and strategic offensive cyber operations for battlespace management purposes. However, the multi-domain formation can be employed tactically or strategically. For example, a multi-domain unit could make use of either tactical or strategic intelligence assets (such as RF kit on the ground or a satellite) to gain access to a network and facilitate delivery of a cyber attack; and the effect achieved could also be either tactical or strategic. It may, for example, disrupt a surface-to-air battery or theatre-level C2. Conversely, while strategic offensive cyber operations would likely be authorised by national cyber commands elements of which could be embedded with a higher echelon formation, they could still be executed tactically. The multi-domain formation would also be responsible for cyber preparation of the battlespace; that is, it may perform activities akin to intelligence preparation of the battlespace, including the probing of enemy networks, assessment of cyber defences and the assembly of attack packages. Moreover, any cyber operation needs adequate preparation time. This is known as the ‘cold-start’ problem (Schulze, 2020a). As Matthias Schulze notes, offensive cyber operations, require:

> a huge logistical effort of keeping track of the status of implants and especially how different attack vectors are intertwined or depend on each other. High-value targets, such as critical infrastructures and command and control systems, are often air-gapped and require specialized intelligence to gain access. In many instances, this requires time-consuming social engineering in advance to gain a foothold on a system (Schulze, 2020a: pp. 188).

The successful integration of all cyber operations embedded within a multi-domain operating concept would be largely dependent on the close coordination of cyber operations between national cyber commands and tactical formations.

C. Doctrinal

At the doctrinal level, multi-domain operations require a mission command doctrine emphasising decentralised decision-making and decentralised pre-approved execution of integrated cyber strikes. Multi-domain operations, including offensive cyber operations, entail significant synchronisation and pre-planning. As several studies have noted, this can stand in fundamental tension with lower-level initiatives based on mission command as it prevents subordinates from seizing the initiative against the adversary at an opportune time in the battlespace:

> [if] the plan they [subordinates] are executing requires excessive synchronisation, then they will simply be unable to exploit these opportunities when they arise for fear of derailing the operation and preventing the convergence of effects' (Stafford, 2019: p. 96).

Should the technological capabilities for AI-enabled C2 sufficiently mature in the coming years, a mission command doctrine centred around decentralised planning and execution could nonetheless be realised under a multi-domain operating concept. In addition to an AI-enabled C2 ability to deconflict and synchronise operations across domains, key to an effective cyber mission command doctrine during multi-domain operations is pre-delegated authorisation to execute offensive cyberattacks at lower echelons of command. In a high-intensity warfighting environment, communication links to higher command or strategic cyber assets may be degraded and disrupted and individual commanders would have to have the appropriate C2 and authorisation to exploit opportunities in the cyber domain.

5. CASE STUDIES

The following three short case studies assess the current status of the three described technical, organisational, and doctrinal requirements for effective integration of offensive cyber capabilities into multi-domain operations.

A. United States

According to the forthcoming International Institute for Strategic Studies (IISS) comparative study of cyber military power, the US possesses the world's most advanced military offensive cyber capabilities. The US Armed Forces represent the primary driving force behind the adaptation of operational concepts based on multi-domain operations for high-intensity warfighting. It is thus unsurprising that it leads development in all three categories, and appears most advanced in integrating kinetic and cyber strike capabilities.

1) IoMT and AI-enabled C2 Capability

The US Department of Defense's (DoD) Joint All Domain Command and Control (JADC2) concept aims to integrate the separate tactical networks of the individual service branches of the US Armed Forces into one single network linking every sensor to every shooter across all levels in an IoMT. According to a recent Congressional briefing document, 'JADC2 envisions providing a cloud-like environment for the Joint force to share intelligence, surveillance and reconnaissance data, transmitting across many communications networks, to enable faster decision-making' (Hoehn, 2020). JADC2 envisions an AI-enabled C2 capability for military commanders similar to the ride-sharing service 'Uber' that provides real-time or near real-time situational awareness of the battlespace and lists available capabilities in all domains for the execution of mission sets. The DoD has tasked the US Air Force with delivering this technological capability in support of the JADC2 concept. For the past two years, it has been working on its Advanced Battle Management System (ABMS), which, according to a senior service official, represents the first attempt by DoD to 'build the Internet of Things for the military' (Hitchens, 2020a; Rivers, 2020). ABMS consists of a set of six systems all concurrently under development, ranging from cloud-based C2 and situational awareness applications to sensor integration. ABMS has caused controversy with other service branches as a potential future C2 platform for all services; for example, the US Army raised a concern that it will face network scaling issues (Hitchens, 2020b). The US Government Accountability Office (GAO) has also raised concerns over ABMS technology and cost (US Government Accountability Office, 2020). Nonetheless, ABMS has shown initial some potential for multi-domain operations in a number of recent demonstrations, including providing AI-enabled C2 support and a real-time common operating picture—two key requirements for effective integration of offensive cyber and kinetic operations across domains. While the specifics regarding the testing have not been made public, reports suggest that they were part of scenarios (Tucker, 2020; Hitchens, 2020c).

2) *Multi-Domain Formations*

The US Army's concept note on MDO specifically calls for the creation of multi-domain formations capable of independent manoeuvre and the employment of cross-domain fires (TRADOC, 2018). In 2018, the Army stood up its first experimental Multi-Domain Task Force, the principal mission of which is the degradation and penetration of Chinese and Russian A2/AD bubbles (Freedberg, 2019). The heart of this task force is a new Intelligence, Information Operations, Cyberspace, Electronic Warfare and Space Operations (ICEWS) battalion capable of defensive and offensive cyber operations as well as 'converging signals intelligence and electronic warfare as an operational capability and space surveillance and effects' (Thompson, 2019). Notably, the battalion is not part of the joint Cyber Mission Force of US Cyber Command, but rather falls under US Army Cyber Command (2020). Both the Army and Marine Corps have been establishing stand-alone offensive cyber units as part of their new multi-domain warfighting approaches, while the Navy and Air Force continue to provide all of their offensive teams directly to Cyber Command (Pomerleau 2019a; 2019b). The Army is also reorganising or creating new cyber and electromagnetic activities planning sections at various headquarters, and standing up entire new units such as the 915th Cyber Warfare Support Battalion (Stover, 2020). A GAO report (2019) highlights 'staffing, equipping, and training challenges' within such units. It is unclear how precisely these new tactical units will integrate with the Cyber Mission Force under US Cyber Command, and precisely what offensive cyber capabilities they will have their disposal. Tactical and strategic offensive cyber capabilities will be coordinated via Joint Force Headquarters-Cyber and cyberspace operations integrated planning elements (CO-IPEs) attached to regional combatant commands (US Army War College, 2020). However, the exact mechanism including speed of decision-making for this is not publicly known.

3) Mission Command Doctrine and Decentralised Execution of Offensive Cyber Operations

According to the Joint Doctrine on cyberspace operations, 'The complex nature of [cyber operations], where cyberspace forces can be simultaneously providing actions at the global level and the theatre or joint operations area level, requires adaptations to traditional C2 structures' (Joint Chiefs of Staff, 2018). The document simultaneously emphasises that the mission command method of 'centralized planning with decentralized execution of operations' also applies to cyber operations. An overview of the current planning processes for joint offensive cyber operations suggests that it will remain fairly centralised in the near term at the upper echelons of command (US Army War College, 2020). This is gradually changing, however. National Security Presidential Memorandum 13, which governs the conduct of offensive and active defensive cyber operations under the doctrine of 'persistent engagement' (Pomerleau, 2019c; Nakasone, 2020), is enabling a more decentralised planning and execution of cyber operations below the strategic level (National Security Agency, 2012). Individual service branches have also been experimenting with the delegation of command authority to lower echelons (Pomerleau, 2018). However, this likely only pertains to more limited RF spectrum cyber operations, which would be closer to electronic warfare operations than strategic offensive cyber operations (US Army War College, 2020). According to the MDO concept note, national- (i.e. US Cyber Command) and theatre-level offensive cyberspace operations would converge at the corps level in the pursuit of operational and tactical objectives (TRADOC, 2018). C2 for offensive cyber operations would thus continue to reside at the highest level of military command, for example, with the corps commander and the geographical and functional combatant commanders (Hofer, 2019). This could make it difficult for field commanders below to exploit opportunities in cyberspace in a degraded operational environment using the mission command tenets should the MDO concept officially be adopted into doctrine.

B. United Kingdom

The UK's understanding of multi-domain operations closely resembles that of the US, though on a smaller scale. Facing greater budgetary and manpower constraints, the UK has focused its efforts on the development of an 'agile' and 'integrated' cyber capability under the umbrella of what it refers to as 'Multi-Domain Integration' (Ministry of Defence, 2017b; Connell, 2020; Stronell & Gady, 2020). The British Ministry of Defence's new Integrated Operating Concept, unveiled in September 2020, emphasises the need for integration across all warfighting domains at the tactical level (Ministry of Defence, 2020a). According to the Ministry of Defence (2017a: p.1), British 'military activities increasingly need to incorporate the often subtle and ambiguous interplay between cyber electromagnetic and information activities which must be integrated, as required, with kinetic effects'. British officials have repeatedly acknowledged the challenge presented by multi-domain operations and there is significant evidence of adaptation within the British armed forces to the challenges presented (Carter, 2019; Sanders 2020).

1) IoMT and AI-Enabled C2 Capability

Statements by British officials and defence research institutions have recognised the importance both of an IoMT and AI-enabled C2 capability to the future multi-domain battlespace, though the development of capability appears to remain in the experimental stage in most cases (Poulter & Mackay, 2018; Royal Air Force, c.2020). There is no dedicated programme to create a battle management system integrating the separate service branches and their systems and platforms in an IoMT underpinned by AI-enabled C2 capability. However, the UK is in the process of developing a large-scale AI-enabled synthetic environment in order to aid in the development of course-of-action analysis. Such a tool could eventually evolve into an operational tool for such an AI-enabled C2 (The Economist, 2019; Warrell, 2020).

Overall, IoMT developments appear to remain relatively fragmented and platform-centred. One key focus is the development of the Future Combat Air System (FCAS) system-of-systems concept, headed by BAE Systems' Tempest, which seeks to connect sensors and shooters into an IoMT and includes the development of an 'air combat cloud' (Harper, 2019). In its Integrated Review and Air Space Proposition, the Royal Air Force (c.2020) emphasises that an IoMT that fuses and distributes data across domains is at the heart of its modernisation efforts: '[b]y harnessing information, fusing data on a cross-domain network of interconnected systems, we will achieve advantage over our adversaries and competitors'. The 'Intelligent Ship' programmes, funded by the UK's defence innovation accelerator, represent another example. One project aim is to 'enable integration and application of intelligence systems' while another is to develop and understand how 'complex networks of humans and machines can effectively team' (DASA, 2019). Both objectives seek to support an AI-enabled C2 capability. The UK Strategic Command has also championed the Integrated Warrior programme which seeks to work with academia and industry to develop new force structures, capabilities and new operating concepts for the future operating environment (Royal Navy, 2020).

2) Multi-Domain Formations

Three main institutional innovations characterise the UK's response to multi-domain operations. UK Strategic Command, established in February 2020, represents the most fundamental of these. Assuming the role of 'defence integrator', the Command's key innovation in relation to its predecessor is its aspiration to more effectively integrate cyber and space capabilities with the three classical warfighting domains, and to achieve seamless planning and execution of multi-domain operations at a pace that outstrips the UK's adversaries (Barry, 2020). Strategic Command succeeds UK Joint Forces Command, itself established in 2012 to integrate British key strategic level military capabilities more effectively. Official statements have repeatedly referred to the new Command as the British response to multi-domain challenges (Curtis 2019; Ministry of Defence, 2019b; 2020c; Sanders, 2020).

The UK National Cyber Force, which combines the cyber capabilities of the UK's technical intelligence agency, Government Communication Headquarters (GCHQ), with those of the Ministry of Defence also represents a relatively new innovation which is likely to assist the UK in multi-domain operations. By combining its military and intelligence cyber capabilities, the UK hopes to attain significant agility in cyberspace operations. As such, the role of Cyber Force is conceived very differently to that of US Cyber Command, intended to overcome inter-agency rivalry and the splintering of cyber capabilities across government present in the American system. Instead, different operations conducted by Cyber Force will fall under the purview of either the intelligence services or the military, depending on the nature of the operation (Stronell & Gady, 2020). Work towards the Force having first been announced in 2018, it is likely in the process of achieving institutional maturity, with its official inauguration likely to be announced in the coming months (The Telegraph, 2018; Sabbagh, 2020; Stronell & Gady, 2020).

The British Army's 6th Division, formed in August 2019, represents a third institutional response to multi-domain operations. The division, which replaced the combat support Force Troops Command, has been dubbed the British Army's 'hybrid warfare' branch by the media (Sengupta, 2019). Intended to provide the British Army with greater capability to defeat adversaries both above and below the threshold of conventional conflict, press releases describe the Division, which represents approximately one-fifth of the UK's Field Army, as tasked with 'cyber, electronic warfare, intelligence, information operations and unconventional warfare' (Ministry of Defence, 2019b; Warfare Today, 2019). The unit also includes the British Army's first 'cyber regiment', which appears to have capabilities for offensive cyber operations (Chuter, 2020). It is unclear how precisely the new unit will integrate with the National Cyber Force.

3) Mission Command Doctrine and Decentralised Execution of Cyber Operations

The British vision of 'Multi-Domain Integration' encompasses not only the three-armed services, but allied capabilities and civilian government organisations including the intelligence services. Capability integration, particularly at the national level, is seen as a force multiplier (Ministry of Defence, 2020a). According to the joint British doctrine for cyber and electromagnetic activities (CEMA), the British military envisions the integration of CEMA into the wider military as part of a full-spectrum approach (Ministry of Defence, 2018). There has been a progressively increased doctrinal emphasis on capability integration (including cyber and space) across the past several editions of capstone British doctrine and the latest joint doctrine note on cyber and electromagnetic activities emphasises the need for a cyber electromagnetic picture as part of a common operating picture to support future military operations for combined kinetic and cyber operations (Ministry of Defence, 2008; 2011; 2014; 2018). The UK is clearly turning its doctrinal focus to the development of a force structure compatible with this multi-domain, integrated operational concept (Sanders, 2020). The publication of the Integrated Operating Concept 2025 sheds considerable light on how the British government envisions the integration and use of UK cyber capabilities in multi-domain operations, anticipating integration of capabilities at the tactical as well as the operational level of war. The doctrine envisions an operational concept 'integrated across all five Operational Domains [...which] will change the way we operate and war fight and the way we develop capability' (Ministry of Defence, 2020a).

Mission command and decentralised execution of offensive cyber strikes were both used during operations against terrorist organisations (Blitz, 2013; Bond, 2018; Stronell & Gady, 2020). In a concept note on future C2 design, the Ministry of Defence (2017a: p.6) stresses that it has to meet the 'enduring requirement for mission command'. However, in a key point of departure from US practice, British practitioners possess an engrained scepticism of the necessity of granting the autonomy to launch cyber operations to tactical-level units. There is also an overall resistance to the tactical-strategic distinction as regards the prosecution of cyber operations. British officials are likely hopeful that an integrated national capability can provide the necessary tactical-level support to troops on the ground while maintaining the ability to achieve strategic effects. In keeping with longstanding British practice, authorisation for the prosecution of cyber operations (either individually or collectively) will likely remain with government ministers; namely, with the Foreign Secretary in peacetime and the Secretary of State for Defence in conflict situations (Stronell & Gady, 2020).

C. Germany

No operating concept around multi-domain operations yet exists in the German armed forces (Bundeswehr). The basic tenets of multi-domain operations, however, have been outlined in various official documents discussing future warfighting and force modernisation (Kommando Heer, 2018). Indeed, according to a Bundeswehr official, multi-domain operations are an integral part of operational planning within the armed forces (Gady, 2020b). While the Bundeswehr Cyber and Information Domain Service possesses a burgeoning offensive cyber military capability, there is little publicly available information about efforts to integrate cyber and kinetic strike capability for high-intensity warfare.

1) IoMT and AI-enabled C2 Capability

An IoMT and AI-enabled C2 capability remain aspirational for the Bundeswehr for the time being. While it has identified an IoMT as part of a set of capabilities needed for generating 'AI-supported quality data' as part of its digitalisation strategy for German land forces (Bundeswehr, 2020: p.2), no funded programme has yet been established. In the near term, German efforts (in collaboration with the Netherlands) for a new battle management system are focused on the Tactical Edge Network (TEN) programme, which is expected to enter service with the German Army in 2023 (Leidenberger et al., 2020). The underlying battle control software, SitaWare Frontline, is not AI-enabled (Defense-Aerospace, 2019). According to state-owned IT service provider BWI, TEN will be a building block of the IoMT and a sensor-to-shooter concept, which will presumably include an AI-enabled C2 capability (Leidenberger et al., 2020). It remains unclear to what degree there are plans to integrate the Bundeswehr Cyber and Information Domain Service, including its offensive cyber capabilities, into such an IoMT. The Bundeswehr has historically encountered difficulties in creating a joint operating picture across services, let alone domains (Dyson, 2011). Within the Cyber and Information Domain Service, however, some AI-enabled operating picture capabilities have been in development since 2016 (BWI, 2020). For the time being, IoMT efforts appear fragmented and platform-focused. For example, in cooperation with Spain and France, Germany is co-developing the Future Combat Air System (FCAS), a system-of-systems (an IoMT) underpinned by a tactical cloud, with an AI-enabled C2 capability (Gros, 2019). The FCAS is expected to enter service in the 2040s. In cooperation with France, Germany is also developing a Main Ground Combat System—a multiplatform concept based on a system-of-systems architecture expected to be deployed in the mid-2030s. Overall, there appears to be no coordinated technological-level effort towards the integration of cyber and kinetic strike capabilities for multi-domain operations set in a high-intensity warfighting scenario within the Bundeswehr.

2) *Multi-Domain Formations*

The Bundeswehr has not established any multi-domain formations for conducting offensive cyber operations, and according to the Cyber and Information Domain Service, there are no existing plans to deploy such formations in the future (Gady, 2020a). Germany only recently established an independent military cyber force, the Bundeswehr Cyber and Information Domain Service, which became operational in 2017, and is loosely modelled on US Cyber Command and its cyber forces. The service consolidates around 14,000 civilian and military personnel divided up into various units and commands, with the majority of formations consisting of electronic warfare and IT-support battalions. Military cyber capabilities are situated within the Centre for Cyber Defence and Centre for Cyber Operations, which is also responsible for conducting offensive cyber operations. The eventual manpower of these two centres is expected to reach 600, with around 100 civilian and military personnel assigned to the Centre for Cyber Operations (Bundesministerium der Verteidigung, 2016; Gady, 2020b). The Bundeswehr intends to deploy Cyber-Information-Domain (CID) teams with individual services and units to act as liaisons and advisors to military commanders. Offensive cyber operations, however, would still be centrally executed through the 'Reach-Back-Verfahren' (reach back procedure) by the Cyber and Information Domain Service (Gady, 2020a). According to a statement by the German Defence Ministry, the main objective of offensive cyber operations will be the attainment of 'information dominance' in the cyber and information spaces to support an accelerated decision-making cycle during kinetic operations (Bundesministerium der Verteidigung, 2017). One likely reason for the absence of multi-domain formations akin to the US Army's cyber battalions or the British Army's 'cyber regiment' is that a Bundeswehr cyber unit would suffer from limited utility at the outset of any high-intensity warfighting scenario since it would likely be legally difficult to conduct cyber preparations of the battlespace without the direct authorisation of the German parliament before the outbreak of hostilities (Schulze, 2020c). While under emergency situations parliamentary consent to military operations can be given retroactively (as long as this is preceded by informing select members of the Bundestag's Defence Committee), it is unclear whether this could apply to cyber preparations of the battlespace, which could require many months of runup time prior to the commencement of hostilities.

3) Mission Command Doctrine and Decentralised Execution of Offensive Cyber Operations

Germany does not possess an official cyber military doctrine. According to recent research, doctrinal discussions on the use of offensive cyber capabilities are found in various government documents, but they are generally vague and offer little guidance about their deployment (Schulze, 2020b). In comparison to British and American legislative institutions, the Bundestag enjoys extended powers over operational matters, including rules of engagement and C2 (Dyson, 2011), underscoring the inhibited decision-making autonomy of the Bundeswehr in the cyber domain. Strong civilian oversight also incentivises more direct control of offensive cyber operations by higher echelons of military command within the armed forces. This stands in tension with the Bundeswehr Networked Operational Command Doctrine (Vernetzte Operationsführung), which aims to create a networked warfighting approach underpinned by mission command (Bundesministerium der Verteidigung, 2017). According to one 2011 study exploring the digitisation of the Bundeswehr, 'the practical experience of digitisation in exercises has led to the temptation for commanders to involve themselves in the 'tactical weeds' [and] networking has been accompanied by enhanced accountability'. The result, according to the study, is that tactical decisions are taken at higher echelons of command. Referring to actual operational experiences from Afghanistan, the study further notes that 'commanders are gathering inappropriate levels of information and are being pulled down to the detailed tactical level, to protect themselves from prosecution' (Dyson, 2011: p.7). All these factors will likely make it very difficult for German commanders to apply mission command, seize the initiative, and exploit opportunities in the battlespace through the combined use of kinetic and cyber capabilities during multi-domain operations. Nonetheless, according to the Cyber and Information Domain Service, cyber operations will be conducted by applying the tenets of mission command (Gady, 2020a). However, the service does caution that the specific characteristics of cyber operations need to be considered.

6. IMPLICATIONS FOR NATO

The three case studies assessing technical, organisational and doctrinal requirements for the effective integration of cyber and kinetic strike capabilities into multi-domain operational concepts in a high-intensity conflict yield several practical conclusions for the NATO alliance.

Firstly, as all three case studies illustrate, the integration of cyber and kinetic capabilities for multi-domain operations remains largely aspirational and at an experimental stage. Little public information exists about precisely how the armed forces of the three countries would execute synchronised cyber-kinetic strikes in a high-intensity conflict. The difficulties of effectively coordinating offensive cyber-kinetic strikes during multi-domain operations implies that they may principally be employed at the outset of a high-intensity conflict for high-value targets such as an enemy's national or theatre-wide C2 networks. Another contributing factor is the 'cold start' problem, and the need for adequate cyber preparation of the battlespace and possible quick depletion of cyber weapons arsenals (for example, malware and 0-day vulnerabilities). Consequently, NATO should have an enhanced focus during wargames and exercises on the initial stages of multi-domain operating in a high-intensity warfighting environment, and must consider to what degree and how offensive cyber capabilities are to be used by military commanders (Schneider, 2017).

Secondly, NATO needs to develop its own, separate doctrine on multi-domain operations. The US is leading the conceptual development of multi-domain operations, but allies must follow suit to adapt the concept to their own future capabilities, resources and requirements. The UK and Germany are in the early stages of doctrinal development, though the former is at a far more advanced stage. Nevertheless, separate national efforts will only go so far, and may impede unity of effort. To facilitate effective integration and interoperability between NATO member states, a clear doctrinal foundation for multi-domain operations should be developed. This would also assist in identifying and prioritising capability requirements among member states for the execution of multi-domain operations. A new multi-domain doctrine would also likely require updates to NATO's *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations* (NATO, 2020). In particular, it would require revision of the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism for offensive cyber operations (ibid.; Goździewicz, 2019).

Thirdly, clear technical requirements and standards for a common systems architecture that enables integration of separate battle management systems need to be established across NATO member states. Only a secure and interconnected battle management system paired with an AI-enabled C2 capability that includes a common cyber electromagnetic picture will be able to effectively integrate kinetic and cyber operations in a high-tempo warfighting environment. Such an effort could be modelled on NATO's Air Command and Control System Programme, or expand on the Dutch-German TEN programme (NATO, 2015). Different capabilities among NATO member states, the cost associated with multi-domain C2 systems, and classification challenges encountered when operating across NATO particularly with regards to cyber operations will make the integration of separate battle management systems a difficult proposition. Given that multi-domain operations inherently involve dependence on technological capabilities, strong AI-enabled cyber defences across the alliance will be an absolute necessity.

Fourthly, as the German case study clearly demonstrates, legal restrictions and domestic political considerations could prevent the effective use of multi-domain formations and offensive cyber operations in high-intensity conflict. Offensive cyber operations require preparation of the battlespace, which may be legally prohibited without a parliamentary mandate. To effectively execute synchronised operations under mission command principles would also require authorisation at lower echelons of command. Neither Germany nor the UK, however, appear eager to decentralise decision-making as regards the use of offensive cyber capabilities. Consequently, the alliance should encourage member states to specify detailed legal requirements for the execution of offensive cyber operations at all levels of command.

7. REFERENCES

Barry, B. (2020) 'New UK Strategic Command faces early challenges'. Military Balance blog, 19th June. London, International Institute for Strategic Studies. Available at: https://www.iiss.org/blogs/military-balance/2020/06/uk-strategic-command-challenges-covid-19 [Accessed: 1st August 2020].

Blitz, J. (2013) 'UK becomes first state to admit to offensive cyber-attack capability'. *Financial Times*, 29th September. Available at: https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de [Accessed: 1st August 2020].

Bond, D. (2018). 'UK reveals Isis target of first military cyber-attack'. *Financial Times*, 12th April. Available at: https://www.ft.com/content/cea9d608-3e3f-11e8-b7e0-52972418fec4 [Accessed: 1st August 2020].

Bonner, E. (2014) 'Cyber Power in 21st-Century Joint Warfare'. *Joint Force Quarterly*, 74, 3rd Quarter, 102-109. Available from: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_102-109_Bonner.pdf [Accessed: 1st August 2020].

Brose, C. (2020) *The Kill Chain: Defending America in the Future of High-Tech Warfare*. New York NY, Hachette Books.

Bundesministerium der Verteidigung. (2017) 'Strategische Leitlinie Digitalisierung'. Government report, March. Available at: https://www.bundeswehr.de/resource/blob/66394/4bbd6bd8e0fe81df975480a081bd1a37/20190703-strategische-leitlinie-digitalisierung-data.pdf [Accessed: 1st August 2020].

Bundesministerium der Verteidigung. (2016) 'Abschlussbericht Aufbaustab Cyber- und Informationsraum'. Government report, April. Available at: http://docs.dpaq.de/11361-abschlussbericht_aufbaustab_cir.pdf [Accessed: 1st August 2020].

Bundeswehr. (2020) 'Strategie Digitalsierung Land: Ein „DO IT-System für Entscheider'. Available at: https://www.bundeswehr.de/resource/blob/164082/597926df1b0c7941f755dda7589f1fc9/faltblatt-strat-digl-data.pdf [Accessed: 1st August 2020].

Butler, B. (2018) 'What is fog computing? Connecting the cloud to things.' *Network World*, 17th January. Available at: https://www.networkworld.com/article/3243111/what-is-fog-computing-connecting-the-cloud-to-things.html [Accessed: 1st August 2020].

BWI. (2020) ‘Von Big Data bis KI – Bundeswehr und BWI starten zweite Ausbaustufe des Gemeinsamen Lagezentrums CIR’. Blog, 1st September. Available at: https://www.bwi.de/news-blog/news/artikel/von-big-data-bis-ki-bundeswehr-und-bwi-starten-zweite-ausbaustufe-des-gemeinsamen-lagezentrums-cir [Accessed: 2nd September 2020].

Carter, N. (2019) ‘Chief of the Defence Staff [...] annual RUSI speech’. Speech transcript, 5th December. London, Ministry of Defence. Available at: https://www.gov.uk/government/speeches/chief-of-the-defence-staff-general-sir-nick-carters-annual-rusi-speech [Accessed: 1st August 2020].

Chuter, A. (2020). ‘British Army launches its first cyberwar regiment’. Defense News, 4th June. Available at: https://www.defensenews.com/global/europe/2020/06/04/british-army-launches-its-first-cyberwar-regiment/ [Accessed: 1st August 2020].

Clark, C. (2020) ‘Gen. Hyten on the New American Way of War: All-Domain Operations’. *Breaking Defense*, 18th February. Available from: https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/ [Accessed: 1st August 2020].

Connell, S. (2020) ‘Why protecting our nation is only possible through better collaboration’. Blog, 15th September. Northwood, UK Strategic Command. Available at: https://stratcommand.blog.gov.uk/2020/09/15/why-protecting-our-nation-is-only-possible-through-better-collaboration/ [Accessed: 15th September 2020].

Curtis, A. (2019) ‘Joint Forces Command to Become Strategic Command’. Commentary, 6th August. London, Royal United Services Institute. Available at: https://www.rusi.org/commentary/joint-forces-command-become-strategic-command [Accessed: 1st August 2020].

Defence and Security Accelerator [DASA]. (2019) ‘Competition document: intelligent ship - the next generation’. London, Ministry of Defence, 15th July. Available at: https://www.gov.uk/government/publications/competition-intelligent-ship-the-next-generation/competition-document-intelligent-ship-the-next-generation [Accessed: 1st August 2020].

Defense Intelligence Agency. (2019) *China Military Power: Modernizing a Force to Fight and Win*. Washington DC, Department of Defense. Available from: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [Accessed: 1st August 2020].

Defense-Aerospace. (2019) ‘SitaWare Frontline Chosen by German Armed Forces as BMS for VJTF(L) 2023’. *Systematic* press release, 12th December. Available at: https://www.defense-aerospace.com/articles-view/release/3/208209/bundeswehr-chooses-systematic-c2-software-for-vjtf.html [Accessed: 1st August 2020].

Deployable Training Division of the Joint Staff J7. (2020). *Mission Command*, January. Second edition. Insights and Best Practices Focus Paper. Suffolk VA, Joint Chiefs of Staff. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/missioncommand_fp_2nd_ed.pdf?ver=2020-01-13-083451-207 [Accessed: 1st August 2020].

Dyson, T. (2011) ‘Managing Convergence: German Military Doctrine and Capabilities in the 21st Century’. *Defence Studies*, June. 11 (2), 244-270. Available at: https://core.ac.uk/download/pdf/397643.pdf [Accessed: 1st August 2020].

Eversden, A. (2020) ‘DARPA wants stronger security for Internet of Things devices,’ 12th August. *C4ISRNET*. Accessed at: https://www.c4isrnet.com/

battlefield-tech/it-networks/2020/08/12/darpa-wants-stronger-security-for-internet-of-things-devices/ [Accessed: 1st September 2020].

Freedberg Jr., S. (2019) 'Army's Multi-Domain Unit 'A Game-Changer' In Future War'. *Breaking Defense*, 1st April. Available at: https://breakingdefense.com/2019/04/armys-multi-domain-unit-a-game-changer-in-future-war/ [Accessed: 1st August 2020].

Gady, F. (2020) Interview with German Cyber and Information Domain Service spokesperson, 25th September.

Gady, F. (2020) Interview with Bundeswehr spokesperson, 16th August.

Gerhartz, I. (2020) 'The Luftwaffe in Multi-Domain Operations'. *Journal of the JAPCC*. 30. Available at: https://www.japcc.org/the-luftwaffe-in-multi-domain-operations/ [Accessed 1st October 2020].

Goure, D. (2019) 'A New Joint Doctrine for an Era of Multi-Domain Operations'. *Real Clear Defense* [via TRADOC], 11th October. Available from: https://www.tradoc.army.mil/Publications-and-Resources/Article-Display/Article/1987883/a-new-joint-doctrine-for-an-era-of-multi-domain-operations/ [Accessed: 1st August 2020].

Government Accountability Office [GAO]. (2020) 'Defense Acquisitions: Action Is Needed to Provide Clarity and Mitigate Risks of the Air Force's Planned Advanced Battle Management System'. Report to Congressional Committees GAO-20-389 April. Washington DC. Available at: https://www.gao.gov/products/GAO-20-389 [Accessed: 1st August 2020].

Government Accountability Office [GAO]. (2019) 'Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping and Training of New Organizations'. Report to Congressional Committees GAO-19-570, August. Washington DC. Available at: https://www.gao.gov/products/gao-19-570 [Accessed: 1st October 2020].

Goździewicz, W. (2019) 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)'. *Cyber Defense Magazine*, 11th November. Available at: https://www.cyberdefensemagazine.com/sovereign-cyber/ [Accessed: 1st October 2020].

Gros, P. (2019) 'The "tactical cloud", a key element of the future combat air system'. Note 19/19, 2nd October. Paris, Fondation pour la recherche stratégique. Available at: https://www.frstrategie.org/en/publications/notes/tactical-cloud-key-element-future-combat-air-system-2019.

Harper, J. (2019) 'What to Expect from Sixth-Gen Aircraft'. *National Defense*, 16th September. Available at: https://www.nationaldefensemagazine.org/articles/2019/9/16/what-to-expect-from-sixth-gen-aircraft [Accessed: 1st August 2020].

Hitchens, T. (2020) 'ABMS Demos Speed New Capabilities to Warfighters'. *Breaking Defense*, 21st January. Available from: https://breakingdefense.com/2020/01/abms-demos-speed-new-capabilities-to-warfighters/ [Accessed: 1st August 2020].

Hitchens T. (2020) 'MDO Exclusive: Air Force Targets Primary Role in Joint C2'. *Breaking Defense*, 21st January. Available at: https://breakingdefense.com/2020/01/mdo-exclusive-air-force-targets-primary-role-in-joint-c2/ [Accessed: 1st August 2020].

Hitchens, T. (2020) 'ABMS Demo Proves AI Chops for C2'. *Breaking Defense*, 3rd September. Available at: https://breakingdefense.com/2020/09/abms-demo-proves-ai-chops-for-c2/ [Accessed: 5th September 2020].

Hoehn, J. (2020) 'Joint All Domain Command and Control (JADC2)'. Congressional briefing paper, 25th August. Washington DC, Congressional Research Service. Available at: https://fas.org/sgp/crs/natsec/IF11493.pdf [Accessed: 1st September 2020].

Hoehn, J. & Theohary, C. (2019) 'Convergence of Cyberspace Operations and Electronic Warfare'. Congressional briefing paper, 13th August. Washington DC, Congressional Research Service. Available at: https://fas.org/sgp/crs/natsec/IF11292.pdf [Accessed: 1st August 2020].

Hofer, M. (2019) 'The C2 of Cyberspace is a Mess!' *Proceedings of the US Naval Institute*, August. 145 (8). Available at: https://www.usni.org/magazines/proceedings/2019/august/c2-cyberspace-mess [Accessed: 1st September 2020].

Hutchins, E., Cloppert, M. & Amin, R. (2010) 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains' Lockheed Martin. Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed: 2nd October 2020].

Johnson, D. (2018) 'Shared Problems: The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle' Santa Monica CA, RAND Corporation, August. Available at: https://www.rand.org/pubs/perspectives/PE301.html [Accessed: 1st October 2020].

Joint Chiefs of Staff. (2019) 'Competition Compendium'. Joint Doctrine Note 1-19, 3rd June. Available from: https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf [Accessed: 1st August 2020].

Joint Chiefs of Staff. (2018) *Cyberspace Operations*, 8th June. Joint Publication 3-12. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf [Accessed: 1st August 2020].

Judson, J. (2020) 'Inside Project Convergence: How the US Army is preparing for war in the next decade'. *Defense News*, 10th September. Available at: https://www.defensenews.com/smr/defense-news-conference/2020/09/10/army-conducting-digital-louisiana-maneuvers-in-arizona-desert/ [Accessed: 15th September 2020].

Kommando Hier. (c.2018) 'Digitalisierung von Landoperationen'. Thesenpapier [Research Paper]. Available at: https://www.dwt-sgw.de/fileadmin/redaktion/SGW-Veranstaltungen/2018/8F7_Landoperationen/Thesenpapier_II_Digitalisierung_Landoperationen.pdf?fbclid=IwAR2_EkjXYoK-kQbMHNArC-K7ecyvjfCQfqQHXaAk80ITTnNE2rDckHttWsAI [Accessed: 1st August 2020].

Kommando Heer. (c.2017) 'Wie kämpfen Landstreitkräfte künftig?' Thesenpapier [Research Paper]. Available from: https://www.pivotarea.eu/wp-content/uploads/2017/09/OOO.pdf [Accessed: 1st August 2020].

Kostyuk, N. & Zhukov, Y. (2017) 'Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?' *Journal of Conflict Resolution*. 63 (2), 317-347. Available from: https://journals.sagepub.com/doi/abs/10.1177/0022002717737138 [Accessed: 1st August 2020].

Kott, A., Swami, A., West, B. (2016) 'The Internet of Battle Things'. *IEEE Computer*. 49 (12), 70-75. Available at: https://arxiv.org/ftp/arxiv/papers/1712/1712.08980.pdf [Accessed: 1st August 2020].

Leidenberger, F., Trampert, M., Bonnen, H. & Haber, T. (2020) 'BWI – Unterstützer der Digitalisierung der Bundeswehr'. *Wehrtechnische Report*. 17-19. Available at: https://esut.de/wp-content/uploads/2020/05/IT_REPORT_2020.pdf [Accessed: 1st September 2020].

Martelle, M. (2020) ‘USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY’. Briefing Book 693 21st January. Washington DC, National Security Archive. Available at: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony [Accessed: 1st October 2020].

Martelle, M. (2018) ‘Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command’s Internet War Against ISIL’. Briefing Book 637 13th August. Washington DC, National Security Archive. Available at: https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil [Accessed: 1st October 2020]

McCoy, K. (2017) ‘The Road to Multi-Domain Battle: An Origin Story’. West Point NY, Modern War Institute at West Point, 27th October. Available at: https://mwi.usma.edu/road-multi-domain-battle-origin-story/ [Accessed: 1st August 2020].

Metcalf, A. & Barber, C. (2014) ‘Tactical Cyber: How to Move Forward’. *Small Wars Journal*, 14th September. Available from: https://smallwarsjournal.com/jrnl/art/tactical-cyber-how-to-move-forward [Accessed: 1st August 2020].

Ministry of Defence. (2020) ‘The Integrated Operating Concept 2025,’ 30th September. Available at: https://www.gov.uk/government/publications/the-integrated-operating-concept-2025 [Accessed: 1st October 2020].

Ministry of Defence. (2020) ‘HMS TAMAR and RAF WYTON Read Outs’. Press release, 16th September. London, Directorate Defence Communications [email].

Ministry of Defence. (2020) ‘Visions for Strategic Command outlined during inaugural RUSI Conference’. Press release, 20th February. Available at: https://www.wired-gov.net/wg/news.nsf/print/Visions+for+Strategic+Command+outlined+during+inaugural+RUSI+Conference+20022020151515 [Accessed: 1st August 2020].

Ministry of Defence. (2019) ‘Joint Forces Command to Strategic Command, the journey’. Press release, 9th December. Northwood, UK Strategic Command. Available at: https://www.gov.uk/government/news/joint-forces-command-to-strategic-command-the-journey [Accessed: 1st August 2020].

Ministry of Defence. (2019) ‘Army restructures to confront evolving threats’. Press release, 1st August. Available at: https://www.gov.uk/government/news/army-restructures-to-confront-evolving-threats [Accessed: 15th August 2020].

Ministry of Defence. (2018) ‘Cyber and Electromagnetic Activities’. Joint Doctrine Note 1/18, February. Shrivenham, Development, Concepts and Doctrine Centre. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf [Accessed: 1st August 2020].

Ministry of Defence. (2017) ‘Future of Command and Control’. Joint Concept Note 2/17, September. Shrivenham, Development, Concepts and Doctrine Centre. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643245/concepts_uk_future_c2_jcn_2_17.pdf [Accessed: 10th September 2020].

Ministry of Defence. (2017) ‘Future Force Concept’. Joint Concept Note 1/17, July. Shrivenham, Development, Concepts and Doctrine Centre. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/

uploads/attachment_data/file/643061/concepts_uk_future_force_concept_jcn_1_17.pdf [Accessed: 1st August 2020].

Ministry of Defence. (2014) 'UK Defence Doctrine'. Joint Doctrine Publication 0-01, November. Shrivenham, Development, Concepts and Doctrine Centre. Fifth edition. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf [Accessed: 1st August 2020]

Ministry of Defence. (2011) 'British Defence Doctrine'. Joint Doctrine Publication 0-01, November. Shrivenham, Development, Concepts and Doctrine Centre. Fourth edition. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf [Accessed: 1st August 2020].

Ministry of Defence. (2008) 'British Defence Doctrine'. Joint Doctrine Publication 0-01, August. Shrivenham, Development, Concepts and Doctrine Centre. Third edition.

Morris, L., Mazarr, M., Hornung J., Pezard, S., Binnendijk, A. & Kepe, M. (2019) *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. Santa Monica CA, RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR2942.html [Accessed: 1st August 2020].

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

Nakasone, P. (2020) 'Statement of [...] Commander United States Cyberspace Command before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities,' 4th March. Washington DC, United States Congress. Available at: https://www.congress.gov/116/meeting/house/110592/witnesses/HHRG-116-AS26-Wstate-NakasoneP-20200304.pdf [Accessed: 1st August 2020].

National Security Agency [NSA]. (2012) 'Presidential Policy Directive 20'. PPD-20. Washington DC, Department of Defense. Available at: https://fas.org/irp/offdocs/ppd/ppd-20.pdf [Accessed: 1st August 2020].

NATO. (2020) *AJP-3.20: Allied Joint Doctrine for Cyberspace Operations*. Edition A. Version 1, January. Brussels. 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 24th November 2020].

NATO. (2015) 'NATO Air Command and Control System (ACCS)' 24th September. Available at: https://www.nato.int/cps/en/natohq/topics_8203.htm [Accessed: 1st August 2020].

Paquin, R. (1999) 'Desert Storm: Doctrinal AirLand Battle Success or "The American Way of War"'. Monograph. Fort Leavenworth KS, School of Advanced Military Studies, United States Army Command and General Staff College. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a370380.pdf [Accessed: 1st August 2020].

Pomerleau, M. (2019) 'The Navy will build tactical cyber teams'. *Fifth Domain*, 6th December. Available at: https://www.fifthdomain.com/dod/navy/2019/12/06/the-navy-will-build-tactical-cyber-teams/ [Accessed: 1st August 2020].

Pomerleau, M. (2019) 'How the Air Force has reorganized its cyber staff'. *Fifth Domain*, 20th September. Available at: https://www.fifthdomain.com/newsletters/digital-show-daily/2019/09/20/how-the-air-force-has-reorganized-its-cyber-staff/ [Accessed: 1st August 2020].

Pomerleau, M. (2019) 'New authorities mean lots of new missions at Cyber Command'. *Fifth Domain*, 8th May. Available at: https://www.fifthdomain.com/dod/cybercom/2019/05/08/new-authorities-mean-lots-of-new-missions-at-cyber-command/ [Accessed: 1st August 2020].

Pomerleau, M. (2018) 'How the Army will infuse cyber operations on the battlefield'. *Fifth Domain*, 5th July. Available at: https://www.fifthdomain.com/dod/army/2018/07/05/how-the-army-will-infuse-cyber-operations-on-the-battlefield/ [Accessed: 1st August 2020].

Poulter, A., Mackay, M. (2018) 'The Internet of Military Things'. Slideshow, 3rd July. Salisbury, Defence Science and Technology Laboratory [DSTL]. Available at: https://www.c-iot.ecs.soton.ac.uk/sites/www.c-iot.ecs.soton.ac.uk/files/AndrewPoulter.pdf [Accessed: 1st August 2020].

Rivers, B. (2020) 'Air Force to Integrate 'Project Maven' AI Scope into ABMS; Will Roper Quoted'. *Executive Gov*, 11th August. Available at: https://www.executivegov.com/2020/08/air-force-to-integrate-project-maven-ai-scope-into-abms-will-roper-quoted/ [Accessed: 10th September 2020].

Rothstein, M. & Saltzman. B. (2019) 'Multi-Domain Operations'. Doolittle Series 18. LeMay Paper 3. Montgomery AL, LeMay Center for Doctrine Development and Education. Available at: https://www.airuniversity.af.edu/Portals/10/AUPress/Papers/LP_0003_Multi_Domain_Operations.pdf [Accessed: 1st October 2020].

Royal Air Force. (c.2020) 'Integrated Review Air & Space Proposition'. RAF Astra.

Royal Navy. (2020) 'Royal Navy backs MoD Initiative to see Defence and Industry work Closer'. Press release, 28th February. Available at: https://www.royalnavy.mod.uk/news-and-latest-activity/news/2020/february/28/200228-integrated-warrior [Accessed: 1st August 2020].

Russell, S., Abdelzaher, T. & Niranjan, S. (2019) 'Multi-Domain Effects and the Internet of Battlefield Things'. *MILCOM 2019: 2019 IEEE Military Communications Conference*. 724-730. Available at: https://ieeexplore.ieee.org/document/9020925/ [Accessed: 1st August 2020].

Sabbagh, D. (2020) 'UK to launch specialist cyber force able to target terror groups.' The Guardian, 27th February. Available at: https://www.theguardian.com/technology/2020/feb/27/uk-to-launch-specialist-cyber-force-able-to-target-terror-groups [Accessed: 1st August 2020].

Sanders, P. (2020) 'Commander Strategic Command [...] Speech at the Air and Space Power Conference,' 15th July. Speech transcript. Northwood, UK Strategic Command. Available at: https://www.gov.uk/government/speeches/commander-strategic-command-general-sir-patrick-sanders-speech-at-the-air-and-space-power-conference [Accessed: 1st August 2020].

Schneider, J. (2017) 'Cyber and Crisis Escalation: Insights from Wargaming'. Draft research paper. Newport RI, United States Naval War College. Available at: https://paxsims.files.wordpress.com/2017/01/paper-cyber-and-crisis-escalation-insights-from-wargaming-schneider.pdf [Accessed: 1st August 2020].

Schubert, J., Brynielsson, J., Nilsson, M. & Svnmarck, P. (2018), 'Artificial Intelligence for Decision Support in Command and Control Systems'. *ICCRTS 2018: 23rd International Command and Control Research and Technology Symposium*, November. Available at: https://www.foi.se/download/18.41db20b3168815026e010/1548412090368/Artificial-intelligence-decision_

FOI-S--5904--SE.pdf [Accessed: 24th November 2020].

Schulze, M. (2020a) Cyber in War: Assessing the Strategic, Tactical and Operational Utility of Military Cyber Operations. In: Jančárková, T., Lindström, L., Signoretti, M., Tolga, I., & Visky G. (eds.) 20/20 Vision: The Next Decade. 12th International Conference on Cyber Conflict. Tallinn, Estonia, NATO Cooperative Cyber Defence Centre of Excellence. Available at: https://ccdcoe.org/uploads/2020/05/CyCon_2020_10_Schulze.pdf [Accessed: 1st September 2020].

Schulze, M. (2020b) 'Militärische Cyber-Operationen: Nutzen, Limitierungen und Lehren für Deutschland'. Stiftung Wissenschaft und Politik. Berlin, SWP-Studie 15, 15th August. Available at: https://www.swp-berlin.org/publikation/militaerische-cyber-operationen/ [Accessed: 16th August 2020].

Schulze M. (2020c). 'German Military Cyber Operations are in a Legal Gray Zone'. *Lawfare*, 8th April. Blog. Available at: https://www.lawfareblog.com/german-military-cyber-operations-are-legal-gray-zone [Accessed: 1st August 2020].

Sengupta, K. (2019) 'Army to form new hybrid-warfare division'. *The Independent*, 1st August. Available at: https://www.independent.co.uk/news/uk/home-news/uk-army-hybrid-warfare-division-conflict-intelligence-cyber-a9030281.html [Accessed: 1st August 2020].

Sfar, A., Natalizio, E., Challal, Y. & Chtourou, Z. (2018) 'A roadmap for security challenges in the Internet of Things'. *Digital Communications and Networks*. 4 (2), 118-137. Available at: https://doi.org/10.1016/j.dcan.2017.04.003 [Accessed: 1st August 2020].

Skinner, D. (1988) 'Airland Battle Doctrine'. Professional Paper 463 September. Alexandria VA, Center for Naval Analyses. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a202888.pdf [Accessed: 1st August 2020].

Smeets, M. (2018) 'Integrating offensive cyber capabilities: meaning, dilemmas and assessment'. *Defence Studies*, 14th August. 18 (4), 395-410. Available at: https://doi.org/10.1080/14702436.2018.1508349 [Accessed: 1st August 2020].

Stafford, N. (2019) 'The Alliance Strikes Back: Using Multi-Domain Operations to Counter Russian Hybrid Warfare in the Baltics'. Master's thesis. Fort Leavenworth KS, United States Army Command and General Staff College. Available at: https://apps.dtic.mil/sti/pdfs/AD1105226.pdf [Accessed: 1st August 2020].

Stover, S. (2020) 'Battalion helping shape Army tactical capabilities in the information environment'. US Army, 30th January. Available at: https://www.army.mil/article/231091/battalion_helping_shape_army_tactical_capabilities_in_the_information_environment [Accessed: 1st August 2020].

Strange, J. & Iron, R. (2004) 'Center of Gravity: What Clausewitz Really Meant'. *Joint Force Quarterly*. 35, 20-27. Available from: https://apps.dtic.mil/dtic/tr/fulltext/u2/a520980.pdf [Accessed: 1st August 2020].

Stronell, A. & Gady, F. (2020) Interviews with former British intelligence official, 14th September – 2nd October.

Taylor, C. & Kay, L. (2019) 'Putting the Enemy between a Rock and a Hard Place: Multi-Domain Operations in Practice'. West Point NY, Modern War Institute at West Point, 27th August. Available from: https://mwi.usma.edu/putting-enemy-rock-hard-place-multi-domain-operations-practice/ [Accessed: 1st August 2020].

The Economist. (2019) ‘Artificial intelligence is changing every aspect of war,’ 7th September. Available at: https://www.economist.com/science-and-technology/2019/09/07/artificial-intelligence-is-changing-every-aspect-of-war [Accessed: 1st October 2020].

The Telegraph. (2018) ‘Britain steps up cyber offensive with new £250m unit to take on Russia and terrorists,’ 21st September. Available at: https://www.telegraph.co.uk/news/2018/09/21/britain-steps-cyber-offensive-new-250m-unit-take-russia-terrorists/ [Accessed: 1st August 2020]..

Thompson, E. (2019) ‘I2CEWS’. Factsheet, 1st October. Atlanta GA, Defense Visual Information Distribution Service [DVIDS]. Available at: https://www.dvidshub.net/news/353065/i2cews-factsheet [Accessed: 1st August 2020].

Townsend, S. (2019) ‘Defining the ‘Domain’ in Multi-Domain’. *Joint Air and Space Power Conference 2019: Shaping NATO for Multi-Domain Operations of the Future*. 7-12. Available at: https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf [Accessed: 30th September 2020].

Tucker, P. (2020) ‘The Air Force’s ‘Connect Everything’ Project Just Had a Big Success’. *Defense One*, 11th September. Available at: https://www.defenseone.com/technology/2020/09/air-forces-connect-everything-project-just-had-big-success/168407/ [Accessed: 12th September 2020].

United States Army War College. (2020) *Strategic Cyberspace Operations Guide*, 1st June. Carlisle PA, Center for Strategic Leadership. Available at: https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf [Accessed: 1st August 2020].

US Army Cyber Command. (2020) ‘Cyber Mission Force’. Factsheet, 10th February. Washington DC, Department of Defense. Available at: https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/ [Accessed: 1st August 2020].

US Army Training and Doctrine Command [TRADOC]. (2018) ‘The US Army in Multi-Domain Operations 2028’. TRADOC Pamphlet 525-3-1, 6th December. Fort Eustis VA, US Army. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf [Accessed: 1st August 2020].

US Army Training and Doctrine Command [TRADOC]. (December 2017) ‘Multi-Domain Battle: Evolution of Combined Arms for the 21st Century, 2025-2040’. Version 1.0. Available from: https://www.tradoc.army.mil/Portals/14/Documents/MDB_Evolutionfor21st%20(1).pdf [Accessed: 1st August 2020].

US Cyber Command. (2017) ‘USCYBERCOM 120-Day Assessment of Operation GLOWING SYMPHONY: Executive Summary’. Internal report, 12th April. Washington DC, Department of Defense. Available at: https://nsarchive.gwu.edu/dc.html?doc=6655597-National-Security-Archive-6-USCYBERCOM [Accessed: 1st October 2020].

US Cyber Command. (2016). ‘USCYBERCOM 30-Day Assessment of Operation GLOWING SYMPHONY: Executive Summary’. Internal report, 13th December. Washington DC, Department of Defense. Available at: https://nsarchive.gwu.edu/dc.html?doc=6655596-National-Security-Archive-5-USCYBERCOM [Accessed: 1st October 2020].

Warrell, H. (2020) ‘Covid-19 crisis accelerates UK military’s push into virtual war gaming’. *Financial Times*, 19th August. Available at: https://www.ft.com/content/ab767ccf-650e-4afb-9f72-2cc84efa0708 [Accessed: 1st October 2020].

Warfare Today. (2019) ‘British Army Launches New 6th Division: Specialist Brigades Group to Deliver Cutting-Edge Capability,’ 1st August. Available at: http://www.warfare.today/2019/08/01/british-army-launches-new-6th-division/ [Accessed: 1st August 2020].

Watling, J. & Roper, D. (2019) ‘European Allies in US Multi-Domain Operations’. Occasional Paper, October. London, Royal United Services Institute. Available at: https://rusi.org/sites/default/files/20190923_european_allies_in_us_multi-domain_operations_web.pdf [Accessed: 1st August 2020].