National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Multi-Domain Operations in the Defeat of Russian Fires: A Way Forward

Major Andrew D.J. Curr

JCSP 47

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 47

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 47 – PCEMI 47

2020 – 2021

MASTER OF DEFENCE STUDIES – MAÎTRISE EN ÉTUDES DE LA DÉFENSE

MULTI-DOMAIN OPERATIONS IN THE DEFEAT OF RUSSIAN FIRES: A WAY FORWARD

By Major A.D.J. Curr

"This paper was written by a candidate attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

« La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale. »

TABLE OF CONTENTS

ABSTRACT

Indirect fire systems are the Russian land forces' centre of gravity in war, and an encompassing strategy to neutralize their effect is required in any future conflict. Russian indirect fires systems have played a central role in the last century and continue to dominate the operational landscape in today's conflict. This paper aims to analyze Russian indirect fire systems vulnerabilities and develop strategies to negate their impact in any future dispute using a multi-domain approach.

Russian indirect fire systems are not the dominating force on the battlefield but rather an extremely fragile and brittle system. They are vulnerable to many vectors of attack using an individual domain approach or multiple domains in synchronization. The attack vectors chosen within this paper illuminate a vulnerability, but by no means is this an exhaustive list. Instead, the vectors selected show just how vulnerable the indirect fire systems are in a multi-domain environment and are a liability rather than security for Russian land warfare doctrine.

Finally, in examining the results of what is possible in a multi-domain environment, a quick examination of where Western allied forces are capability-wise, emphasizing Canada's current and future capacity, was conducted. This final detail demonstrates that while the vulnerabilities exist in Russian indirect fire systems, the Western-allied partners need to continue to invest and modernize to capitalize on this emerging doctrine.

INTRODUCTION

The indirect fire (IDF) threat posed by the Russian Armed Forces in a conventional war is exceptionally high to friendly forces. Russian forces prize their long-range tube and rocket systems as the lynchpin to success on the battlefield, and the West must prepare to counter this war-winning capability. Traditionally, the Western-allied powers would envision achieving this using the Air/Land Battle doctrine. However, these templates will no longer work in the modern environment against a near-peer/peer adversary. Multi-domain operations are the future of warfighting. When targeted explicitly against the critical assets of Russian land forces, it will prove devastating in its ability to negate any Russian advantage on the battlefield.

Neutralizing the advantage of the long-range tube and rocket artillery within any future Russian anti-access area-denial environment will be critical to Western allies' success. Far from being the dominant and monolithic presence that must cause pause and concern amongst forces, the Russian IDF system is ripe for exploitation and negation. Years of modernization and the introduction of new technology enablers such as uncrewed aerial vehicles (UAVs) have demonstrated the weakness in the Russian order of battle. Using a multi-domain operations (MDO) approach, harnessing all five domains to achieve an effect, Russian IDF systems are a liability to be exploited rather than an asset to be feared.

This thesis is an illustration of the potential of multi-domain operations when approaching the Russian indirect fires threat. While specifically engaging in a thought experiment against the IDFD threat, it is entirely plausible and possible to extrapolate the same types of vulnerabilities and avenues of exploitation and applying them to other

Russian systems or using them against altogether different adversaries. The objective is not to demonstrate an actual method of attack but rather to illustrate the immense potential against an adversary. The Russian IDF threat is real but brittle, intractable, and vulnerable to allies' efforts.

The first chapter in this paper is an introduction to multi-domain operations. I will illustrate what comprises the five distinct domains and how each is an integral part of MDO. I also examine how MDO is different from previous doctrinal templates, like Air/Land Battle, and why this is important. Additionally, I describe the goal of MDO, which is to create convergence windows, where one or more domains achieve localized superiority and temporary advantage. Lastly, I will explain the necessity of not only thinking jointly but thinking in a multi-domain manner. The shift in mindset from one service or domain to a pan-domain structure is necessary for future operations.

In the second chapter, I examine Russian doctrine. I briefly surmise Russian doctrine en masse to describe the fundamental difference between Western and Russian doctrine. Following this examination, I describe the transformation and revitalization of Russian indirect fires systems and how this has influenced their approach to conflict. Lastly, I look briefly at the contemporary use of Russian IDF in the Ukrainian/Russian war in the Donbas Region of Ukraine in 2015. The critical element of this chapter is understanding the importance of IDF within Russian doctrine and some of the essential enablers it uses on the modern battlefield.

The third chapter analyzes several instances of using a multi-domain approach and the corresponding cases of highly vulnerable Russian IDF systems. This chapter examines the vulnerability of Russian communications, indirect fire software and systems, counter-UAS strategies, the destruction of the physical cannons or rockets themselves, and the reliance on space-based capabilities. Lastly, this chapter concludes with an examination of the importance of network integration that enables all MDO. This chapter examines several avenues of attack that could defeat the Russian IDF system, but it is not exhaustive, far from it. Even in the examination of IDF systems, applied in the same manner to any aspect of Russian military operations, these processes and attacks are applicable.

The fourth chapter examines the current capabilities of Canada, the United States and its allied partners to carry out such types of operations. This examination uses the five domains as a starting point to determine how capable the allied forces are and the current level of network integration. This chapter naturally flows into the fifth and final chapter, examining how prepared Canada is to conduct MDO. The final chapter looks into current capabilities and thoughts and the next bound in procurement and experimentation.

CHAPTER ONE - MULTI-DOMAIN OPERATIONS

Multi-domain operations is a new type of warfare conceived following the examination of modern warfare's strategic, operational and tactical realities by US and allied forces. As initially envisioned in the US Army White Paper on Multi-Domain Battlespace:

> Through credible forward presence and resilient battle formations, future ground and maritime forces integrate and synchronize joint, interorganizational and multinational capabilities to create temporary windows of superiority across multiple domains and throughout the depth of the battlefield to seize, retain, and exploit the initiative; defeat enemies; and achieve military objectives.[1]

A new series of tactics are required to close with and engage the enemy when faced with increased stand-off and efficacy of adversarial weapons systems. Integration of the three traditional domains, land, air, and sea, with the burgeoning domains of space and cyber, promotes increased effects when layered, synchronized, and fully enabled. MDO relies on doctrinal principles of cooperation and service synchronization as a solid foundation. While there is a great debate on whether MDO is genuinely a new form of doctrine within military and academic circles or whether MDO is Air/Land Battle revitalized with the incorporation of cyber and space operations. This debate is not for this review but, the underpinning of MDO is Air/Land battle, with the conceptual framework of modern, joint, and agile networked forces.[2]

[1] US Army Training and Doctrine Command, *Multi-Domain Battle: Combined Arms for the 21st Century*, Draft Version 0.53, (Kansas City: US Army Training and Doctrine Command, 2016), 6, https://community.apan.org/wg/aucoi/jadcc/m/mediagallery1/178247

[2] Wojtowicz, Tomas, “Multi-Domain Battle: New Doctrine of the United States Armed Force,” *Zeszyty Naukowe Akademii Sztuki Wojennej 112(3), 69. DOI: 10.5604/01.3001.0013.0879 https://www.researchgate.net/publication/331696091_MULTI-DOMAIN_BATTLE_NEW_DOCTRINE_OF_THE_UNITED_STATES_ARMED_FORCES*

Envisioned as a counter to Russian and Chinese Anti-Access/Area Denial (A2/AD) capabilities and doctrine, the US Army developed MDO to increase the chances of successfully achieving a break-in operation against a near-peer or peer adversary.[3] To note as well, the necessity of MDO, acknowledged by all levels of authority, is the understanding and belief that the US and NATO forces will be unable to achieve supremacy in every domain at all times.[4] US Army Training and Doctrine Command (TRADOC), the original authors of the Multi-Domain concept of warfighting, summarize the changing nature of war-related to the US and allied dominance by writing:

> As the Joint Force responds to adversaries contesting international norms in either competition or armed conflict, it will conduct operations in an emerging operational environment shaped by four interrelated characteristics: adversaries are contesting all domains, the EMS, and the information environment and US dominance is not assured; smaller armies fight on an expanded battlefield that is increasingly lethal and hyperactive; nation-states have more difficulty in imposing their will within a politically, culturally, technologically, and strategically complex environment; and near-peer states more readily compete below armed conflict, making deterrence more challenging.[5]

Domains will remain contested, and there will be periods where the adversary has temporary superiority of any given environment. MDO strives to bring temporary dominance to friendly forces to exploit each opportunity to the fullest.

Constituent Parts

Five constituent domains comprise the MDO framework. Each domain acts distinctly from the others, but many overlay areas in action and a physical presence. Land, maritime, aerial, space, and cyber domains are the areas of conflict today that need

[3] US Army Training and Doctrine Command, The US Army in Multi-Domain Operations 2028, (Kansas City: US Army Training and Doctrine Command, 2018), 6, https://www.hsdl.org/?view&did=820569, 15.
[4] Multi-Domain Battle, 2.
[5] The US Army in Multi-Domain Operations 2028, 6.

to be harnessed and optimized to achieve an enhanced effect on future battlefields. While each part is distinct from the others, thinking, planning, and operating across all battlespace domains is critical. To fully realize the sum of the elements, each domain must first be understood to be used to best effect.

The land domain is the cornerstone of future warfare and MDO. While the vast majority of land functions do not change under MDO, there is an emphasized shift in several critical areas where the US and NATO forces are considered vulnerable. Noted in the draft US Army White Paper on Multi-Domain Battle, "US ground combat capabilities are out of balance to effectively confront emerging conditions presented by peer adversaries. Enemy ground formations now have parity or overmatch with US forces in many weapons systems' range, lethality, protection, and mobility."[6] It is the return to dominance of the land force which spurred on the concept of MDO. Within the MDO concept, re-emphasis upon long-range fires assets, air and missile defence protection and non-kinetic fires is championed.[7] The re-emphasis of these functions is required to increase the land domain's lethality against adversarial forces while enabling the other environments in their action.

The maritime domain plays a central role in the future of MDO. The operationalization of the naval environment increases the full effect across all others. During break-in actions against adversaries who specialize in Anti-Access/Area Denial (A2AD) operations, it is crucial in many potential conflict zones. Increasing the maritime domain's ability to influence the other domains and vice versa enlarges the operational

[6] Multi-Domain Battle, 3.
[7]The US Army in Multi-Domain Operations 2028, 19.

area and effects range, thereby increasing the opportunity for convergence of effects.[8] Besides break-in operations, the maritime realm is increasingly responsible for global trade, commerce, and international movement of goods and persons. All countries require access to the maritime domain, and the denial of that access is an increasingly important avenue of warfare.[9]

The air domain has played an increasingly important role in operations since the Second World War through to the modern day. Air/Land Battle, pioneered following the Vietnam War, saw the air domain operating in concert with ground forces to clear lanes of exploitation into the heart of the enemy. In MDO, this concept is extant but is enhanced by additional roles and duties, such as increased intelligence, surveillance, and reconnaissance (ISR) tasks across multiple spectrums.[10] The air domain is again in a revolution by introducing remotely piloted air systems (RPAS) or UAVs. In his article on the subject of the proliferation of UAVs on the modern battlefield, Noel Sharkey notes, "There were only 150 robots in the Iraq War in 2004, including bomb disposal robots. Troops on the ground are now using thousands of small, unarmed aerial surveillance drones– so many that it is difficult to obtain an accurate estimate of their number.[11] These RPAS's have enabled all domains in their tasks, and they will continue to be prevalent in the future battlefield.

[8] Ibid, 48.

[9] Marco Fugazza, "Maritime Connectitity and Trade," Policy Issues In International Trade and Commodities Research Study Series, No. 70, (New York and Geneva: United Nations, 2015), 1. https://unctad.org/en/PublicationsLibrary/itcdtab72_en.pdf

[10] Pat Host, "US Air Force analysing future of multi-domain C2," *Jane's Defence Weekly* (26 July 2017), https://customer-janes-com.cfc.idm.oclc.org/Janes/Display/FG_595364-JDW

[11] Noel Sharkey, "The Automation and Proliferation of Military Drones and the Protection of Civilians," *Law, Innovation and Technology*, 3:2, 229, DOI: 10.5235/175799611798204914. https://www-tandfonline-com.cfc.idm.oclc.org/doi/abs/10.5235/175799611798204914

Cyber is the newest domain with tremendous potential for future development and action. Relatively new, cyberwarfare accesses military and civilian information technology systems, achieving military domination of equipment, information, communications and all processing systems linked and networked[12]. Cyberwarfare looks to create an advantage within the digital world by accessing military and civilian networks, thereby creating an edge in the other domains. This highly contested domain, either by adversarial, friendly and third-party entities, frequently act within the "grey space" of modern warfare.[13] Critical to MDO, the cyber domain is of vital concern and must be leveraged, when possible, to engage the enemy in its entirety.

The space domain is the least understood of all domains within MDO. Rather than acting primarily as an avenue to attack or defence, the space domain enables all others in their operations. In his address to the US Army War College in 2019, the Commanding General Space Command, General Raymond, said, "There is nothing that isn't enabled by space, whether RPA[S]s being flown through commercial SATCOM, ISR being collected from there, GPS weapons -- and I would suggest to you there is nothing, absolutely nothing, that isn't enabled by space."[14] The availability of space-based assets for modern intelligence collection is critical for future warfare. The space domain enables intelligence collection and surveillance, communications, and positioning and timing information, all of which are crucial to today's military demands. The ability to view adversarial areas without endangering personnel and equipment while simultaneously

[12] James A. Green, *Cyber Warfare: A Multidisciplinary Analysis*, edited by Green, James A. 1st ed. (Abingdon, Oxon;New York, NY;: Routledge, 2015), 1-2.
[13] Merrin, William. Digital War: A Critical Introduction. 1st ed. Abingdon, Oxon;New York, N.Y;: Routledge, Taylor & Francis Group, 2019; 185.
[14] "U.S. Army War College: Space Assets Enable Multi-Domain Operations," Targeted News Service, May 21, 2019. https://search-proquest-com.cfc.idm.oclc.org/newspapers/u-s-army-war-college-space-assets-enable-multi/docview/2233217006/se-2?accountid=9867.

providing many products pushes space into the essential information domain.[15] Imagery and full-motion video of military or civilian satellites' target locations enable operations within the other domains. Communications satellites allow for additional communication methods at the tactical, operational, and strategic levels where decisions can be made by those empowered to do so regardless of location. Lastly, global positioning and timing are critical to all domains. The space domain has revolutionized navigation of ships, planes and armoured vehicles, situational awareness of forces, and precision-guided munitions. The space domain must be harnessed to its fullest potential to thrive and to remain dominant in modern warfare.

Convergence and Effect

Convergence windows, the result of deliberate synchronization and coordination of effects, at multiple levels of command, from the tactical to the strategic, enable friendly operations. It is a space in which conventional and unconventional forces can conduct their regular operations with added effect. In the original US Army White Paper on Multi-Domain Battle, the three components to the solution were "to create and exploit temporary windows of opportunity, restore capability balance and build resilient battle formations and alter force posture to enhance deterrence."[16] While any element can create a local convergence window, achieving some advantage over the adversary, multi-domain battles are different because it plans these windows and collaborates across distinct domains.

[15] Multidomain Operations Transition in Thought, 69.

[16] US Army Training and Doctrine Command, *Multi-Domain Battle: Combined Arms for the 21st Century*, Draft Version 0.53, (Kansas City: US Army Training and Doctrine Command, 2016), 7, https://community.apan.org/wg/aucoi/jadcc/m/mediagallery1/178247

As an example of this effect, a tactical level event such as an attack by one force on the other can use several measures to create an advantage. For example, an artillery bombardment on enemy positions, a feint manoeuvre or other methods could create a local advantage for attacking forces. What then elevates this tactical advantage to a convergence window is other domain resources' addition to increasing the effect. Air forces might add local air superiority for a limited time, thereby shielding friendly forces from adversarial attack helicopters. Naval forces may fire ship-to-shore missiles at defined hostile command and control nodes.

Further, using space assets to limit precision navigation and timings at critical junctions throughout the battle to disorient hostile forces looking to counterattack. Finally, cyberattacks on enemy communications software may deny the enemy avenue to communicate its peril and request additional resources. These effects may not be of long duration or full effect, but together, it allows a distinct advantage on the battlefield to be exploited.

Lastly, in examining MDO and its core functions, the real value of this action is that it can be orchestrated at multiple command levels and benefitting those below and above it. Resource intensity and cost is a limiting factor in today's military. As a result, it is improbable that tactical actions will benefit from cyberattacks on enemy communications as this is not timely or cost-effective. What can be done is the tactical level taking advantage of strategic or operational convergence windows to enact some operation simultaneously. This advantage is realized through the echeloning system described in *The US Army in Multi-Domain Operations 2028*.[17] Acting under the

[17] The US Army in Multi-Domain Operations 2028, 2.

strategic convergence window umbrella, tactical commanders can seize the initiative for action. This convergence window further enhances the operational level orchestrating other effects.

MDO is more than the integration and synchronization of the before-mentioned domains. MDO pursues a more significant effect by integrating said domains into specific time windows to create the most significant impact upon the enemy. Windows of convergence, the period where MDO is fully utilized and the enemy at a disadvantage, is the opportunity to gain the initiative and are advantaged somehow against the enemy.[18] Again, in *The US Army in Multi-Domain Operations 2028,* the need for dominance through windows of opportunity are noted succinctly, "Future operations against a near-peer threat, however, will require the Joint Force to conduct continuous and rapid integration of multi-domain capabilities to gain cross-domain overmatch at decisive spaces."[19] The advantage created is inherently time-limited, but additional windows of convergence can be synchronized to later effect.

Synchronizing these windows of convergence is practically tricky and time-consuming, but the principle is relatively simple. In two basic examples, friendly land forces are privileged on the offensive by cyber forces, and from an air power perspective, air forces achieve local air supremacy for 24-48hrs. There are a thousand areas where multi-domain operations may strike, creating an overmatch of opposing forces' ability to defend on a thousand planes. It is the calculated nexus of opportunity to achieve

[18] Sean Atkins, "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace," *Air and Space Power Journal* Vol 32, No. 3 (Fall 2018): 27. https://search-proquest-com.cfc.idm.oclc.org/docview/2099885702?pq-origsite=summon
[19] The US Army in Multi-Domain Operations 2028, 20.

dominance in one or many domains, enabling further action against the enemy at a great advantage.

The synchronization of multiple domains to enhance effects on the battlespace is more than increasing the joint aspect of current operations but rather the full embrace of a new concept, outside the box of any single service. Traditionally, tacticians approach a problem and attempt to overmatch the enemy within each domain, even for a relatively short time. This parts-based approach is an example of a joint operation. What MDOs do is plan to overmatch the adversary in specific domains while also minimizing vulnerabilities in the others. As in the example above, to create freedom of movement in the battlespace, temporary air superiority is required for land forces. This requirement does not mean that friendly forces need conventional air superiority and absolute dominance with aircraft, as this effect may be achievable by other means. A disruption to the adversarial identification of friend or foe (IFF) transponder system could ground all aircraft, thereby achieving the same effect with a cyber-based tool vice an aerial platform.

In addition to examining MDO as a tool utilized in traditional warfighting, MDO is also a cornerstone of deterrence operations. The leveraging of all domains, with added non-traditional enablers such as the media and other related information products/tools, is hugely effective in creating spectacular problem sets that are exceedingly difficult for adversaries to exploit. The ability to use MDO as a foundational approach, both in the offence and defence, lends itself to many possibilities which create challenges for future adversaries. Discussing cross-domain deterrence in their collection of essays, Gartzke and Lindsay illustrate the advantage of MDO in deterrence:

> Thus policymakers may use air strikes to retaliate for terrorism, cyber operations to disable an adversary's command and control to to influence

> its electorate, targeted economic sanctions to punish cyber intrusion, or even migration policy to coerce neighbouring states. Indeed, non-military options for exerting influence and extracting concessions are increasingly available right alongside novel weaponry.[20]

Knowing an adversary has access and ability in all domains creates a significant amount of deterrence as the methods of striking back are countless. The weaponization of all domains and areas of influence makes a strong deterrence posture possible and probable.

Most importantly to this concept of MDO, vulnerabilities created by the exploitation of one domain can have drastic consequences in the others. Jeffrey Reilly, in his article on MDO and the subtle transition in military thought, offers:

> These factors [technological advances and their corresponding effects] are creating an environment where failure in one domain has cascading effects in one or more of the others. Postmodern technology is quickly fusing a continuum of integrated and interdependent domains.[21]

Performing as both the shield and act function, MDO enhances the sums of its parts, increasing the capabilities of a multi-domain force. Necessary in modern operations is the reliance on other domains to secure vulnerabilities across the spectrum. In harnessing the ability of a domain to protect another, increased effects are achievable in all subsequent phases of conflict. Critical to this venture, though, is understanding the force as a whole and thinking in the multi-domain headspace.

[20] Eric Gartzke and Jon R. Lindsay, *Cross-Domain Deterrence: Strategy in an Era of Complexity, (*New York: Oxford University Press, 2019), 4, doi:10.1093/oso/9780190908645.001.0001. https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=5647786
[21]Multidomain Operations Transition in Thought, 67.

CHAPTER TWO - SOVIET RUSSIAN DOCTRINE AND INHERENT VULNERABILITIES

The Soviet Union and the Russian Federation's military forces share a similar doctrinal philosophy that has remained particularly rigid over the last half-century. The land forces' central theme has been the prominence of indirect fires as the decisive factor on the battlefield with infantry and armoured manoeuvre forces in a supporting role. Fires prominence is in direct contrast to Western military thought, which privileges manoeuvre, supported by fires as the central tenant of modern warfare. While rigid in its foundations, Russian doctrine continues to evolve, incorporating emerging technologies, ideas and embracing modern global culture. Looking forward as well as back, "Russian tactics will continue to emphasize gaining and maintaining fire superiority over an adversary heavily; leveraging improved ISR capabilities and a wide range of fires platforms; and using speed, surprise, and integrated combined arms in maneuver forces to disrupt and overwhelm enemies once encountered."[22] These adaptations were developed over several decades and tested in minor regional conflicts such as Georgia 2008, Crimea 2014 and Syria 2015.

The development of this doctrinal evolution traces its lineage back decades but was without a champion until the current Chief of the General Staff of the Armed Forces of Russian, General Valery Gerasimov, realized its necessity. By embracing modern technology and thought, Gerasimov has operationalized a large swath of the Russian Armed Forces. Through further organizational changes, meant to increase the armed forces' professionalism and morale, the Russian military is a peer competitor to the

[22] Scott Boston and Dara Massicot, *The Russian Way of Warfare: A Primer*. Santa Monica, CA: RAND Corporation, 2017, 9. https://www.rand.org/pubs/perspectives/PE231.html.

world's militaries.[23] By highlighting the evolution and modernization of the Russian Armed Forces, the intention here is to demonstrate that the Russians are far from incapable of modern warfare and are a genuine threat to Western powers, necessitating a thorough analysis. Therefore, current Russian doctrine requires examining their elite, modern force, the Rapid Reaction Force (RRF) and their overarching doctrinal theme of anti-access area denial in all realms. With these areas examined, a proper mental projection of a skillful force is possible, necessitating the multi-domain approach to operations. Unfortunately:

> Few in the West have paid much attention to Russia's doctrinal pivot towards "New Generation War" until its manifestation in Ukraine. This emerging strategy has been both under-appreciated and misunderstood – often muddled with our own constructs of "fourth generation warfare;" or "non-linear warfare" or "hybrid war."[24]

The Russian military's adoption of a Rapid Reaction Force (RRF), combining air, land, and sea elements into a single command, demonstrates a significant change in the Russian hierarchy's focus. Instead of the modernization and bolstering of heavy mechanized forces, the Russian military has focused its efforts on creating highly agile forces capable of a broad range of actions. Relying primarily on the highly professional *Vozdushno-desantyne voiska* (VDV), or airborne troops, augmented by Spetnaz, motorized rifle brigades, naval Spetnaz forces, and special operations forces, this formation is skillful and quite dangerous.[25] This formation, or its constituent parts, has

[23] Kiernann Kane, "Adapting Towed Artillery Today to Meet a Near-Peer Competitor Tomorrow," *Fires* (Sep, 2017): 27. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/adapting-towed-artillery-today-meet-near-peer/docview/2101836407/se-2?accountid=9867.
[24] Phillip Karber, *Lessons Learned" from the Russo-Ukrainian War*. (Draft Document). (The Potomac Foundation, 6 July 2015): 1. https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf
[25] Charles K. Bartles and Roger N. McDermott, "Russia's Military Operation in Crimea," *Problems of Post-Communism* Vol 61, No. 6 (2014): 49. https://www-tandfonline-com.cfc.idm.oclc.org/doi/abs/10.2753/PPC1075-8216610604

been the “shock troops” for Russian Forces in the last decade globally. While this model is highly potent, it is not reproducible beyond the current structure. Reliance is on the best and most professional Russian soldiers; the conscripted remainder cannot reproduce the same results, even with the same opportunities and funding. Further formations like the RRF would require significant re-investment and re-organization, likely beyond current capabilities and aspirations.

The Russian Armed Forces’ most remarkable ability is to defend its interests in a pan-domain environment. The hallmark of any discussion surrounding Russian forces today is the discussion of its ability to conduct Anti-Access/Area Denial (A2AD) using its Integrated Aerial Denial Systems (IADS) over vast areas of air, land, and sea. Remaining unable to challenge the West, specifically the United States, the ability to conduct research and development on many cutting-edge technologies and concepts above and below the earth, Russia has focused its priorities on defending itself in a far more cost-efficient method. By developing and integrating advanced radars, sonars, and suites of missile systems, Russia has enveloped itself in one of the world’s most comprehensive missile and aircraft shields.[26] Specifically, “the IADS complicates the ability of an adversary to employ air-delivered fires against Russian forces, and the considerable artillery and missile forces available are intended to allow Russia to gain and leverage superiority in fires on the ground.”[27] As a result of these developments, the United States must continue to develop newer and more effective stealth technologies on every pricier fifth-generation aircraft and suitable contemporary advances in other

[26] John Gordon, Igor Mikolic-Torreira, D. Sean Barnett, Katharina Ley Best, Scott Boston, Dan Madden, Danielle C. Tarraf, and Jordan Willcox, *Army Fires Capabilities for 2025 and Beyond,* (Santa Monica, CA: RAND Corporation, 2019), 109, https://www.rand.org/pubs/research_reports/RR2124.html.
[27] The Russian Way of Warfare: A Primer, 10.

domains. Conversely, NATO efforts must reaffirm combined joint suppression of enemy air defence (C/JSEAD) capabilities that enable Joint Force Entry (JFE) operations. The arms race may technically be over, but East and West rivalry still drives arms production and research and development.

Russian Artillery/Fires Doctrine Review

Throughout time in the Soviet Union and into the Russian Federation, artillery and fires assets have been the preeminent weapon on the battlefield. Marek Depczynski, a faculty member in the war studies university in Warsaw, Poland, succinctly notes, "In armed conflicts with the participation of Russian Armed Forces, in most cases, the artillery fire determined the course of battles and campaigns."[28] As opposed to Western nation's doctrine and ways of war, manoeuvre forces are not enabled by artillery but are instead enablers to artillery fires. The belief in artillery and rocket fire as the most significant influence on the tactical battlefield has led to the implementation of several different approaches to their use and an extremely capable development of long-range artillery capable of outclassing any Western response in both range and destructive capabilities.

The grouping of Russian artillery units at the brigade and divisional level is an operational advantage to their doctrine, emphasizing massed fires with superior level assets. Emphasis is on applying timely and accurate fires by large artillery organizations to achieve immediate enemy effects.[29] By grouping both rocket and tubed artillery under

[28] Marek Depczynski, "Renaissance of Russian high-Powered Artillery," *Scientific Journal of the Military University of Land Forces*, 51, No 4 (2019): 616. DOI: 10.5604/01.3001.0013.6455 https://zeszyty-naukowe.awl.edu.pl/resources/html/article/details?id=195930&language=en

[29] Lester Grau and Charle Bartles, "Russian Artillery Fire Control for Large-Scale Combat Operations," *Fires* (May, 2019): 8. https://search-proquest-com.cfc.idm.oclc.org/docview/2246860502?accountid=9867.

the same command structure, fires networks achieve efficiency while command and control of the preeminent Russian tactical asset remain ensured. This system, within Russian doctrine, was exported to other satellite and allied states such as Iran, China, North Korea, and other legacy Soviets proxy states. Together, they view artillery organizational changes as fundamental to conflict, regardless of their equipment's modernity. Schmid and Wilson write, "Although at different levels of technology in their use of artillery, all believe in the massing of brigade and above fires assets leading with artillery to shape and win battles."[30] As the cornerstone of doctrine, this organizational structure is unlikely to change in the immediate future and must be countered at the tactical and operational level by allied forces.

Within Russian fires doctrine, high-power, long-range artillery units are the cornerstone of Russian tactics and philosophy. Since its early adoption within Russia, cannon artillery has played a considerable part in every conflict and forms Russian forces' nucleus. Primarily developed during the late Soviet era, Russian high-power artillery continues to evolve and is upgrading its capabilities for future conflict. Within the Russian army, there are three distinct levels of tube artillery support available within combat operations. The organic assets prescribed to any manoeuvre unit, usually in medium artillery units or shorter ranged heavy mortars. As well as organic assets, long-range artillery and rockets are available from the brigade and divisional artillery groups. Lastly, there are surface-to-surface missile systems at the operations level, ranging deep into the strategic area. In this matter, the availability of artillery resources is somewhat

[30] Joseph Schmid and Adam Wilson Jr, "Calling for Improvements on US Army's Cannon Artillery," *Fires* (Nov, 2017), 53. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/calling-improvements-on-us-armys-cannon-artillery/docview/2101842153/se-2?accountid=9867.

guaranteed, regardless of organic capabilities or functions, ensuring the engagement of priority targets, as available with appropriate fires.

The modernization of the 2S7 Pion and 2S4 Tulipan platforms and the introduction of longer barreled self-propelled artillery pieces positions Russian forces to remain preeminent in indirect fires capabilities compared to Western allies. Through the process of modernization, both in the physical aspects of the indirect fire system and the software systems to calculate and fire, Russian fires forge ahead, overmatching most Western indirect fire and rocket systems, not to mention the inherent quantity of the Russian order of battle.[31] Maintaining dominance in range and efficacy allows Russian forces to engage enemies beyond their equivalent formations capabilities, either out of range of counter-battery fire or forcing enemy forces to unmask higher-level assets to conduct strikes. With improvements in counter-mortar/artillery radar systems, UAVs with greater range, and the ability to prosecute distant targets with long-range precision fires, Russian forces force their operational advantages over their enemies. This process fundamentally begins in development where the range and rate of fire of assets are essential but continues right up the command and control chains. Russian forces are allowed the freedom of action with higher-level or longer-ranged rockets to strike in depth with virtual impunity by using long-range tubed artillery as the foundation of their IDF system.

Rocket artillery remains a powerful and highly relevant Russian asset on the battlefield. Universally feared by foes, Russian BM-27 and BM-30 rocket systems are incredibly lethal at great distances and parade in significant numbers within the Russian

[31] Ibid, 53.

order of battle. Modernization of these systems has increased their range, lethality, and accuracy, allowing Russian manoeuvre forces to bypass destroyed enemy formations. As seen in the Ukrainian conflict, "the main "killer" in the Donetsk and Lugansk areas are artillery units, especially those equipped with high-range barrels, usually mobile reactive / missile launch, BM - 21Grad / Tornado, B.M. - 27 Uragan and B.M-30 Smerch."[32] The numerical advantage in rocket artillery alone advantages Russian forces, but modernization has ensured that Russian rocket artillery remains technologically equivalent for tactical operations.

Russian IDF fire control systems and task organizations are pretty distinct from Western militaries and are also under a Russian army revolution. The simplified command and control structure allows the rapid scaling of indirect fires on the battlefield, enabling brigade and division fires to influence the tactical battlespace with ease.[33] Additionally, streamlining the command and control structure from observer to high-level artillery system allows for faster engagement and increased target destruction. Using modern communication infrastructure, evolving observation equipment such as UAS, and increased range lethality of projectiles, the grouping of artillery is a highly potent asset, specifically when Russian artillery is estimated to overmatch western artillery at a three to one ratio.[34] This ratio is also realized in early planning figures for the new Russian Brigades, which saw the indirect fires combat power being equal to an older division, or

[32] Florin, Cotet, "Aspects Regarding the Use of Field Artillery in Contemporary Operations," *Bulletin of "Carol I" National Defense University* 8, no. 1 (2019): 38. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/aspects-regarding-use-field-artillery/docview/2371519352/se-2?accountid=9867.
[33] Russian Artillery Fire Control for Large-Scale Combat Operations, 14.
[34] Calling for Improvements on US Army's Cannon Artillery, 52.

roughly double what a Brigade had previous to the reforms.[35] Targeting this grouping is central to defeating Russian forces now and into the future.

Case Study: Ukraine

The Russian invasion of Ukraine in the Donbas and Crimean regions in 2014 was a masterful and well-choreographed plot meant to defeat Ukrainian forces in the area and thwart the international community's intervention. A significant hallmark of the campaign, which saw the destruction of many Ukrainian formations, was the tactically well-employed and highly effective use of indirect fires. Employing the latest in Russian long-range precision fires with UAVs acting as observation parties, Russian fires could mass on Ukrainian forces to a degree not foreseen by local and Western troops.[36] Russian observation parties influenced the battlefield decisively in Russia's favour when coupled with long-range tube and rocket artillery. With this latest Russian firepower demonstration, Western allies must take definitive action to examine Russia's dominant arm underlying capabilities and successes.

The use of Russian IDF systems in the Donbas Region of Ukraine was a classic example of indirect fires' effectiveness and lethality. Harkening back to the First World War, estimates are that 80% of all Ukrainian forces' casualties resulted from Russian IDF.[37] This contrasts Western-allied notions and intentions where the vast majority of casualties would be achieved through the integration of manoeuvre forces and air power.

[35] Daivis Petraitis, "The Russian Military Reform 2005-2015," Lithuanian Annual Strategic Review 9, no. 1 (2011): 160. doi:http://dx.doi.org.cfc.idm.oclc.org/10.2478/v10243-012-0003-6. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/russian-military-reform-2005-2015/docview/1323403804/se-2?accountid=9867

[36] Ibid, 53.

[37] Steven Yeadon, "Toward Understanding Fires on Near-Peer Battlefield," *Fires* (Sep, 2019), 59. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/toward-understanding-fires-on-near-peer/docview/2314499511/se-2?accountid=9867.

A manoeuvre and airpower focus contrasts Russian doctrine and illustrates the difference between the opposing forces. This will likely create many varied opinions on the value of artillery in future conflicts and correlating ability to disrupt those same systems using a multi-domain approach. However, what is not under dispute is Russia's devastating effect upon its Ukrainian foes during the height of the conflict. What is essential now is to understand how this occurred, where it was enabled, and lastly, where to target for the most significant effect.

One of the most traditional but relevant factors in the success of Russian IDF in the Donbas region was the Russian ability to mass fires, specifically their long-range tube artillery and tactical level rocket systems. Mass fires at the tactical through to the operational level are a hallmark of Russian artillery tactics. It is incredibly successful in dominating the battlefield at the time and place of its choosing. In examining this ability, Captain's Schmid and Wilson reference one of the leading experts on the new Russian doctrine at the Army's Capability Assessment Center, Joseph Thibeault. They write, "Thibeault made an assessment that the Russians have at least a 3 to 1 advantage in cannon artillery over the United States. Russia also has an advantage in munitions mentioned above and the ability to mass fires at the division and corps level with ease."[38] The ability to mass fires provided the ability to capitalize on Ukrainian vulnerabilities and demonstrated a continued valuation to traditional Russian doctrine. Demonstrating this same standard methodology to the West and allies' consternation is Iran, China, and North Korea, amongst many others.[39] Knowing the proven value of massed artillery in modern conflict, as demonstrated by Russia in the Donbas, has likely reinforced the

[38] Calling for Improvements on US Army's Cannon Artillery, 53.

[39] Army Fires Capabilities for 2025 and Beyond, 165-174.

belief amongst both allies and adversaries that traditional bases of power are still quite relevant and capable well into the twenty-first century.

The other great observation born out of the Russian incursion into the Donbas region of Ukraine was UAVs' weaponization to act as forward observation parties, calling down artillery fire with great precision and accuracy. UAVs' use as forward observation parties is not a new revelation and has been used for several years with allied and adversarial armies. However, the difference in this conflict was the frequency of fires from UAVs and the efficacy. The use of UAVs proved to be decisive in this application and acquitted themselves with high accolades. In an article for *Joint Force Quarterly*, arguing the need for US forces to quickly develop a counter-UAV capability to combat these exact types of attacks seen in the Donbas region, the authors note, "the latter instance widely believed to be the first in which every belligerent used drones to produce decisive battlefield results—Russia and its proxies used tactical drones to provide ISR targeting information for supporting artillery units."[40] Not only were these UAVs providing direct tactical information to Russian IDF command posts, but they were also improving the overall efficiency of the Russian IDF system:

> The near real-time intelligence from these small platforms improved target location accuracy, counterfire response times, and fire mission lethality, and in one instance in July 2014, Russia used this technique to destroy four Ukrainian army brigades preparing to conduct a cross-border attack against Russian-backed separatists' lines of supply.[41]

[40] Edward A. Guelfi, Buddhika Jayamaha, and Travis Robison, "The Imperative for the U.S. Military to Develop a Counter-UAS Strategy," *Joint Force Quarterly : JFQ* no. 97 (Second, 2020): 6. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/imperative-u-s-military-develop-counter-uas/docview/2394262817/se-2?accountid=9867.

[41] Ibid, 6.

The value of small and relatively inexpensive UAVs cannot be discounted by Western militaries, as can be witnessed from Ukrainian forces' experience. The ability to use UAVs in the observation role, reporting directly from UAV operator to artillery command post, is highly efficient and effective.

UAVs' integration directly into the reporting chain of Russian IDF has exponentially increased UAVs' lethality and quickened the kill chain of Russian IDF systems. In the traditional approach, mainly maintained by Western armies, UAVs are integrated into reconnaissance units or used as precision strike assets. This approach increases manoeuvre units' ability to find, fix, and strike opposing forces but creates additional reporting chains to call for fires assets to strike. As seen in the Donbas, UAVs acted as manoeuvre forces for fires to attack, eliminating several steps in calling for fires.[42] This speed plays to Russian doctrine and the adversary's strength, reducing friendly forces' ability to close with manoeuvre units, shielding themselves from Russian IDF.

Continued use of UAVs as designated observers will continue for Russian and allied forces. Increased range past friendly positions allows for the targeting of higher echelon forces by IDF systems, exploiting increased lethality and ever-extending lethal ranges. Unlike the use of reconnaissance forces, UAVs are significantly harder to detect, deter, and eventually destroy by opposing forces. The loss of a single platform is also relatively insignificant as there is no loss of life and the UAVs exponentially lower cost

[42] Fox Amos, "Understanding the Modern Russian War: Ubiquitous rocket, artillery to enable battlefield swarming, siege warfare," *Fires* (September – October, 2017): 25. https://search-proquest-com.cfc.idm.oclc.org/docview/2101833448?pq-origsite=summon

than modern fighter aircraft, some of which are available from commercial sources.[43] Although highly effective alone, coupled with long-range counter-mortar/artillery radar systems, UAVs enable other assets to ensure battlefield effects are succinct. Supporting artillery systems with increasingly sophisticated and effective UAVs and radars are enabling fires.[44]

The effectiveness and veracity of Russian IDF systems are undeniable in the recent conflict against Ukrainian forces in the Donbas. Massing fires has been a staple of Russian doctrine since the arrival of cannon on the Steppes to the First and Second World Wars. Nowhere was it greater emphasized, though, as it was in the Cold War, which sees continuation to this day. The modernization of those same systems, to increase their relevance and lethality, continues to be introduced by Russian forces. This modernization has led to an unexpected turn, though, ripe for Western forces' exploitation. Russian Forces are showcasing numerous vulnerabilities in the Donbas, which can be readily exploited by adequately equipped and trained forces. In simplistic terms, using digital systems or near-constant communications with an observer, such as a UAV in both circumstances, creates an inherent chink in the armour. Vulnerabilities have shifted from traditional models to modern digital gaps in coverage, and it remains the responsibility of allied forces to exploit them to the fullest.

[43] Margarita Konaev, "The Future of Urban Warfare in the Age of Megacities," *Focus stratégique, IFRI*, (March 2019): 42. https://www.ifri.org/sites/default/files/atoms/files/konaev_urban_warfare_megacities_2019.pdf

[44] Calling for Improvements on US Army's Cannon Artillery, 53.

CHAPTER THREE - THE DEFEAT OF RUSSIAN IDF SYSTEMS

The defeat of Russian Indirect Fire systems is not only possible but highly probable using MDO. As the heart of the Russian land forces, indirect fires assets are critical to offensive and defensive operations. As opposed to strong integrated air defence systems (IADS) protecting Russian operational airspace, the ground forces have long-range artillery to achieve its tactical aims, "The employment of indirect fires en masse at the tactical level is one of the signature characteristics of Russian ground forces."[45] As a result of the reliance on IDF assets as the critical capability in all phases of operations, using MDO as an operational and tactical framework, these systems' vulnerabilities become readily apparent, offering numerous avenues of exploitation. Due to the networked nature of contemporary warfare, where the definition of battlespace is murky, and domains must act in coordination to achieve effects, "These factors are creating an environment where failure in one domain has cascading effects in one or more of the others. Postmodern technology is quickly fusing a continuum of integrated and interdependent domains."[46] Using the five realms within multi-domain operations, combined with enhanced network integration of sensors and decision-makers on the battlefield, Russian IDF systems are exposed.

The critical vulnerability of the Russian indirect fire systems and the entire land forces doctrine, as a result, is the numerous areas of exploitation that are available to forces using multi-domain operations. By targeting the IDF systems in all domains and at

[45] *The Russian Way of Warfare: A Primer*, 11.

[46] Jeffrey M. Reilly, "Multidomain Operations: A Subtle but Significant Transition in Military Thought," *Air & Space Power Journal*. Spring2016, Vol. 30 Issue 1, 67. http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/detail/detail?vid=2&sid=041a1d03-2c0d-4299-ab9f-12e5452f9968%40sessionmgr102&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=113399783&db=a9h , 67.

all critical junctures, the system is brought to a grinding halt. The kill-chain, the link from the sensor to command and control node to IDF asset, cannot be hardened sufficiently to allow for the free flow of information at all times.[47] By coordinating and synchronizing within the multi-domain, establishing convergence windows, using any gateways into the Russian IDF systems, stripping away critical assets at decisive times, allowing friendly force freedom of action and denying the same to Russian forces. The intent is not to examine every vulnerability within the Russian IDF system but rather to explore and vector into a few generic avenues that can turn into specific and detailed target arrays for future exploitation.

Communications Attack

A critical vulnerability to any indirect fire systems is the communication system linking the observer to the command and control centre to the weapon system itself. Whether digital or analog, the communications system across the battlefield is vulnerable to multi-domain operations across numerous domains at any one time. Digital communications travel the globe in seconds while satellite communications are quickly bounced within the operational area. Additionally, analog radio communications are used within the tactical fight, calling for counter-fires and massing artillery on targets.[48] These communications systems combined are relatively robust and provide for some redundancy, but within the multi-domain construct, each system is stripped of mutual support and exploited to best effect.

Within the Russian IDF concept of operations, digital, analog, and satellite communications methods are used to link forward observation teams, UAVs, or other

[47] Ibid, 67.

[48] Russian Artillery Fire Control for Large-Scale Combat Operations, 13.

ISR assets to command and control centres.[49] Due to Russian IDF's nature, these communications legs usually are quite distant, ranging from the immediate close fight of 5-10kms, through the tactical deep battle of 10-30km, and finally to the operational level fight at more than 50kms.[50] While this may be a strength, the ability to affect the tactical level fight with operational level assets also presents a vulnerability that can be exploited by forces acting within multiple domains, especially if in concert.

Using MDO, it is possible to disrupt, delay, or destroy these critical Russian communications networks. In at least the short term, the degradation of Russian IDF communications can be accomplished through various means. Any degradation, though, must be predicated on the successful mapping of said communications means and within the joint multi-domain environment; all five domains can conduct this. With the integration of electronic warfare (E.W.) suites in some fifth-generation fighters and fourth-generation specialty E.W. aircraft, this mapping can occur in real-time with distribution to all domains and command and control nodes.[51] This in itself is likely enough to begin the degradation of IDF communications system but can further be targeted with ground sensors conducting the same types of missions, space-based systems monitoring satellite communications pathways, and lastly, cyber surveillance and mapping missions to determine digital routings.[52] This multi-domain mapping sets the

[49] Ibid, 7.

[50] Renaissance of Russian High-Powered Artillery, 629.

[51] Anika Torruella, "F-35 Project Seeks to Overcome EW Obsolescence." *International Defence Review* 46, no. 11 (2013). https://customer-janes-com.cfc.idm.oclc.org/InternationalDefenceReview/DisplayFile/idr16067?edition=2013

[52] Benjamin Jensen, Brandon Valeriano & Ryan Maness, "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist," *Journal of Strategic Studies*, 42:2, (2019): 215. DOI: 10.1080/01402390.2018.1559152 https://www-tandfonline-com.cfc.idm.oclc.org/doi/epub/10.1080/01402390.2018.1559152?needAccess=true

conditions for future attacks as it defines multiple communications methods, probing for the weakest communications systems chain.

The degradation of communications systems needs to occur synchronously to achieve the most significant effect across the entire electronic spectrum. The degradation may not be required for significant periods or maybe phased depending on the critical needs, but regardless, the converge window must be coordinated. Depending on the resources attributed to this attack and the operational level of the convergence window, targeted systems identified in the mapping stage can be isolated from their communications chain at friendly force convenience.[53] Likewise, this window of opportunity can be scaled from the operational level to the tactical to achieve the required effect over a short period. Without the communications chain from observer to weapon system, the heart of Russian land forces is impotent to friendly parties.

Indirect Fire Software and Systems Attack

The advancements in indirect fire capabilities over the last quarter-century have been only surpassed by the improvements in artillery digitization. The introduction of increasingly powerful and accurate hardware and software systems has revolutionized the employment of Russian IDF and allied IDF.[54] Though increasingly precise and responsive, providing an advantage to newer IDF over legacy systems, increased digitization also presents an additional avenue of exploitation by multi-domain forces. The introduction of wireless digital communications systems within the Russian IDF

[53] Nadia Kostyuk and Yuri Zhukov, "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* Vol. 63, No. 2 (2019): 320.

[54]Florin Cotet, "Harmonizing Field Artillery Entities With Similar Nato Field Artillery Units In The Current Complex Battlespace." (Bucharest: "Carol I" National Defence University, 2019): 14. https://search-proquest-com.cfc.idm.oclc.org/conference-papers-proceedings/harmonizing-field-artillery-entities-with-similar/docview/2237828139/se-2?accountid=9867.

forces has allowed software and systems attacks by friendly forces using multi-domain operational methods.[55]

In continuation of the mapping mentioned above of communication systems, network entry points are determined across the entire spectrum but most notably within the digital realm. Cyber forces can deliberately target these access points to conduct any number of missions to achieve an effect, in some instances a similar effect to kinetic actions.[56] These effects can range from the mundane with eavesdropping and keystroke logging to the changing of critical firing data or the destruction of the IDF firing software. Albert Harris' article on preparing for multi-domain operations discusses one of the possibilities for an actual cyber attack having implications within the physical world. He writes:

> Offensive actions conducted in the logical network could render systems inaccessible, denying war planners and operators access to essential mission data and communications. Access points in the logical network can also be leveraged to target physical network systems, bringing down I.T. hardware and leaving a technology-dependent unit nonmission capable. Virtual identities, or cyber personas, can be targeted to gain access to the physical or logical I.T. layers.[57]

The real challenge is not in effect achieved but in the access to the affected systems.

After accessing the affected systems, changes can be implemented to achieve the desired timeframe's effects. Overall, the outcomes achieved may seem relatively trivial, but they may be enough within the tactical environment. A simple example of this may be changing target location data from friendly forces to the location of the enemy

[55] Russian Artillery Fire Control for Large-Scale Combat Operations, 14.

[56] Dean alexander, "Cyber Threats in the 21st Century," *Security* (September 2012): 72. https://search-proquest-com.cfc.idm.oclc.org/docview/1223497697?pq-origsite=summon

[57] Albert Harris, "Preparing for Multidomain Warfare: Lessons from Space/Cyber Operations." *Air & Space Power Journal* 32, no. 3 (Fall, 2018): 51.. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/preparing-multidomain-warfare-lessons-space-cyber/docview/2099884315/se-2?accountid=9867

observer. This would, of course, have devastating effects on the observation party with minimal impact on friendly forces. This might also not be immediately identified by Russian troops as a data intrusion and may allow the cyber operator additional time to make further attacks.

In examination of this type of attack vector, there is the possibility that the time and effort involved would not be worth targeting the cyber applications for Russian IDF systems. Normally, this is likely accurate, but this type of scenario has played out within modern warfare and the results were stunning. In the Russo/Ukrainian War, Russian malware was responsible for infecting a Ukrainian ballistic software application widely used by Ukrainian forces. Once infected, it likely broadcasted the user's location to the hackers and Russia was able to target and eliminate up to 20% of all Ukrainian D-30 artillery pieces in the conflict.[58] While not identical to the attack envisioned in this paper, this demonstrates a similar result at the appropriate tactical level.

While effective in its own right, the exploitation of Russian IDF software and digital systems is better used in conjunction with other layered effects. The actual value in this nature of intrusion is the ability to use enemy force munitions and systems against their own forces. Additionally, the resources expended may prove to be scarce or costly. Finally, these systems' intrusion and initial use may force the systems to retreat from the networks and transition to standalone systems. Becoming standalone only creates additional delay to their eventual use and creates different areas for future exploitation.

[58] Adam Myers, "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," Crowdstrike (blog), Crowdstrike (December 22, 2016). https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Counter-UAS Operations

UAS/RPAS use by Russian IDF forces has increased exponentially since their debut in modern conflict. As seen in Crimea and the Donbas regions of Ukraine, UAS have been heavily relied on to acquire targets for long-range artillery systems.[59] They have been highly effective in their operations and have garnered great respect from all modern conflict participants. Although essential, Russian reliance will prove highly problematic as they are incredibly susceptible to allied multi-domain operations.

Russian UAS systems used to conduct IDF missions or develop IDF targets are generally at the tactical and lowest operational levels.[60] As a result, their ability is the most significant limiting factor because their size and altitude constraints, which are not insurmountable, could increase their vulnerability across the MDO spectrum with an appropriate counter-UAS strategy. Without the specifics of classified sources, the strategy is best summed up by stating the requirements for "A U.S. Army counter-UAS strategy must provide a framework for a persistent and comprehensive approach that links Soldier, materiel, and software solutions."[61] The re-introduction of tactical-level actions to defeat UAS is in of itself multi-faceted without mention of multi-domain possibilities.

UAS is uniquely vulnerable to multi-domain operations due to their natural characteristics and requirement to operate within each domain simultaneously. This exposure expresses itself in two distinct ways. First, with the physical UAS and secondly, in which the data is procured. UAS is susceptible to traditional kinetic operations by land,

[59] Lester Grau and Chuck Bartles, "Integration of Unmanned Aerial Systems within Russian Artillery," *Fires* (Jul, 2016): 37. https://search-proquest-com.cfc.idm.oclc.org/docview/1823336156?accountid=9867
[60] Ibid, 34.
[61] The Imperative for the U.S. Military to Develop a Counter-UAS Strategy, 8.

sea, and air assets as a low-flying aircraft. Allies armed with low-cost kinetic systems for small tactical UAS and air-to-air or ground-to-air missile systems for operational and strategic level UAS, multi-domain forces can deny the use of these precious resources on the physical plane As technology changes as well, movement away from kinetic projectiles to directed energy weapons will further create additional challenges for the tactical use of UAS as IDF observers.

In addition to the traditional realms and disruption methods, UAS are susceptible to both cyber and space operations. This directly affects the second vulnerability of Russian UAS as UAS are by necessity tethered to the ground via digital or analog control stations.[62] This link to a ground control station or digital satellite link creates a vulnerability to cyber exploitation. This exploitation can take many forms but can easily be categorized using disrupt, deny, and deceive. Temporary or permanent loss of control by the ground stations, the denial or targeting data and information or the false imprinting of incorrect data are possible effects of cyber operations.[63] Additionally, with the addition of the space domain, spoofing or denial of target location and timing data can achieve some of these same effects, just through different means.

The critical factor in examining counter-UAS operations by multi-domain forces is that each domain can conduct some form of an effect upon UAS at any given time. Through proper planning and the synchronization of forces, systems and effects, Russian UAS are highly vulnerable. Stripping this asset which has increasingly been adopted as a

[62] Integration of Unmanned Aerial Systems within Russian Artillery, 36.

[63] Cesar Gomez, "Cybersecurity of unmanned aircraft systems (UAS)," (Master's thesis., Utica College, 2015), 19, https://search-proquest-com.cfc.idm.oclc.org/docview/1750068515/fulltextPDF/78CB7A5D050941A1PQ/1?accountid=9867

critical element to the Russian IDF system of systems, would have devastating short and long-term effects.

Destruction of Russian IDF Systems

The traditional means of denying an adversarial advantage is to destroy those means, and within the MDO concept, this method remains relevant. The destruction of Russian IDF and air defence (A.D.) systems, both in the traditional sense of destroying long-range artillery and missile launchers, as well as the destruction of their ancillary equipment, computers, vehicles, and other necessary items, is needed to maintain increased periods of localized dominance within the multi-domain environment.[64] This is achieved through four of the five domains, possibly enabled by the fifth, space.

The detection and destruction of long-range artillery and missile units are a land domain priority within the traditional fight.[65] As Russian forces are developed around artillery supremacy within the land domain, their destruction enables allied ground manoeuvre and exploitation.[66] In the *U.S. Army in Multi-Domain Operations 2028*, this act is detailed explicitly in "defeating the enemy's mid-range systems." It specifically says, "The corps continues to attack the enemy's mid-range fires during exploitation… The combination of corps fires and division maneuver overcomes this enemy attempt to prevent the defeat of its mid-range systems, which are the most dangerous element of its tactical systems."[67] The detection process is typically determined through analytical intelligence skills and deep penetrating ISR platforms. Within the MDO construct, this is enhanced further with maritime and aerial surveillance and strike assets.

[64] Toward Understanding Fires on Near-Peer Battlefield, 61.
[65] The U.S. Army in Multi-Domain Operations 2028, 40.
[66] Ibid, 42.
[67] Ibid, 42.

In addition to conventional assets supporting the destruction of Russian IDF systems, the cyber domain will increasingly play a more prominent role in reducing the Russian IDF threat on the physical plane. As IDF communications systems become further digitized and the integration of computer components in modern artillery and missile systems increases, cyber warfare experts will develop additional exploitation avenues within the physical elements themselves. This case is best illustrated from a Russian cyberattack on Ukrainian forces, which:

> In 2016, the cyber security firm Crowdstrike reported that Russia used an Android-based malware to infect apps Ukrainian units were using to compute the math required for targeting artillery. These infections enabled digital reconnaissance and helped Russian units geolocate Ukrainian artillery formations and preemptively strike them.[68]

While this was a digital cyber attack on a software application used in conjunction with an artillery system, it demonstrates its applicability. The nature of long-range artillery and missile systems demands high precision, and by changing these characteristics, or the timing of specific actions, catastrophic malfunctions can be engineered digitally. A digital attack vector in Russian IDF systems adds a physical vulnerability to the cyber dimension.

Denial of Space-Based Capabilities

The denial of specific space-based capabilities, supporting Russian IDF systems, whether at the point of target or within the entire kill chain, will significantly affect Russian abilities, denying them freedom of action and significantly reducing their long-range artillery and missile system potency. Since the advent of the Global Positioning System (GPS), first genuinely used in the First Gulf War, Russian IDF systems have been

[68] Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist, 227.

enabled by complementary systems, Global Navigation Satellite System (GLONASS), and the utilization of the civilian GPS signals themselves.[69] Using these systems, and in some cases relying on them totally, IDF systems have become vulnerable to their denial as precision fires, used at great distances, are no longer feasible or are reliant on secondary or tertiary systems for guidance. The attack on these space-based capabilities provides a distinct advantage to allied forces.

The degradation of Russian space-based assets, plus the potential denial of allied space-based satellite systems, would inhibit Russian IDF's ability to maintain optimal performance and capabilities. The GLONASS system provides reliable satellite data and voice communications across multiple domains and areas of interest and conducts critical reconnaissance functions for operational and tactical level events.[70] The denial, or even degradation, of these services would affect the Russian IDF's ability to perform their primary mission.

To deny or disrupt Russian space-based capabilities is genuinely a multi-domain operation, enabling individual domain capabilities at their respective levels. It is customary for allied forces to deny satellite information to the enemy within the land, maritime, and aerial domains by using GPS jammers.[71] This is achieved by various assets, ranging from localized tactical denial devices to operational level assets flying high over the battlefield. This is naturally a temporary feature relying on localized

[69] Lester Grau and Charle Bartles, *The Russian Way of War*, (Fort Leavenworth: Foreign Military Studies Office, 2016): 263.
[70] Ibid, 263.
[71] Tim Fish, "Europe Ponders SEAD Modernization as Russia Fields New Threats," *The Journal of Electronic Defense* (May, 2018): 26. http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/detail/detail?vid=0&sid=c7f856f5-60ed-4d9e-aded-2198633088f8%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=mth&AN=129625407

overpowering of satellite signals but can be leveraged at critical times to deny the precision of information or disrupt the vital links to ground-based communications assets and control stations. This effect operationalizes other avenues of exploitation and can be extremely valuable to gain temporary windows of convergence.

The denial of space-based assets requires a note of strategic caution to ensure the weaponization of space does not become a reality. Weaponizing space and using this domain for kinetic actions is not the intent of MDO, but certain circumstances must be examined. Viewed as hands-off for kinetic operations, any foray into the space realm in a provocative and kinetic manner will lead to all nations immediately weaponizing space. This foray is not the intent, and therefore the focus of effort will rely on non-kinetic means to deny space assets. Deterrence in the space domain is the critical enabling function of MDO and is the one that must be thoroughly pressed in future operations.

The denial of space-based capabilities exists within the same framework as any other networked asset at the cyber level. The modification or outright rejection of a satellite system would enable friendly force action while hindering enemy force reactions. Again, this act could be clandestine or very overt, depending on the effect required. Simply by exploiting space-based communications or location assets, Russian IDF forces might be forced to rely on ground-based communications and manual survey methods, which are far better mapped and used for a future attack. This may result in immediate consequences or better develop the intelligence picture for friendly forces. As allied forces prepare for a GPS and satellite denied environment, Russian IDF forces must likewise do the same as “The threat to GPS-reliant systems is diverse: denial and deception of receivers, cyberattacks on the GPS infrastructure, and a variety of other means exist that are unambiguously designed to interrupt our ability to use and trust GPS data."[72] Denial or disruption of space-based capabilities will not result in a wholesale negation of Russian IDF systems but instead adds vector exploitation. This vector will result in a reaction from Russian systems, thereby increasing intelligence gathering capabilities or avenues for an immediate attack.

Network Integration

Network integration is the accumulation, sharing, and distribution of relevant and necessary information across the multi-domain spectrum in real or near-real-time. The integration of information sharing acts within all five military functions, sense, shield, act, sustain, and command, and in both current and future operations. The information gleaned from an ISR asset operating at the tactical level may indirectly feed into strategic decision-making processes without the need for understanding the relevance of the information at each subsequent level.[73] The inability to share information at all levels of command and will be detrimental to both current operations and future planning, "information must be assessed, understood and translated rapidly into successful, integrated battlefield actions."[74] Automatically feeding data into the multi-domain network, expedient information passage becomes the norm, enabling operations, linearly and horizontally.

Network integration is critical to the success of multi-domain operations to reduce and defeat Russian IDF capabilities. It is crucial in all future operations, timely decision-

[72] Neal MacDonald, "Preparing for Artillery Operations in a GPS Denied Environment," *Fires* (May, 2019): 35. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/preparing-artillery-operations-gps-denied/docview/2246858872/se-2?accountid=9867.
[73] Russian Artillery Fire Control for Large-Scale Combat Operations, 9.
[74] Susan Lawrence," Incoming: Multidomain Operations and What Innovation Means for the Future of Warfare," *Signal*, (November, 2019): 56. https://www.afcea.org/content/incoming-multidomain-operations-and-what-innovation-means-future-warfare

making based on the best available information. The dissemination of knowledge at all levels enables both current and future operations against Russian IDF. By combining data sets produced from all domains available, a far superior intelligence picture can be created.[75] The intelligence picture is necessary for multi-domain operations to use the domains to target Russian IDF effectively. By compiling then exploiting intelligence on Russian IDF systems, proper assessments can be made on targets and convergence windows can be established. This systems-based approach enables each domain to target Russian IDF in its own manner, understanding what the other domains are doing and ensuring that resources are not misused or unnecessary.

Understanding the role that network integration plays in defeating Russian IDF can best be examined from the inverse of connectivity, information silos. As mentioned in the previous chapter, the Russian IDF has recently come through a period of reinvigoration and digitization. Russian forces are now far more connected than before and can transmit and receive target information almost instantaneously quickly.[76] This process of digital modernization is ongoing:

> For example, in 2014 Russia established the National Defense Management Center, pursuing the interation of existing communications systems within a single network, as well as the development of UAVs, space-based intelligence, surveillance, and reconnaissance (ISR), and other sensors."[77]

This enables the Russian IDF to further strike targets in-depth, with greater precision, fewer munitions, and at increasing speeds. This allows those same systems to move

[75] Russian Artillery Fire Control for Large-Scale Combat Operations, 10.
[76] The Russian Way of War, 241.
[77] Andrew Radin and others, *The Future of the Russian Military: Russia's Ground Combat Capabilities and Implications for U.S.-Russia Competition*, (Santa Monica, CA: RAND, 2019): 54. Access at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3099/RAND_RR3099.pdf

quickly after engaging targets to disperse the force and reduce the chances of counter-battery fires or other targeting acts. A distinct advantage exists for Russian IDF forces in this example.

Allied forces are without the ability to share information immediately across all domains. A lack of network integration would mean that target acquisition radars capable of determining the firing location of Russian IDF cannot push this information to the sortie of F-35s, which are currently over the battlespace. Also, space command assets are unaware of these targets' location and are not positioning satellites within the area in priority. Cyberwarfare assets are not examining the cellphones within this area in real-time to develop network linkages.

The future of network integration rests with the United States Joint All Domain Command and Control (JADC2) network amongst the U.S. and its allies. The common framework and connection allow the processes of MDO to occur, but this network is still in its infancy and not fully operational. There will be many pains in the operationalization of such a network, integrating vastly different operating systems, manufacturers and end-users all in a single network which must by its very definition be robust, accessible, and persistent. Streamlining of future integration efforts will ensure network compatibility, but in the meantime, legacy systems may require additional time and resources to ensure network capability. As stated previously, though, it remains to be seen if partner nations will have the access necessary without insurmountable filters and firewalls to integrate into the network and become truly integrated. Recent comments by U.S. Northern Command commander General Glen VanHercy on how to increase the speed of implementation across the U.S. and allied forces are heartening towards this fear though.

His comments are, “How can we field innovatively, quickly, these capabilities and assume a little bit of risk while we essentially build them and utilize them right now . . . and have them available not only to us, but to allies and partners, sooner?”[78] This realization may take additional time and resources to rectify but remains a necessity for future warfighting optimization.

The MDO system does not work without network integration. As U.S. Deputy Defense Secretary under President Obama, Bob Work, said of MDO “this effort requires moving beyond mere synchronization of joint capabilities to the complete integration of capabilities.”[79] It is necessary not just to synchronize the backbone of the system but to incorporate network integration across all domains truly.

Conclusion

The destruction, denial, disruption, denigration, and combat capabilities reduction are all victories against Russian IDF systems. The totality of any of these effects does not need to remain permanent for the advantage to swing towards the allied force. It is through the combined impact of MDO that the result is complete.

In examining these select, specific examples, it is clear that Russian IDF systems are not a monolithic force, capable of dominating the future battlefield, but rather a brittle fragment to be exploited in a future war. While these examples are incredibly generic and lack fidelity in their actual operational value, they illustrate that cross-domain fires are capable of winning the fight. The implementation of MDO does not negate the capacity

[78]Courtney Albon, "NORTHCOM EXERCISE DEMONSTRATES READY-TO-FIELD JADC2 CAPABILITIES," *Inside the Pentagon's Inside the Air Force* 32, no. 14 (Apr 09, 2021). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/northcom-exercise-demonstrates-ready-field-jadc2/docview/2510185960/se-2?accountid=9867.

[79] Jordana Mishory, "Work Encourages Army to Continue Efforts on Multidomain Battle." *Inside the Pentagon* 32, no. 40 (Oct 06, 2016). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/work-encourages-army-continue-efforts-on/docview/1826103044/se-2?accountid=9867.

or capability of a single domain to be adequate or win the war. Inversely, each domain acting in concert may not be effective in any given situation. The vital feature of MDO is that it is possible to achieve temporary supremacy over the Russian IDF systems in each of these examples. By amplifying any one of these attacks using an additional vector, the results could be strengthened, sustained, or further obscured, thereby furthering allied forces' advantage.

CHAPTER FOUR - ALLIED IMPLIMENTATION POSSIBILITIES

In examining how multi-domain operations could potentially affect Russian IDF systems, the opportunities expressed were presented vaguely and hypothetically. The crucial piece of information that determines whether MDO is a practical doctrine and is the new path forward for allied militaries is whether those same allied militaries have the forces and capabilities to achieve it. Having the doctrinal framework is excellent, but if the resources, personnel, and networks are not established, it is of little value.

Determining whether Canada, the United States, NATO, and other allied countries have the capabilities to enact MDO is a difficult task within the hypothetical and open-source realm. For instance, the Canadian Surface Combatant procurement has not officially ended, and changes are possible. The same set of circumstances exists for the future fighter program as well as the future RPAS system. Many unknowns are subject to change, but what does live can revolutionize Canada's ability to conduct multi-domain operations and collaborate seamlessly with US armed forces within a decade. Opportunities must be exploited and capabilities truly matched for the future of the CAF.

Land Domain

Canada and its international partners' ability to defeat the Russian IDF threat within the land domain is possible but far from assured. Traditional capabilities that dominated military thinking until the fall of the USSR were replaced with lessons learned over the last two decades of fighting global terrorism. Priorities changed significantly as counter-terrorism operations were prioritized, necessitating today's re-investment in resources.[80] Tactical and operational fires assets were sacrificed for increased capacity in armed UAVs. Air defence assets were divested at the tactical level to reduce funding requirements and maximize other programs as the were seen as unnecessary as the US, Canada and NATO had air supremacy in all operations.[81] The cultural shift towards fighting insurgencies lasted just under two decades, resulting in many warfighting deficiencies in allied armies. While currently weakened, recent efforts within the United States and Canada to invest in these programs have been championed. These efforts will bring renewed capability and warfighting capacity to defeating the Russian IDF threat.

The Canadian Armed Forces (CAF) is significantly vulnerable to Russian IDF threats based on current capabilities. This present truth is being resolved by a reinvigoration of its capacity to defeat the Russian IDF threat in two distinct areas, as well as the long-held practice of operating only within the support and participation of its allies. The first such area is the stated need to reacquire a ground-based air defence (GBAD) system, and the second is the modernization of its indirect fires network.[82] Both of these objectives have been extensively spoken about in other venues and published in the Canadian government's national defence policy, *Strong, Secure, Engaged,* and most recently in the Canadian Army (CA) modernization strategy *Advancing with Purpose*. Detailed is a requirement to bolster the ability to interdict a variety of air threats from a ground-based capability. This GBAD capability speaks directly to defeating several Russian IDF capabilities posed on the modern battlefield.

[80] Canada. Department of National Defence, "Strong Secure, Engaged," (June 7, 2017), 33. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html
[81] Ian Coutts, "Air Defence: Reacquiring a Vital Capability," *Canadian Army Today*, (27 June, 2019). https://canadianarmytoday.com/air-defence-reacquiring-a-vital-capability/
[82] "Advancing with Purpose," 4th Ed, 54.

The modernization of the indirect fires process and systems within the CA will shield Canadian forces from Russian threats and increase its ability to defeat Russian IDF threats. The ability to shield the force with Canadian IDF capabilities is being achieved through network integration across fires platforms, systems, increased sensor connectivity, and the eventual replacement of the main IDF systems. As recommended for the US Army to defeat Russia in a future A2AD environment, Canada should develop a "prototype multi-domain fires battalion to develop, test, and exercise joint and combined defensive concepts."[83] This could operationalize the CAF's divisional fires units while also leveraging allies capabilities. In addition to these factors, it must be assumed that rudimentary artificial intelligence and other hard analytical systems will be implemented to assist in data collation and other networking tasks as this is a CA initiative across all warfighting functions.[84]

In addition to the CA's work in its modernization to defeat the Russian IDF threat, the United States Army and Marine Corps are making concrete and actionable force structure and capability changes that will immediately reduce Russian IDF forces' capacity to dominate the land environment. Like the CA, efforts have been made to reacquire short-range air defence (SHORAD) capabilities to defeat Russian helicopters and aircraft and UAVs with proven adequate IDF spotters in recent conflicts.[85] This capability will add additional lines of effort to Russian IDF forces' defeat, providing much needed protection measures. As well as investing in shield functions, US armed

[83] Timothy Bonds et al, *What Role Can Land-Based, Multi-Domain Anti-Access/Anti-Denial Forces Play in Deterring or Defeating Aggression?* (Santa Monica: RAND Corporation, 2017): xviii. https://www.rand.org/pubs/research_reports/RR1820.html
[84] Ibid, 52.
[85] Integration of Unmanned Aerial Systems within Russian Artillery, 37.

forces are also working towards the modernization of the range of its indirect fire.[86] This will increase its capabilities and enable allied forces to engage additional targets without resorting to higher-level assets.

These Canadian, US, and allied countries' efforts directly respond to Russian aggression and counter their ability to dominate the land domain. The Russian ability to dominate on land is predicated on finding, fixing, and striking targets with IDF. By keeping capacity on the land domain, ensuring that the Russian forces do not dominate this domain, allied forces can leverage other environments to ensure convergence windows are attained and successfully exploited.

Maritime Domain

The maritime domain is a critical element to any future campaign against a peer/near-peer enemy such as Russia. However, it has the most negligible impact on the Russian IDF systems' defeat due to its environment. What is necessary to achieve with allied naval forces is the ability of naval assets to fully integrate within the multi-domain environment, providing command and control nodes, intelligence processing capacity, deep strike fires with surface-to-surface missile systems, and integrated communications chains.[87] This is the critical feature that must continue to be developed as multi-domain operations primary reason for existence is fighting through Russian anti-access area-denial systems (A2AD) and gaining lodgement in theatres of war.[88] This fact does not negate its ability to continue fighting against Russian IDF systems but shapes it to circumstance.

[86] Future Army Cross Domain Fires, 29.
[87] Multidomain Operations and what Innovation Means for the Future of Warfare, 56.
[88] The US Army Multi-Domain Operations 2028, 15.

The Royal Canadian Navy is unable to integrate into multi-domain operations as it currently stands. With ageing frigates and older diesel/electric submarines, it is ill-equipped to conduct MDO against Russian forces. Although unable to fully engage within the networked approach to warfare, it can affect targets using its ship-to-shore missile systems and can be used in extremis situations when in range.[89] Likewise, when in littoral waters they can provide limited air defence coverage which can be used to augment indigenous air defence assets. The future surface combatant ships will have the capacity to be fully integrated within the modern defence networks. However, the critical concern to be addressed is whether they will be capable of integrating within US Navy defence networks in real-time and fifth-generation fighters such as the F-35. As tne scope of the Future Surface Combatant has yet to be fully realized and defined, this remains a mere possibility and not definitive.

As mentioned above, the US Navy is far more capable of engaging in MDO within the maritime domain than any of its allies. As a strike platform, it is capable of engaging targets deep within the enemy battlespace with ship-to-shore-based missiles as well as aircraft strikes from its carrier groups. Additionally, the United States Marine Corps is one of the most joint integrated forces globally and will likely be bolstered shortly to become fully multi-domain capable.[90] The effects on Russian IDF within this sphere are likewise the least potent but still formidable should the United States be forced to break into Europe through the Russian A2AD framework. Allied naval integration into

[89] David Carl, "RCN Conducts First Ship-to-Shore Missile Test," *Jane's Defence Weekly* 53, no. 23 (2016). https://customer-janes-com.cfc.idm.oclc.org/DefenceWeekly/DisplayFile/jdw61544?edition=2016

[90] Lee Hudson, "USMC Focus on all Domain Access in Joint, Combined Forces Wargame," *InsideDefense.Com's SitRep* (Apr 07, 2015). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/usmc-focus-on-all-domain-access-joint-combined/docview/1696928870/se-2?accountid=9867.

MDO will provide a seamless transition from the maritime domain to any entry operation onto a mainland which will assist in command and control issues in complex operations.

Air Domain

The air domain provides an exceptional ability for Western-allied powers to leverage MDO against Russian forces. With the implementation of fifth-generation and supported fourth-generation enhanced fighters, the allied powers are prepared and equipped to conduct all manner of effects within hostile air space, including the destruction of Russian IDF capabilities and systems. The connectivity implemented in existing and new aircraft continues to increase exponentially, ensuring that modern aircraft are not just bombers or fighters but sensor platforms simultaneously.[91] This creates a significant advantage in comparison to enemy opposition.

Canada can vault into multi-domain operational capability within the next decade. Currently, the Royal Canadian Air Force cannot fully integrate its fleet of aircraft within an MDO context due to aircraft age. Within the next decade, with the future fighter's adoption and the acquisition of some RPAS system, the RCAF and the CAF might be fully integrated for future operations.[92] This fact is not a given though due to the variety of options to acquire new aircraft and RPAS systems. However, the RCAF's future is an excellent opportunity to be fully compliant with US and NATO forces, passing tactical information in real-time and acting on the most accurate and timely intelligence. This

[91] F-35 Project Seeks to Overcome EW Obsolescence.

[92] Al Stpehenson "Anatomy of a Buy: The Four Dimension of Procuring a Future Fighter for Canada," *Policy Paper* (May 2019), 3. https://www.cgai.ca/anatomy_of_a_buy_the_four_dimensions_of_procuring_a_future_fighter_for_canada#Requirement

ability will change the way the RCAF would operate in the future wartime scenario and its domestic responsibilities.

The United States Air Force (USAF) is fully capable of multi-domain operations within a coalition and purely along national lines. With the adoption of the F-35 and the F-22 fifth-generation fighters, as well as the fourth-generational plus aircraft such as the F-16 and F-18 Super Hornets, the USAF is well placed to not only defeat the Russian IADS in the A2AD roles but also to prosecute ground targets in-depth and at the tactical level. Leveraging fourth and fifth-generation fighters' ability to conduct their primary functions while simultaneously collecting and disseminating intelligence enables the process of understanding the entire operational picture far easier.[93] The intelligence sharing better develops the deep intelligence picture and the tactical fight in all domains. The cumulative information and intelligence gained from routine operations by all allied air forces operating within an MDO construct ensure tactical and operational excellence, assisting in creating or exploiting convergence windows.

Space Domain

The space domain is a critical advantage for allied forces worldwide, primarily due to the United States' efforts. Since the fall of the USSR, the United States has been a world leader in space-based capabilities that have been leveraged both by civilian enterprise and pure military assets. The Global Positioning System is a fundamental feature of people's daily lives and remains a cornerstone to military operations at home and abroad.[94] Communications satellites continuously orbiting global hotspots ensure

[93] Ibid, 6.

[94] Bernard J. Gruber, Col and Jon M. Anderson Col, "Space Superiority, Down to the Nanosecond: Why the Global Positioning System Remains Essential to Modern Warfare," *Air & Space Power Journal* 27, no.

constant communications ability in theatre and to higher domestic headquarters. And finally, intelligence satellites using all facets of the light spectrum enable real-time data collection and dissemination of tactical to strategic events. [95]

The ability of allied forces, specifically those aligned with the United States and NATO, to dominate in the Space realm is readily acknowledged currently. This does not negate recent strides by Chinese agencies and the continued modernization of Russian GLONASS systems but remains consistent that this is now a US domain. The persistent domination of this domain is not guaranteed, and like the premise behind all multi-domain operations, supremacy will be caveated into a localized advantage during windows of convergence.[96] As noted by the Australian Armed Forces in their 2014 *Future Land Warfare Report 2014*, “A fully digitised force will depend on access to space-based capability for battlefield management, communications and precision navigation and timing (GPS, for example).”[97] Access will be required; it will just not always be accessible.

The space domain’s future remains quite positive for allied forces as US and allied space agencies have continued to build in additional redundancy to space-based assets and features that shield the force from Russian forces attempting to deny the domain. Additional satellites are prepared to be deployed should an issue present itself to ensure that space-based assets fully enable allied forces.[98] As well, a spectrum of

5 (Sep, 2013): 101. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/space-superiority-down-nanosecond-why-global/docview/1475068997/se-2?accountid=9867.

[95] Preparing for Multidomain Warfare, 50.

[96] Future Army Cross Domain Fires, 26.

[97] Australian Defence Force, *Future Land Warfare Report 2014,* Canberra: Directorate of Future land Warfare, April 2014, 27. https://researchcentre.army.gov.au/sites/default/files/flwr_web_b5_final.pdf

[98] Space Superiority, Down to the Nanosecond: Why the Global Positioning System Remains Essential to Modern Warfare, 111.

satellites is currently in orbit to provide intelligence and surveillance activities enabling significant reduction in traditional surveillance tasks for ground or air based sensors. These will continue to operate to significant effect, providing different capabilities to counter Russian-based capabilities.

While there are threats to the space domain's current dominance by allied forces, Canada, the United States, and NATO will continue to persevere in this domain. The United States' efforts to modernize its GPS arrays, allowing for increased signal strengths to bypass most Russian jamming attempts and the increased security surrounding supporting the military codes within the array, will maintain GPS as the dominant precision navigation and timing system in the world.[99] Additionally, increased capacity for the launch of new satellites, either military, commercial, or mixed, will only increase with additional commercial satellite launch companies. This adds extra capacity to a small market, to the benefit of allied countries.

Cyber Domain

The cyber domain is arguably the least effective domain for Canadian and allied forces in comparison to Russian and Chinese states. This does not negate the allied forces' capabilities as these skills must be put in the proper context and suitably operationalized. However, what is required is the sustained prioritization of cyber capabilities to defeat and defend from Russian forces in all domains, specifically within their IDF systems.[100] James Howard, in his article on the future of cross-domain fires stresses this point at the tactical level. He writes "Army and JIM forces face serious

[99] Ibid, 116.

[100] Rebecca Slayton, "What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessments," *International Security* Vol 41, No. 3 (2016): 109. https://direct.mit.edu/isec/article/41/3/72/12149/What-Is-the-Cyber-Offense-Defense-Balance

competition in cyberspace and the EMS, particularly at tactical levels where friendly capabilities are far less mature than those of peer competitors."[101] The prioritization of these efforts will likely not be known unless conventional war is entered. However, effort and forethought must be sustained in peacetime to ensure this endstate is achievable.

As mention in *Strong, Secure, Engaged*, and numerous other government documents, the Canadian effort at increased cyber-warfare must continue to be developed at both the operational and strategic levels. This is ultimately achievable when imagined in a two-front context, one that sees cyberwarfare's practical use on offensive and defensive cyber missions which will achieve Canada's short-term goals. In contrast, the other front sees strategic endstates being achieved over the longterm. There is no operational reason at this time to invest in engaging Russian IDF systems using Canadian cyberwarfare specialists, but this might remain a strategic goal with significant energy. Like many emerging capabilities, cyber is being adopted by each domain as a distinct organization to assist it in achieving its own operational goals. The CA, RCN, and RCAF are all investing in cyber capabilities at the same time as a CAF cyber capability is being established.[102]

Within the Western coalition, the necessity of robust cyberwarfare capabilities is readily agreed upon as a pillar in MDO. Cyber operations not only provide for offensive and defensive operations but enable all other operations as well. It acts as the lynchpin between operations and domains:

[101] Future Army Cross-Domain Fires, 25.

[102] Canada. Department of National Defence, "Canadian Armed Forces Cyber Activities," *Supplementary Estimates A 2019-2020 – Appearance of the Minister of National Defence Before the Committee of the Whole*. Last modified 07 April 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html

> Cyberspace and EMS superiority are not only a critical enabler for all joint functions, but it fosters the cross-domain integration essential to success in any major combat operation. Achieving EMS superiority is a precondition for successful joint combined arms operations.[103]

The backbone of any future allied network integration initiative is defensive cyber capabilities, which remains opaque to those outside this specialty. Open-source material cannot answer the question as to how capable the defensive measures are surrounding its networks. However, it is safe to assume that future operations will rely on allied countries' ability to defend their military information networks and resource accordingly.[104]

Cyber operations are uncertain at the tactical and operational level of war for allied armies. This is not a result of their capabilities but their ability to be operationalized at the appropriate level. This is the current unknown within the defence community and is the area in which the most action must be taken. How does a Brigade use a cyber attack to achieve a local effect necessary to achieve localized dominance but not invest six months of research and time, and resources into achieving it? Tjhis problem of course is a contextual one as well and will likely diminish in the future as cyber capabilities are integrated at lower levels annually. Commanders who have the opportunity to integrate cyber must take the opportunity immediately. As Stephanie Seward writes in her article *Cyberwarfer in the Tactical Battlespace* "Maneuver commanders need to ensure they understand what cyber enablers bring to the fight.

[103] James Howard, "Future Army Cross Domain Fires: Bridging tomorrow's implications with initiatives today," *Fires* (2017): 25.
[104] What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessments, 109.

Commanders who understand cyber enablers can drive requirements at all levels."[105] On the same note, how does a Brigade defend itself from cyber intrusion attempts, or is this a national issue? These questions are not meant to waylay the future of cyber warfare but need to be examined by Canada, the United States and its allies to achieve some of the effects described in previous chapters. It is about empowering the tactical to achieve the operational and vice versa.

Allied Network Integration

Network integration is the crux in the MDO construct which will, by necessity, enable or disadvantage the allied fight. Without the ability to share tactical, operational, and strategic information and intelligence in real-time, allied forces will not fully appreciate multi-domain operations' ability.[106] The architecture to enable this type of information sharing is understandably highly complex. The integration of partner nations, never mind just the individual military services, into a single command and control structure is daunting. This is the hurdle that must be vaulted but which is currently unable.

The Joint All Domain Command and Control (JADC2) battle management system is the latest attempt at including all domains within a single command and control architecture, led by the United States. JADC2 sees all operative domains enabled using a single system, coordinating and controlling the effects for entire regions and theatres, ensuring that any action is taken within an all-domain perspective. This network enables single domains that populate its matrixes and the other domains through information

[105] Stephanie J. Seward, "Cyberwarfare in the Tactical Battlespace: An Intelligence Officer's Perspective," *Infantry* 107, no. 2 (Apr, 2018):14. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/cyberwarfare-tactical-battlespace-intelligence/docview/2118247860/se-2?accountid=9867
[106] The US Army Multi-Domain Operations 2028, 47.

sharing and common operating picture.[107] While this system is not fully functional, enabled by all domains, it is the start of increased cooperation across the many domains. The critical challenge that will be faced next is not integrating multiple domains and services within the JADC2 system but the necessity of integrating allied domains within the same architecture to provide seamless participation and integration.

One avenue of network integration that will have to be addressed is the open and accessible dissemination of information amongst allies in operations. Modern fully integrated systems, nested within the MDO concept, cannot work without the inherent requirement to share information without caveats. As Douglas Creviston writes in his article published in *Joint Force Quarterly* in 2020:

> The chain of command should be given a right to share authority over all information the commander has access to for all members, U.S. and coalition, under his or her command. This right to share will likely require limits to protect strategic interests and/or prevent the present chain of command from reaping current rewards at the cost of increased future risk.[108]

As noted above, some information must be withheld, but the vast majority of information must be shared expeditiously. The ability to share extensive data sets to enable better and faster decision-making is a force-multiplier over Russian forces. The immediate and unequivocal sharing of data and intelligence is crucial to defeating the Russian IDF threat.

[107] Ibid, C-1.

[108] Douglas Creviston, "Transforming DOD for Agile Multidomain Command and Control," *Joint Force Quarterly*, no.97 (2020): 89. https://search-proquest-com.cfc.idm.oclc.org/docview/2394262825?pq-origsite=summon

CHAPTER FIVE – CANADIAN IMPLICATIONS AND OPPORTUNITIES

The Canadian Armed Forces are ill-equipped and unprepared to defeat the Russian indirect fire threat using multi-domain operations. The CAF's capabilities on land are woefully inadequate or non-existent. In the air domain, Canada lacks the modern fifth-generation fighters to prosecute targets in an A2AD environment. Our naval vessels are ageing ungracefully and unable to keep pace with modern US networked fleets. Our cyber capabilities are still in their infancy, as are our space-based satellites. The fact of the matter is that Canada cannot defeat this threat now and must change in the short-term to ensure that any future fight is fought on Canada's terms. The change in future doctrine has come at an auspicious time for the CAF as it looks to replace its critical platforms at sea and in the sky, with central procurement happening concurrently on land. Adding new emphasis and capabilities to its cyber warfare division and additional space-based assets only enhances its prospects. The CAF can not only remedy its pitiful state for contemporary operations but can do so within the next decade.

To defeat the Russian IDF threat, the CAF must embrace MDO and modernize its warfighting capabilities. This opportunity must be welcomed at the political, strategic, operational, and tactical levels to be truly successful. Not only embrace, but the integration process must also be facilitated at each level, so underlying reasons and concepts are fully realized. The transition to MDO requires the new generation of soldier/sailor/aviator to believe in network integration, data analytics, and digitization for this to be successful. The opportunity is arisen and must be grasped as rival forces have adopted it themselves. Within the Canadian Army, the dependency upon the other domains as well as other key enablers is understood fully. Within its capstone operating concept, *Close Engagement: Land Power in an Age of Uncertainty*, the Army fully articulates its need for integration and coordination, “other CAF capabilities will play a pivotal role in generating effective land power. The capability development goals of the Army must therefore remain aligned with those of the RCAF, the RCN and other CAF components.”[109] Working together is the future of all domains and the CAF will need to appreciate this reality in short order.

The land domain, the primary domain bearing responsibility for the destruction of the Russian IDF threat, needs to privilege the Brigade level with additional resources and capabilities to become fully integrated into the modern theatre. As stated in *Advancing with Purpose*, the brigade is the lowest level of joint integration as it has the staff and capabilities to embrace those roles fully.[110] The brigade is capable but lacks the networking capabilities and critical enablers to achieve this aim. Investment in GBAD, RPAS, digital communications, and modernized indirect fires systems will enable the Canadian Mechanised Brigade Group to defeat numerically superior Russian forces, specifically their indirect fire systems. Investment though must be made now and cannot be delayed for the normal procurement processes that are far too long in duration and ineffective in procuring relevant technologies directly.

The maritime domain for the Canadian Armed Forces is ripe for an incredible explosion of capabilities and capacity within the next generation. As the future surface combatant project gets underway, along with the ongoing Arctic and Offshore Patrol Vessels production, the ability to integrate multi-domain operations into their project

[109] Canada, Department of National Defence, *Close Engagement: Land Power in an Age of Uncertainty: Evolving Adaptive Dispersed Operations*, (Kingston, ON: Canadian Army Land Warfare Centre, 2019): 47. http://publications.gc.ca/collections/collection_2019/mdn-dnd/D2-406-2019-eng.pdf
[110] Advancing with Purpose, 17.

spine is unparalleled. By incorporating the fundamental operating concepts which presuppose MDOs, the Royal Canadian Navy (RCN) can form a strong pillar in any future Canadian doctrine.[111] In addition to acting in a multi-domain operation domestically and with Canadian allies, the RCN can lead the CAFs integration effort. Providing long-range fires, integrating air defence capabilities in littoral waters, harnessing communications capabilities to act as relay stations or command and control nodes will all be possible with these vessels. The RCN must embrace these upcoming integration opportunities with all partners.

In a similar opportunity space to the RCN, the Royal Canadian Air Force (RCAF) poises itself to slingshot into a fully integrational multi-domain partner within the decade. Investment in the future fighter program, leveraging at least fourth-generation plus aircraft, will ensure the RCAF's ability to integrate into modern aerial combat operations with allied partner nations.[112] Realizing the RCAF's ability to operate within A2AD airspace or at least contested airspace will ensure freedom of manoeuvre abilities for friendly forces on the ground and sea. These future fighters' ability to penetrate enemy airspace with a reasonable opportunity to conduct deep fires against high-value Russian IDF targets changes the modern battlefield dynamics.[113] Stripping the enemy of its deep strike assets will allow freedom of action for allied forces. The best accomplishment of

[111] Canada. Department of National Defence, “Canadian Surface Combatants,” (18 Feb, 2021). http://www.navy-marine.forces.gc.ca/en/fleet-units/csc-home.page

[112] Al Stephenson, “Anatomy of a Buy: The Four Dimension of Procuring a Future Fighter for Canada,” *Canadian Global Affairs Institute* (Policy Paper), (May 2019): 5. https://www.cgai.ca/anatomy_of_a_buy_the_four_dimensions_of_procuring_a_future_fighter_for_canada#Requirement

[113] Jeff Harrigian and Max Marosko, “Fifth Generation Air Combat: Maintaining the Joint Force Advantage,” *Joint Air Power Competence Centre*, no. 24. (Spring/Summer, 2017): 55. https://www.japcc.org/fifth-generation-air-combat/

these abilities lies within the MDO framework, and the RCAF is on the cusp of championing this effort.

The Canadian Armed Forces are unprepared for future cyber operations and will face many challenges into the next decade to rectify this deficiency. The CAF capability is increasing at an alarming rate, but the ability to train future cyber operators is lengthy and complicated.[114] This fact directly influences the rates of operator employment. The capability can be increased but will face complex retention issues in the future. These factors are working against a true cyber warfare capability within the CAF, but each service is committed to increasing its cyber ability for the future. The dedication to implementing a cyber capability is promising, but the CAF must harmonize and operationalize its cyber warfare capability in a concise term. This short-term strategy will allow for greater interoperability with allied partners and the potential to take advantage of their training and operational opportunities.

Lastly, the CAF is relatively well-positioned to capitalize on the space domain in the future decades. Relying on US and allied position and timing capabilities has allowed the CAF to specialize in other space capabilities proven effective in the North and specific imagery-based abilities. Using these facts as a backstop, the CAF is well situated to continue to specialize in its space-based capabilities with spare capacity to reinvest in Northern targeted capabilities.[115] While not directly impacting the fight against Russian IDF capabilities, having access to the US and allied powers, while also augmenting when

[114] Alex Ardnt, "Cyber Operations in the Canadian Armed Forces," PowerPoint presentation, (01 Nov, 2018): 27-30. https://www.countermeasure.ca/wp-content/uploads/2018/01/documents_2018_presentations_Alex-Arndt-IT_Security_VS_Defensive_Cyber_Operations.pdf
[115] Canada, Department of National Defence, "Space Capabilities," (12 Oct, 2020). http://www.rcaf-arc.forces.gc.ca/en/space/capabilities.page

able with our own, Canada is well-positioned to continue to increase its capacity with new satellite launches, ensuring they are compatible with a multi-domain approach.

The single most significant capability that the CAF will approach within the next decade and beyond is its ability to integrate networks. Data integration and processing in the future of warfare that the CAF could wage in the short-term. Using the recently created position of Senior Advisor on Future Capabilities, LGen Rouleau is poised to shepherd network integration into the forefront.[116] In his appointment, LGen Rouleau can ensure that future projects, specifically IDF modernization, GBAD, Future Surface Combatant, Future Fighter Program, and the upcoming RPAS project, can integrate. Ensuring that these assets and capabilities can communicate in real-time in a warfighting scenario will ensure Canada's preparation for future conflict. Should any of these projects be excluded from network integration requirements, the future multi-domain fight will become far more complex and expensive.

As mentioned before, Canada is well-positioned to move quickly and authoritatively into an MDO footing. What is needed is to achieve this is the ruthless prioritization of acquiring new capabilities and resources, controlled at the highest levels to ensure compatibility and ability. Additionally, the most extraordinary effort to obtain these resources must be championed to achieve the most excellent effect. Every future acquisition of new equipment and technology will not be compatible with multi-domain operations, but support for the showcase procurement projects must occur. Integration of the future fighter, future surface combatant, digital enabler, and the network spine must occur to ensure the full integration of domains. Should full network integration not be

[116] Canada, Department of National Defence, “CANFORGEN 022/21 CMP 013/21 081349Z MAR 21- Promotions and Senior Appointments 2021 – General and Flag Officers.” (08 Mar, 2021).

achieved in any domain, the results will not be catastrophic but will see a degradation in understanding and effect into the future. Hope springs eternal in many things, but military procurement and technology are a fool's gamble.

CONCLUSION

Multi-domain operations demonstrate the ability to exploit and dominate the Russian indirect fires capability now and into the future. Targeting these systems, the heart and soul of the Russian land forces, to defeat them is critical to future conflict. The defeat of the Russian fires network is easily accomplished using a multi-domain approach, negating the advantage in Russian firepower. With future pan-domain network integration and the acquisition of new compatible equipment, Canada can significantly influence this scenario into the future. Without immediate investment in capital and thought, Canada will quickly be relegated to third-tier status and left on the sidelines of future global action. Relegation to the sidelines of international affairs and warfare is not what Canada and its allies desire, and hard choices must be made to secure the future of our choosing.

Multi-domain operations will not work as it currently stands within Western militaries as a severe change in thought processes must occur before a revolution in warfare is possible. The next step for research in this field is cultural change, which must occur before new and emerging technologies enter the realm. The historical nature of war has cemented thought in discussion of domains and continues to be impressed upon new soldiers, sailors, and aviators.

Identification of which branch of the military, beginning at the first onset of one's career, and the resultant self-identification is anathema to MDO. Thinking must start as a pan-domain from these early instances and continue throughout one's career. This change must be realized before true multi-domain thought can flourish. Knowing that the enemy is vulnerable may bring about immediate change in tactics and equipment. However, long-term change management is necessary to solidify the advantage and become a genuinely multi-domain operational force.

The avenues of discussion and exploitation that I present here are generic and work to illustrate the advances possible against the Russian IDF systems. The best use of this examination is as a primer for thought into future review of adversarial capabilities and systems while advancing a better understanding of multi-domain action to achieve the desired effect. IDF systems were the chosen target for this thesis as they exist as the enemies' centre of gravity, but this obviously could change. Future airframes and surface combatants will likewise integrate new technologies and be vulnerable to further attacks from unknown vectors, and this is what MDO seeks to achieve. Future academic work will only strengthen the case for multi-domain operations as the operational construct to defeating Russian forces but it is for the Western allies to implement now.

BIBLIOGRAPHY

Albon, Courtney. "NORTHCOM Exercise Demonstrates Ready-To-Field JADC2 Capabilities." *Inside the Pentagon's Inside the Air Force* 32, no. 14 (Apr 09, 2021). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/northcom-exercise-demonstrates-ready-field-jadc2/docview/2510185960/se-2?accountid=9867.

Alexander, Dean. "Cyber Threats in the 21st Century." *Security*, (September 2012): 70-76. https://search-proquest-com.cfc.idm.oclc.org/docview/1223497697?pq-origsite=summon

Amos, Fox. "Understanding the Modern Russian War: Ubiquitous rocket, artillery to enable battlefield swarming, siege warfare." *Fires*. (September – October, 2017) 20-25. https://search-proquest-com.cfc.idm.oclc.org/docview/2101833448?pq-origsite=summon

Ardnt, Alex. "Cyber Operations in the Canadian Armed Forces." PowerPoint presentation (01 Nov, 2018). https://www.countermeasure.ca/wp-content/uploads/2018/01/documents_2018_presentations_Alex-Arndt-IT_Security_VS_Defensive_Cyber_Operations.pdf

Atkins, Sean A. "Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace." *Air and Space Power Journal* Vol 32, No. 3 (Fall 2018): 26-44. https://search-proquest-com.cfc.idm.oclc.org/docview/2099885702?pq-origsite=summon

Australian Defence Force. *Future Land Warfare Report 2014*. Canberra: Directorate of Future land Warfare, April 2014. p. 3-24. https://researchcentre.army.gov.au/sites/default/files/flwr_web_b5_final.pdf

Bartles, Charles K. and Roger N. McDermott. "Russia's Military Operation in Crimea." *Problems of Post-Communism* Vol 61, No. 6 (2014): 46-63. https://www-tandfonline-com.cfc.idm.oclc.org/doi/abs/10.2753/PPC1075-8216610604

Bonds, Timothy et al. *What Role Can Land-Based, Multi-Domain Anti-Access/Anti-Denial Forces Play in Deterring or Defeating Aggression?* Santa Monica: RAND Corporation, 2017. https://www.rand.org/pubs/research_reports/RR1820.html

Boston, Scott and Dara Massicot. *The Russian Way of Warfare: A Primer*. Santa Monica: RAND Corporation, 2017. https://www.rand.org/pubs/perspectives/PE231.html

Canada. Department of National Defence. "Canadian Armed Forces Cyber Activities." *Supplementary Estimates A 2019-2020 – Appearance of the Minister of National Defence Before the Committee of the Whole*. Last modified 07 April 2020. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/cow-estimates-a-2019-20/joint-capabilities.html

—. Department of National Defence. "CANFORGEN 022/21 CMP 013/21 081349Z MAR 21- Promotions and Senior Appointments 2021 – General and Flag Officers." (08 Mar, 2021).

—. Department of National Defence. *Close Engagement: Land Power in an Age of Uncertainty: Evolving Adaptive Dispersed Operations*. Kingston, ON: Canadian Army Land Warfare Centre, 2019. http://publications.gc.ca/collections/collection_2019/mdn-dnd/D2-406-2019-eng.pdf

—. Department of National Defence. "Space Capabilities." Last modified 02 October 2020. http://www.rcaf-arc.forces.gc.ca/en/space/capabilities.page

Carl, David. "RCN Conducts First Ship-to-Shore Missile Test," *Jane's Defence Weekly* 53, no. 23 (2016). https://customer-janes-com.cfc.idm.oclc.org/DefenceWeekly/DisplayFile/jdw61544?edition=2016

Cotet, Florin. "Apsects Regarding the Use of Field Artillery in Contemporary Operations." *Bulletin of "Carol I" National Defense University* 8, no. 1 (2019): 35-39. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/aspects-regarding-use-field-artillery/docview/2371519352/se-2?accountid=9867

—. "Harmonizing Field Artillery Entities With Similar Nato Field Artillery Units In The Current Complex Battlespace." In *"Carol I" National Defence University*, 2019. https://search-proquest-com.cfc.idm.oclc.org/conference-papers-proceedings/harmonizing-field-artillery-entities-with-similar/docview/2237828139/se-2?accountid=9867

Coutts, Ian. "Air Defence: Reacquiring a Vital Capability," *Canadian Army Today*, 27 June 2019. https://canadianarmytoday.com/air-defence-reacquiring-a-vital-capability/

Creviston, Douglas. "Transforming DOD for Agile Multidomain Command and Control." *Joint Force Quarterly* no. 97 (2020): 83-90. https://search-proquest-com.cfc.idm.oclc.org/docview/2394262825?pq-origsite=summon

Depczynski, Marek. "Renaissance of Russian high-Powered Artillery." *Scientific Journal of the Military University of Land Forces*, Vol 51, No 4 (2019): 616-632. DOI: 10.5604/01.3001.0013.6455 https://zeszyty-naukowe.awl.edu.pl/resources/html/article/details?id=195930&language=en

Fish, Tim. "Europe Ponders SEAD Modernization as Russia Fields New Threats." *The Journal of Electronic Defense* (May, 2018): 26-34. http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/detail/detail?vid=0&sid=c7f856f5-60ed-4d9e-aded-

2198633088f8%40sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=mth&AN=129625407

Gruber, Bernard J., Col and Jon M. Anderson Col. "Space Superiority, Down to the Nanosecond: Why the Global Positioning System Remains Essential to Modern Warfare." *Air & Space Power Journal* 27, no. 5 (Sep, 2013): 98-119. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/space-superiority-down-nanosecond-why-global/docview/1475068997/se-2?accountid=9867

Gomez, Cesar. "Cybersecurity of unmanned aircraft systems (UAS)." Master's thesis, Utica College, 2015. https://search-proquest-com.cfc.idm.oclc.org/docview/1750068515/fulltextPDF/78CB7A5D050941A1PQ/1?accountid=9867

Gordon, John IV, Igor Mikolic-Torreira, D. Sean Barnett, Katharina Ley Best, Scott Boston, Dan Madden, Danielle C. Tarraf, and Jordan Willcox. *Army Fires Capabilities for 2025 and Beyond*. Santa Monica: RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR2124.html

Gartzke, Eric and Jon R. Lindsay. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York: Oxford University Press, 2019. doi:10.1093/oso/9780190908645.001.0001. https://ebookcentral.proquest.com/lib/cfvlibrary-ebooks/reader.action?docID=5647786

Grau, Lester and Chuck Bartles. "Integration of Unmanned Aerial Systems within Russian Artillery." *Fires* (Jul, 2016): 31-38. https://search-proquest-com.cfc.idm.oclc.org/docview/1823336156?accountid=9867

—. "Russian Artillery Fire Control for Large-Scale Combat Operations." *Fires* (May, 2019): 7-14. https://search-proquest-com.cfc.idm.oclc.org/docview/2246860502?accountid=9867

— . *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces.* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016). https://www.armyupress.army.mil/Portals/7/Hot%20Spots/Documents/Russia/2017-07-The-Russian-Way-of-War-Grau-Bartles.pdf

Green, James A. *Cyber Warfare: A Multidisciplinary Analysis*, edited by Green, James A. 1st ed. Abingdon, Oxon; New York, NY;: Routledge, 2015.

Guelfi, Edward A., Buddhika Jayamaha, and Travis Robison. "The Imperative for the U.S. Military to Develop a Counter-UAS Strategy." *Joint Force Quarterly* no. 97 (Second, 2020): 4-12. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/imperative-u-s-military-develop-counter-uas/docview/2394262817/se-2?accountid=9867

Harrigian, Jeff and Max Marosko. "Fifth Generation Air Combat: Maintaining the Joint Force Advantage." *Joint Air Power Competence Centre*, no. 24. (Spring/Summer, 2017): 54-60. https://www.japcc.org/fifth-generation-air-combat/

Harris, Albert. "Preparing for Multidomain Warfare: Lessons from Space/Cyber Operations." *Air & Space Power Journal* 32, no 3 (Fall, 2018): 45-61. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/preparing-multidomain-warfare-lessons-space-cyber/docview/2099884315/se-2?accountid=9867

Host, Pat. "US Air Force analysing future of multi-domain C2." *Jane's Defence Weekly* (26 July 2017). https://customer-janes-com.cfc.idm.oclc.org/Janes/Display/FG_595364-JDW

Howard, James. "Future Army Cross Domain Fires: Bridging Tomorrow's Implications with Initiatives Today." *Fires* (2017): 25-29. https://search-proquest-com.cfc.idm.oclc.org/docview/1902443780?pq-origsite=summon

Hudson, Lee. "USMC Focus on all Domain Access in Joint, Combined Forces Wargame," *InsideDefense.Com's SitRep* (Apr 07, 2015). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/usmc-focus-on-all-domain-access-joint-combined/docview/1696928870/se-2?accountid=9867

Jensen, Benjamin, Brandon Valeriano & Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist." *Journal of Strategic Studies*, 42:2, (2019): 212-234, DOI: 10.1080/01402390.2018.1559152 https://www-tandfonline-com.cfc.idm.oclc.org/doi/epub/10.1080/01402390.2018.1559152?needAccess=true

Kane, Kiernan. "Adapting Towed Artillery Today to Meet a Near-Peer Competitor Tomorrow." *Fires* (Sep, 2017): 26-29. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/adapting-towed-artillery-today-meet-near-peer/docview/2101836407/se-2?accountid=9867

Karber, Phillip. "Lessons Learned" from the Russo-Ukrainian War." (Draft Document). The Potomac Foundation, 6 July 2015. https://prodev2go.files.wordpress.com/2015/10/rus-ukr-lessons-draft.pdf

Konaev, Margarita. "The Future of Urban Warfare in the Age of Megacities." *Focus stratégique, IFRI*, March 2019. https://www.ifri.org/sites/default/files/atoms/files/konaev_urban_warfare_megacities_2019.pdf

Kostyak, Nadia and Yuri Zhukov. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" *Journal of Conflict Resolution* Vol. 63, No. 2 (2019): 317-347. https://journals-sagepubcom.cfc.idm.oclc.org/doi/full/10.1177/0022002717737138?utm_source=summon&utm_medium=discovery-provider

Lawrence, Susan. "Multidomain Operations and what Innovation Means for the Future of Warfare." *Signal* 74, no. 3 (11, 2019): 56. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/multidomain-operations-what-innovation-means/docview/2458971154/se-2?accountid=9867

MacDonald, Neal. "Preparing for Artillery Operations in a GPS Denied Environment." *Fires* (May, 2019): 34-37. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/preparing-artillery-operations-gps-denied/docview/2246858872/se-2?accountid=9867

Merrin, William. *Digital War: A Critical Introduction*. 1st ed. Abingdon, Oxon;New York, N.Y;: Routledge, Taylor & Francis Group, 2019.

Mishory, Jordana. "Work Encourages Army to Continue Efforts on Multidomain Battle." *Inside the Pentagon* 32, no. 40 (Oct 06, 2016). https://search-proquest-com.cfc.idm.oclc.org/trade-journals/work-encourages-army-continue-efforts-on/docview/1826103044/se-2?accountid=9867

Myers, Adam. “Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units.” *Crowdstrike* (blog), Crowdstrike, December 22, 2016. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/

Petraitis, Daivis. "The Russian Military Reform 2005-2015." *Lithuanian Annual Strategic Review* 9, no. 1 (2011): 139-171. doi:http://dx.doi.org.cfc.idm.oclc.org/10.2478/v10243-012-0003-6. https://search-proquest-com.cfc.idm.oclc.org/scholarly-journals/russian-military-reform-2005-2015/docview/1323403804/se-2?accountid=9867

Radin, Andrew. *The Future of the Russian Military: Russia’s Ground Combat Capabilities and Implications for U.S.-Russia Competition*. Santa Monica: RAND, 2019. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3099/RAND_RR3099.pdf

Reilly**,** Jeffrey M. “Multidomain Operations: A Subtle but Significant Transition in Military Thought.” *Air & Space Power Journal***,** Vol. 30 Issue 1 (Spring 2016): 61-73. http://web.b.ebscohost.com.cfc.idm.oclc.org/ehost/detail/detail?vid=2&sid=041a1d03-2c0d-4299-ab9f-12e5452f9968%40sessionmgr102&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#AN=113399783&db=a9h

Schmid, Joseph and Adam Wilson Jr. "Calling for Improvements on US Army's Cannon Artillery." *Fires* (Nov, 2017): 50-55. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/calling-improvements-on-us-armys-cannon-artillery/docview/2101842153/se-2?accountid=9867

Seward, Stephanie J. "Cyberwarfare in the Tactical Battlespace: An Intelligence Officer's Perspective." *Infantry* 107, no. 2 (Apr, 2018): 10-14. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/cyberwarfare-tactical-battlespace-intelligence/docview/2118247860/se-2?accountid=9867

Sharkey, Noell. “The Automation and Proliferation of Military Drones and the Protection of Civilians.” *Law, Innovation and Technology*, 3:2 (2011): 229-240. DOI: 10.5235/175799611798204914. https://www-tandfonline-com.cfc.idm.oclc.org/doi/abs/10.5235/175799611798204914

Slayton, Rebecca. “What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessments.” *International Security* Vol 41, No. 3 (2016): 72-109. https://direct.mit.edu/isec/article/41/3/72/12149/What-Is-the-Cyber-Offense-Defense-Balance

Stephenson, Al. “Anatomy of a Buy: The Four Dimension of Procuring a Future Fighter for Canada.” *Policy Paper* (May 2019). https://www.cgai.ca/anatomy_of_a_buy_the_four_dimensions_of_procuring_a_future_fighter_for_canada#Requirement

Torruella, Anika. "F-35 Project Seeks to Overcome EW Obsolescence." *International Defence Review* 46, no. 11 (2013). https://customer-janes-com.cfc.idm.oclc.org/InternationalDefenceReview/DisplayFile/idr16067?edition=2013

Ullian, Rick. "Bursting the Russian Integrated Air Defense System Bubble." *Fires* (Jul, 2017): 40-45. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/bursting-russian-integrated-air-defense-system/docview/2101836477/se-2?accountid=9867

United States. *The U.S. Army in Multi-Domain Operations 2028*. (United States: Army Training and Doctrine Command, 2018). https://www.hsdl.org/?abstract&did=820569

"U.S. Army War College: Space Assets Enable Multi-Domain Operations," *Targeted News Service*, May 21, 2019. https://search-proquest-com.cfc.idm.oclc.org/newspapers/u-s-army-war-college-space-assets-enable-multi/docview/2233217006/se-2?accountid=9867

Yeadon, Steven. "Toward Understanding Fires on Near-Peer Battlefield." *Fires* (Sep, 2019): 59-63. https://search-proquest-com.cfc.idm.oclc.org/trade-journals/toward-understanding-fires-on-near-peer/docview/2314499511/se-2?accountid=9867