Spacepower and Malicious Non-State Actors

A Monograph

by

Major Paul R. Kellmurray
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2021

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
20-05-2021	Monograph	JUN 2020 – MAY 2021

4. TITLE AND SUBTITLE
Spacepower and Malicious Non-State Actors

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Major Paul R. Kellmurray

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ADVANCED MILITARY STUDIES PROGRAM

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

A recent, and underappreciated, development is occurring in the space domain with the ability of Malicious Non-State Actors (MNSA) to harness space-based capabilities to conduct operations. MNSA uses technologies such as Satellite Communication (SATCOM) and the Global Position System (GPS) to increase their operational reach by using the space domain to link small operations across multiple domains. The use of space for warfighting has been the traditional realm of powerful nation-states such as the United States. This monograph investigates how current US spacepower concepts and doctrine is insufficient to respond to MNSA using space-enabled capabilities.

The advent of MNSA use of space requires a shift in American operational and doctrinal thinking of what or who constitutes a spacepower. MNSA such as Lebanese Hezbollah, Lashkar-e-Taiba (LeT), and Islamic State of Iraq and Syria (ISIS) have demonstrated an ability to adopt space capabilities to conduct operations to achieve their organizational goals. The examples of Hezbollah, LeT, and ISIS, when compared to current US spacepower concepts and doctrine, shows a gap in the current spacepower theory paradigm. This gap in thinking suggests that a change is needed in current US doctrine and concepts to better prepare for the emergence of new hostile space powers.

15. SUBJECT TERMS
Spacepower, Hezbollah, LeT, ISIS, Paradign, Domains, Space Capabilites

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Paul R. Kellmurray
(U)	(U)	(U)	(U)	50	**19b. PHONE NUMBER** *(include area code)* 254 423 9144

Monograph Approval Page

Name of Candidate: Major Paul R. Kellmurray

Monograph Title: Spacepower and Malicious Non-State Actors

Approved by:

_//Signed/6 April 2021/JKG//_____, Monograph Director
James K. Greer, PhD

_//Signed/6 April 2021/MTA//_____, Seminar Leader
Matthew T. Archambault, COL

_____//signed/14 MAY/BAP//___ _____ __, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 20th day of May 2021 by:

_____, Assistant Dean of Academics for Degree Programs
Dale F. Spurlin, PhD and Research, CGSC

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Abstract

Spacepower and Malicious Non-State Actors, by MAJ Paul Kellmurray, 50 pages.

A recent, and underappreciated, development is occurring in the space domain with the ability of Malicious Non-State Actors (MNSA) to harness space-based capabilities to conduct operations. MNSA uses technologies such as Satellite Communication (SATCOM) and the Global Position System (GPS) to increase their operational reach by using the space domain to link small operations across multiple domains. The use of space for warfighting has been the traditional realm of powerful nation-states such as the United States. This monograph investigates how current US spacepower concepts and doctrine is insufficient to respond to MNSA using space-enabled capabilities.

The advent of MNSA use of space requires a shift in American operational and doctrinal thinking of what or who constitutes a spacepower. MNSA such as Lebanese Hezbollah, Lashkar-e-Taiba (LeT), and Islamic State of Iraq and Syria (ISIS) have demonstrated an ability to adopt space capabilities to conduct operations to achieve their organizational goals. The examples of Hezbollah, LeT, and ISIS, when compared to current US spacepower concepts and doctrine, shows a gap in the current spacepower theory paradigm. This gap in thinking suggests that a change is needed in current US doctrine and concepts to better prepare for the emergence of new hostile space powers.

Contents

Acknowledgments

I would like to acknowledge and express my deep gratitude to my monograph director, Dr. James Greer, for his mentorship and trust as I explored the ideas within this monograph. I am also thankful for the challenging and wide-ranging conversations with MAJ Jerry Drew and CPT Duane Kelley that always sharpened my thinking. I am also in the debt of Ms. Bonnie Joranko for her feedback, editing, and formatting that assisted me with the completion of this monograph. Finally, and most importantly, I would like to thank my wife Holly. Her patience, support, and eagerness to read and challenge my ideas was indispensable.

Abbreviations

D3SOE	Denied, Degraded, and Disrupted Space Operating Environment
DOD	Department of Defense
DOTMLPF-P	Doctrine, Organizational, Training, Material, Leadership, Personnel, Facilities and Policy
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IDF	Israeli Defense Force
ISIS	Islamic State of Iraq and Syria
ISR	Intelligence Surveillance and Reconnaissance
JP	Joint Publication
LeT	Lashkar-e-Taiba
MDO	Multi-Domain Operations
MNSA	Malicious Non-State Actors
PNT	Position, Navigation, Timing
SATCOM	Satellite Communications
UAV	Unmanned Aerial Vehicles
USSF	US Space Force

Figures

Tables

Introduction

The United States faces an increasingly complex security environment with the resurgence of great power competition combined with advanced and ubiquitous technologies. The focus of many studies and inquiries has been to analyze an ascendant China and a revisionist Russia. However, the United States and its partners still face the challenge of low-intensity conflict, small wars, counterinsurgencies, and counterterrorism throughout the globe. The advancement, proliferation, and diffusion of technologies have a significant impact on the outlook on these small wars. These technologies create opportunities to access and use sophisticated domains such as space and cyberspace. This study aims to analyze how space technology affects the way malicious non-state actors (MNSA) are capitalizing on their varying levels of access to space in ways not conceptualized by the US military.

MNSA is the term chosen for this study because not all non-state actors use violence to achieve their goals.[1] MNSA includes terrorists and insurgents with violent means, but it also includes those with the technical capability to achieve effects in space and cyberspace with non-kinetic systems. These groups operate at varying levels of sophistication around the globe. What they share is a general willingness to adopt tactics and technologies to achieve their ends. These groups will continue to evolve regardless of whether they hold the United States' attention at any given moment.

If the US military has not thoroughly conceptualized how MNSA are using space in increasingly sophisticated ways, what does that mean for the future of US military operations? If a gap in appreciation of MNSA sophistication exists, is it a matter of doctrine, arrogance, or language? What changes must the United States make to avoid losing its perceived asymmetric

[1] Rachel A. Gabriel and Barnett S. Coven, "Malicious Non-state Actors and Contested Space Operations," NSI Inc., February 2018, 4, accessed August 2, 2020, https://nsiteam.com/malicious-non-state-actors-and-contested-space-operations/.

advantage in space to MNSA? The answers to these questions are likely found in the analysis of the current intellectual paradigm regarding the space domain.

Dr. Gregory D. Miller, an associate professor at the Air Command and Staff College, probes these questions in his article, "Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists." He looks at various groups, such as guerillas or terrorists, and attempts to extrapolate current MNSA tactics into the space domain.[2] He postulates that future terrorist groups will be able to use a satellite as a space-born, improvised kinetic device. Miller argues that the ever-greater dependence on space for economic purposes will produce malicious actors in the same way the oceans continue to entice pirates.[3] Guerillas, pirates and terrorists will continue long into the future as the same past motivations and ideologies continue to imbue human actions. These MNSA are going to apply whatever tools they can access, harness, and use to achieve their aims. The proliferation of space-enabled technologies is not a distant conception. Space technologies already pervade the commercial market.[4] As great power competition grabs the attention of the national security enterprise for legitimate reasons, low-intensity conflict is not going away. MNSA will continue to challenge American power and interests. MNSA organization, tactics, techniques, and procedures will not remain static either, given the drivers of change that are necessity and desperation. Consideration must be given to MNSA using space-based capabilities and assets to further their aims.

---

[2] Gregory D. Miller, "Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists: Nonstate Threats in Space," *Air & Space Power Journal* 33, no. 3 (Fall 2019): 35, accessed September 12, 2020, https://search.proquest.com/openview/3555c15671f813f1a75817ced0a5f2d1/1?pq-origsite=gscholar&cbl=26498.

[3] Miller, "Space Pirates," 38.

[4] Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, "Others: Kinetic Physical," in *Space Threat Assessment 2018* (Washington, DC: Center for Strategic and International Studies, April 2018), 22, accessed September 20, 2020, https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf#page=28.

The ideas postulated in Miller's scenarios may seem farfetched. Regardless, the idea of space pirates and terrorists signals a conceptual paradigm shift occurring in envisioning the potential capabilities of MNSA. The reality is that the day when a MNSA can leverage the space domain to its advantage is already here.[5] The ubiquity of space-enabled technologies in everyday life is changing preconceived notions and the language of what it means to be a spacepower. More accurately stated, it is time to acknowledge, in the context of Multi-Domain Operations (MDO), that the non-zero-sum nature of spacepower is not fully captured in current military conceptualizations. MDO is the concept that the Army, within the joint force, must plan, combine, and synchronize effects across all named domains (space, air, sea, land, cyber, information) at speed to win on the modern battlefield.[6] MDO is a movement to understand the vital advantage—or disadvantage if neglected—an actor accrues by combining effects across the domains.

However, the concept may fall short when capturing how actors, without resources of the nation-state, use space. MNSA are using satellite communication (SATCOM), global navigation satellite systems (GNSS) enabled devices, publicly available satellite imagery, jamming techniques, and more in operations around the world.[7] These technologies create an environment where MNSA can achieve sophisticated cross-domain effects. Cross-domain effects are attacks, kinetic or non-kinetic, from one domain(s) to achieve effects in another domain(s).[8] Presuming the evolution of domain sophistication for MNSA, what are the implications for the US military?

The current US conceptualization, theory, and grammar of spacepower, as it pertains to MNSA, is inadequate to prepare for future conflict with less than near-peer competitors. The

---

[5] Harrison, Johnson, and Roberts, "Others: Kinetic Physical," 24.

[6] US Department of the Air Force, Doctrine Annex 3-99, *Department of the Air Force Role in Joint All-Domain Operations (JADO)* (Washington, DC: Government Publishing Office, 2020), 5.

[7] Gabriel and Coven, "Malicious Non-State," 6.

[8] Ibid.

investigation of this thesis will be guided by three related research questions. The goal of the research questions is to assemble conclusions and recommendations within the Doctrine, Organizational, Training, Material, Leadership, Personnel, Facilities and Policy (DOTMLPF-P) construct.[9]

The first research question is whether the contemporary descriptions of spacepower theory are sufficient to constitute a comprehensive framework for the development of effective concepts and doctrine. The second question investigates if MNSA have already demonstrated sufficient activity within and through the space domain to constitute spacepower. The third question asks if current US doctrine and concepts use the proper grammar to account for MNSA actions in the space domain. To investigate the thesis and research questions, this monograph uses case studies and compares them to US doctrine and concepts within the contemporary environment of spacepower theory.

This monograph examines three case studies: The 2006 Lebanese-Hezbollah War; the 2008 Mumbai terrorist attack carried out by the Lashkar-e-Taiba; and the Islamic State of Iraq, and Syria (ISIS) operations in Syria and Iraq between 2014 and 2016.[10] These case studies were chosen for three primary reasons. The first is for their timeliness; these studies show an evolution in the use of space to show a trend line for future MNSA space-enabled operations. The second reason these case studies were chosen is to show the use of space by MNSA with various levels of sophistication and organization. The final reason for their inclusion is the implications of the use of space in these case studies have yet to be fully understood. These cases help to illustrate how seemingly unsophisticated non-space powers are already using the space domain.

---

[9] This monograph argues that the current grammar used by the US military is insufficient to properly conceptualize the true potential of MNSA Space Power. It is worth considering that the DOTMLPF-P framework may be insufficient to deal with future challenges as well. However, for the purpose of this monograph, recommendations will be made within the DOTMLPF-P framework.

[10] The Islamic State of Iraq and Syria goes by multiple names in different countries. To maintain consistency, this monograph will use Islamic State of Iraq and Syria (ISIS).

This monograph consists of seven different sections. The first section lays out the foundational problem under examination. Following the introduction of the problem, the monograph proposes the thesis and corresponding research questions. The second section is the literature review, which covers three categories: contemporary theory and definitions about spacepower, historical studies of MNSA, and current conceptual thinking observed in US military doctrine. The third section outlines the methodology used to assess the thesis. The fourth section establishes and reviews definitions and concepts as they are related to spacepower in warfare. The fifth section presents the case studies that are central to this investigation. This section provides an overview of the cases and specifically highlights the use of space-enabled technologies within each case. The fifth section concludes with a synthesis of the three case studies to illustrate the current capabilities of MNSA. The sixth section analyzes the case studies within the framework of current US military conceptualization, current doctrine, and the MDO concept. The goal of the sixth section is to show the mismatch between current US military language regarding space and that of potential and current MSNA adversaries. The concluding section assesses the major threads of this research including conclusions and recommendations.

Literature Review

The purpose of the literature review is to evaluate existing literature about topics covered within this monograph. Furthermore, the literature review attempts to highlight any gaps in the current literature and provide areas for future research on these subjects. This literature review will cover three categories. The first category covers spacepower theory as the framework to conceptualize phenomena observed within the space domain. The second category reviews the literature on the case studies within this study. The third category covers the current understanding of spacepower within US doctrine and the MDO concept.

Spacepower theory, in its current form, is still in the early phases of testing and comprehension. Imperfect as any spacepower theory may be, a theory is a prerequisite to the

development of policy and doctrine. As spacepower theorist John J. Klein observed, a theory is needed so the rules of a system may be articulated to gain some semblance of understanding the way the system operates.[11] That is to say, without the theory there is no language to discuss, strategize, and develop doctrine to coherently operate within a system. As Carl von Clausewitz proposed, "Its grammar, indeed, may be its own, but not its logic."[12] Spacepower theory may have similar characteristics to other theories of military domains but needs a unique language. Given the complex ways in which space interacts with other domains such as cyber, land, sea, and air; a useful theory is crucial to develop doctrine and practice. Spacepower theories must be challenged and reassessed as the technologies and actors in the space domain evolve. The nascent stage of spacepower theory shows how misunderstanding of theory may lead to errant development of policy.

The initial challenge of investigating spacepower theory is the absence of historically tested theories. Many theorists are trying to solidify the theory of spacepower. However, the relatively new phenomenon of space being harnessed for national and military power implies most spacepower theories have yet to be rigorously tested. It seems unlikely that any spacepower theory will be proved absolute. When considering the advent of air power theory at the initial stages of the last century, it is reasonable to conclude that these are still the early days of spacepower theory. Airpower theorist Giulio Douhet is still hotly debated one hundred years after the advent of his theories.[13] Any authoritative spacepower theory should be viewed with skepticism.

---

[11] John J. Klein, *Space Warfare: Strategy, Principles, and Policy* (London, UK: Routledge, 2006), 4.

[12] Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 605.

[13] Robert S. Douhet Dudney, "The Legendary and Controversial Airpower Theorist is Debated to this Day," *Air Force Magazine* (April 2011): 64, accessed November 12, 2020, https://www.airforcemag.com/PDF/MagazineArchive/Documents/2011/April%202011/0411douhet.pdf.

Numerous publications have investigated and proposed theories regarding spacepower. Published literature has been drawn from books, journals, and articles. The authors of these works come from institutions such as academia, the military, and think tanks. To narrow the abundant sources for this study a cross-section has been taken from the categories listed above. The main goal of this study was to gain a wide variety of perspectives on the current and future state of spacepower. Author John J. Klein in his 2006 work, *Space Warfare,* uses his background in the Navy to evaluate emerging spacepower theory in the light of historical land and navy case studies.[14] Klein also relies heavily on naval theorist, Sir Julian Corbett, to show how the space domain may be used as a strategic launching point for operations in other domains.[15] Author M. V. Smith offers an Air Force perspective in his 2001 thesis, *Ten Propositions Regarding Space Power*. Smith's goal is to offer propositions to frame the nature and character of the space domain to move toward a sound spacepower theory.[16] Smith's work is exceedingly useful as it offers a framework for thinking about space that is lacking in current doctrine. Scholars in the spacepower theory field such as Joan Johnson-Freeze, Wilson W. S. Wong, and James Fergusson offer further perspective. Johnson-Freeze has two works that were critical to this study: *Space as a Strategic Asset* and *Space Warfare in the 21st Century*. In *Space as a Strategic Asset*, Johnson-Freeze offers an overview of the emergent competition in space between great powers as well as the way the diffusion of technology will create nearly limitless new space actors.[17] *Space as a Strategic Asset* also analyzes how all space technology is dual-use in nature. All space technology may be

[14] Klein, *Space Warfare*, 3.

[15] Ibid.

[16] M. V. Smith, *Ten Propositions Regarding Space* (Ann Arbor, MI: Nimble Books LLC, 2011), 42. Smith's ten propositions are: space is distinct operational medium; the essence of space power is global access and global presence; space power is composed of a state's total space activity; space power must be centrally controlled by a space professional; space power is a coercive force; commercial space assets make all actors space powers; space power assets form a national center of gravity; space control is not optional; space professional require career-long specialization; and weaponizing space is inevitable.

[17] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), 24–26.

used for peaceful or military purposes, potentially without the consent of the owner of a given satellite.[18] In *Space Warfare in the 21st Century*, Johnson-Freese offers a compelling case as to why spacepower and the space domain are critical, yet vulnerable, to national policy and US military means.[19] In *Military Space Power*, Wong and Fergusson articulate an idea central to this study: the current commercial space age, with an ever-increasing number of actors, requires an evolution of thinking and concepts to effectively meet the future of space.[20] Furthermore, the US Space Force (USSF) offers a robust, perhaps ineffable, definition of spacepower theory in their capstone document, *Spacepowe*r. *Spacepowe*r attempts to articulate the nature of spacepower without directly pointing to the definition. The document states that spacepower is a source and conduit of national power and prestige.[21] National spacepower is the totality of all space activities including military spacepower.[22] The document falls short as the capstone document for USSF because it does not expressly articulate what spacepower is, instead, the document points to the branch's core competencies.[23] A literature shortfall in spacepower theory is in dedicated research on historical case studies. The general arc of the literature is trying to establish a basic theory.[24] However, spacepower has been used to one degree or another in every conflict starting at least

[18] Johnson-Freese, *Space as a Strategic Asset,* 27–50.

[19] Joan Johnson-Freese, *Space Warfare in the 21st Century: Arming the Heavens* (London: Routledge Taylor, 2017), 4–16.

[20] Wilson W. S. Wong, and James G. Fergusson, *Military Space Power: A Guide to the Issues* (Santa Barbara, CA: Praeger, 2010), 12.

[21] Headquarters, United States Space Force (USSF), US Space Force Capstone Publication, *Spacepower* (Washington, DC: Government Printing Office, 2020), 12.

[22] USSF, *Spacepower*, 13–16.

[23] Ibid., 34. The core competencies are Space Security, Combat Power Projection, Space Mobility and Logistics, Information Mobility, and Space Domain Awareness. These competencies are activities within the domain but do not explain the purpose of military spacepower, which at is basis is coercion. The document could use an explanation of how spacepower could be used to achieve national objective.

[24] Although there are numerous books, journal articles, and reports that propose and analyze the future of space and the theories behind spacepower, a literature shortfall exists from a lack of historical evidence to support any single school of thought.

with Desert Storm.[25] Most of the spacepower theories reviewed for this study have a forward-looking perspective. A thorough investigation into the ways spacepower has influenced decisions, risks, doctrine, and organizations may yield the structure of the nature of spacepower.

The case studies used within this study are the 2006 Lebanese-Hezbollah War, the 2008 Mumbai terrorist attack carried out by Lashkar-e-Taiba, and ISIS operations in Syria and Iraq between 2014 and 2016.[26] The literature for the case studies ranged from news articles to journal articles. News articles were the starting point for these case studies as they are useful primary sources given the recent nature of the conflicts. Publications such as the *New York Times*, *the Guardian*, and the *Washington Post* offer multiple articles on all three cases. News reports were particularly useful in tying actual use of space-enabled technologies to the case studies as opposed to a retrospective broad overview of the events. The *New York Times* analyzed the ways the Mumbai terrorists incorporated space technology in their operations.[27] Journalist Ben Watson wrote an expose on the ways ISIS produced and used drones in Syria.[28] Government investigations were also instrumental to this study. The Senate Committee for Homeland Security and Governmental Affairs also investigated the Mumbai terrorist attack. The Congressional investigation looked at how the Mumbai tactics and use of technology might be exported for other attacks.[29] The Homeland Security Committee staff report, *Terror Gone Viral*, established

---

[25] Larry Greenenmeier, "GPS and the World's First 'Space War,'" *Scientific American*, February 8, 2016, accessed September 12, 2020, https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/.

[26] There are numerous case studies of the 2006 Hezbollah war. See Bibliography. These case studies primarily focus on Israel and lessons to be learned for other nations, such as the US. There appears to be less writing dedicated to understanding Hezbollah's strategic, operational, and tactical objectives as well as means they sought to achieve those objectives.

[27] Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks," *New York Times*, December 09, 2008, accessed July 15, 2020, https://www.nytimes.com/2008/12/09/world/asia/09 mumbai.html.

[28] Ben Watson, "The Drones of ISIS," Defense One, January 12, 2017, accessed October 15, 2020, https://www.defenseone.com/technology/2017/01/drones-isis/134542/.

[29] *Lessons from the Mumbai Terrorist Attacks: Hearings before the Committee on Homeland Security and Governmental Affairs*, 111th Cong., 1st sess., January 8 and 28, 2009.

the way ISIS used technology to export their ideas.[30] This monograph also reviewed numerous academic accounts to develop the case studies, such as the Rand Corporation and the Federation of American Scientists. RAND's *The Lessons of Mumbai* provides a detailed overview of how the Mumbai terrorists integrated and planned their operation utilizing space technologies.[31] The Federation of American Scientists publication, *Hezbollah and the Use of Drones as a Weapon of Terrorism*, offers an excellent assessment of the way Hezbollah executed drone operations during the Second Lebanese War.[32] Other publications contain a further exploration of Hezbollah's drone use, the challenge Israel faced with shutting down Hezbollah's satellite TV network, the lesson of the Second Lebanese War, and the significance of an MNSA, such as ISIS, use of drones in a broader strategic narrative.[33] Possible shortfalls and opportunities for research in this category are specific, historical, assessments of the use of space-enabled operations within the broader category of terrorism, insurgency, and other malicious actors.

---

[30] Homeland Security Committee, *Terror Gone Viral: Overview of the 243 ISIS-Linked Incidents Targeting the West: House Homeland Security Committee Majority Staff Report 2014-2018*, Version 2.0 (Washington, DC: Department of Homeland Security, 2018), 4–7, accessed October 20, 2020, https://www.hsdl.org/?view&did=817196.

[31] Angel Rabasa, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, and Ashley J. Tellis, *The Lessons of Mumbai* (Santa Monica, CA: RAND Corporation, 2009), 3–6, accessed October 18, 2020, https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf.

[32] Milton Hoeing, "Hezbollah and the Use of Drones as a Weapon of Terrorism," Federation of American Scientists, June 5, 2014, accessed October 16, 2020, https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism.

[33] Liran Antebi, "Unmanned Aerial Vehicles in Asymmetric Warfare: Maintain the Advantage of the State Actor, In *The Quiet Decade: In the Aftermath of the Second Lebanon War, 2006-2016* (Tel Aviv, Israel: Institute for National Security Studies, 2017) 83–87; Paul Cochrane, "Bombs and Broadcasts: Al Manar's Battle to Stay on Air," Arab Media & Society, March 7, 2007, accessed November 22, 2020, https://www.arabmediasociety.com/bombs-and-broadcasts-al-manars-battle-to-stay-on-air/; Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War* (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 1–3, accessed October 13, 2020, https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf; Emily Archambault and Yannick Veilleux-Lepage, "Drone Imagery in Islamic State Propaganda: Flying like a State," *International Affairs* 96, no. 4 (July 2020): 955–956, accessed October 20, 2020, https://academic.oup.com/ia/article/96/4/955/5813533.

The third category of this literature review is the assessment of current literature outlining conceptualizations of the application of spacepower within the US military. The primary documents come from US military doctrine and concepts. The key doctrinal documents are Joint Publication (JP) 3-14, *Space Operations*; Field Manual 3-14, *Army Space Operations;* Field Manual 3-24, *Insurgencies and Countering Insurgencies;* and the USSF's capstone doctrinal document, *Spacepower*. JP 3-14 provides an overview of space capabilities, benefits of access to space, and generalized threats in the space operational environment.[34] The document then outlines the discrete role of military spacepower in the joint force and those roles' relation to the joint warfighting functions.[35] The document is a practical overview for those unfamiliar with US space capabilities. FM 3-14, *Army Space Operations*, is written similarly to JP 3-14. FM 3-14 offers a wide swath of space domain information, covering everything from policy, orbital mechanics, and the various army space formations to a single chapter that covers integrating space into the operations process.[36] FM 3-14 is designed to advise soldiers of US space capabilities as opposed to informing the reader of methods to employ those space capabilities. Furthermore, these documents insufficiently articulate how space operations may change against distinct types of actors.[37] JP 3-14 and FM 3-14 do not effectively connect capabilities with their implementation on the battlefield. FM 3-24, *Insurgencies and Countering Insurgencies* was reviewed to assess how the primary doctrinal document for conflict with MNSA accounts for MNSA space capabilities. The document includes MNSA space activities in the context of

[34] US Department of Defense, Joint Staff, Joint Publication (JP) 3-14, *Space Operations* (Washington, DC: Government Printing Office, 2018), viii.

[35] US Joint Staff, JP 3-14 (2018), ix-x.

[36] US Army, Field Manual (FM) 3-14, *US Army Space Operations* (Washington, DC: Government Publishing Office, 2019), i–iii.

[37] The current Joint and Army Space Doctrine (see JP 3-14 and FM 3-14) focus on the integration and planning for space capabilities for the joint and army forces. The potential threats proposed in these documents looks generically at state actors.

information operations.[38] Furthermore, FM 3-24 only touches broadly on MNSA use of space via the electromagnetic spectrum (EMS) and the potential vulnerabilities of MNSA communication networks if they were to access the space domain.[39] Overall, *Insurgencies and Countering Insurgencies* does not assess the capabilities or the significance of fighting a MNSA with space capabilities. The second crucial document in this category is the USSF capstone document, *Spacepower*. This document was used to understand the USSF's articulation of spacepower as well as how the document establishes USSF doctrine.[40] This document outlines guiding principles such as the nature of space, the strategic use of space, and the application of space in warfare.[41] As noted earlier, without a coherent definition of spacepower the doctrinal basis of the document is less than convincing. This is reasonable considering the USSF is still in its emerging stage. *Spacepower* does tie itself to the emerging concepts of All-Domain Operations and MDO by discussing space power in relation to the other domains.[42]

This portion of the literature review also assesses the MDO concept. The primary document for this portion of the review is Training and Doctrine Command Publication 525-3-1, *The U.S. Army in Multi-Domain Operations 2028*. This document offers the future vision of the Army. The concept is an effort to integrate, coordinate, and synchronize operations across all the named domains; space, air, sea, land, cyber, and information.[43] The purpose is to create future doctrinal solutions for the US Army to fight successfully from the land domain by, with, and through all the other named domains. The MDO concept acknowledges that the land domain

---

[38] US Army, Field Manual 3-24, *Insurgencies and Countering Insurgencies* (Washington, DC: Government Publishing Office, May 13, 2014), 7-18.

[39] Ibid., 5-1–3.

[40] USSF, *Spacepower*, xi.

[41] Ibid., viii–ix.

[42] Ibid., vii.

[43] US Department of the Army, Training and Doctrine Command Pamphlet (TRADOC Pam) 525-3-1, *The US Army in Multi-Domain Operations 2028* (Washington, DC: Government Publishing Office, 2018, 18-21.

interfaces nearly ubiquitously with all the other domains. The challenge for the US Army becomes: how is the force manned, trained, and equipped to fight when an adversary uses effects from multiple domains simultaneously? The concept is not truly novel.[44] However, the document is trying to answer how to mass and counter effects in a time-constrained and geographically unconstrained environment. The gap within this current research and existing literature is regarding MNSA. These documents, for understandable reasons, focus on near-peer competition.[45] MNSA unique characteristics, such as organization and tactics, deserves consideration for further research into operational and doctrinal approaches.

Methodology

This monograph uses case studies viewed through the lens of current US thinking on spacepower and doctrine to investigate the central argument; current US conceptualization, theory, and grammar of spacepower, as it pertains to MNSA, is inadequate to prepare for future conflict with less than near-peer competitors. This study first establishes critical concepts and definitions regarding space in warfare. The definitions and concepts are reviewed for two central purposes. Firstly, these terms need to be examined as they are currently informing United States' thinking on spacepower. Defining terms shows how these concepts have inherent gaps as well as how they may lead to narrow or errant conclusions. As Everett Dolman argues in *Pure Strategy*, "No issue, then, ought to be more vital for the strategist, who deals daily with perceptions and symbols, than semantics."[46] The words used to articulate how a system works will drive the way actors behave within a given domain. The second purpose of defining terms is to use them as a

[44] Phil Clare, "The Answer is Multi-Domain Operations – Now What's the Question?" Wavell Room, February 13, 2020, accessed November 13, 2020, https://wavellroom.com/2020/02/13/the-answer-is-multi-domain-operations-now-whats-the-question/.

[45] The 2018 National Security Strategy has as its focus a return to great power competition. Understandably, the DOD has shifted its main focus from counterinsurgency and counterterrorism.

[46] Everett C. Dolman, *Pure Strategy: Power and Principle in the Space and Information Age* (New York: Frank Cass, 2005), 13.

bridge between the case studies and the examination of current US conceptualizations. Using the terms as a bridge, between the case studied and US thinking, illustrates potential gaps that are critical to assessing the thesis of this study.

This monograph investigates three case studies: The 2006 Second Lebanese War, the 2008 Mumbai terrorist attacks, and the height of ISIS between 2014 and 2016. The use of historical case studies is to assess the current ability and capability of a select group of MNSA's to use spacepower. This assessment is primarily qualitative in nature. The goal of this qualitative assessment is to demonstrate how MNSA's use of space has already moved beyond the United States' current paradigmatic thinking on space. Appraisal of the case studies in the context of established definitions will be the basis of the assessment of current US spacepower concepts.

This monograph then establishes the current paradigm of US military thinking regarding spacepower. The focus is whether US concepts of spacepower are sufficiently developed to deal with the phenomenon of MNSA using space. The analysis of current thinking will draw out gaps and anomalies in current theory and doctrine. As Thomas Kuhn wrote, "anomaly appears only against the background provided by the paradigm."[47] The goal of this section is to establish areas within the US paradigm that most readily need revaluation.

This study relies heavily on the theories of Thomas S. Kuhn in *The Structure of Scientific Revolutions*. Kuhn's model of paradigm, anomaly, crisis, revolution, emergent paradigm (see Figure 1) is instrumental for describing the structure of the interplay of phenomenon occurring with MNSA use of space and current US military thinking.[48] Comparing the case studies to the current US lexicon and thinking on spacepower will highlight anomalies within the current paradigm. This monograph does not presume the current paradigm on spacepower theory and

[47] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: The University of Chicago Press, 1996), 65.

[48] Kuhn, *The Structure of Scientific Revolutions*, 92–93.

application within the US military is so flawed the paradigm must be replaced.[49] The anomalies identified within may be reconcilable to current thinking. Furthermore, this study does not claim there is necessarily a crisis within the current spacepower paradigm, instead, a grammar that is currently insufficient to deal with evolving threats. The intent of identifying anomalies within the current paradigm is to help draw out recommendations.

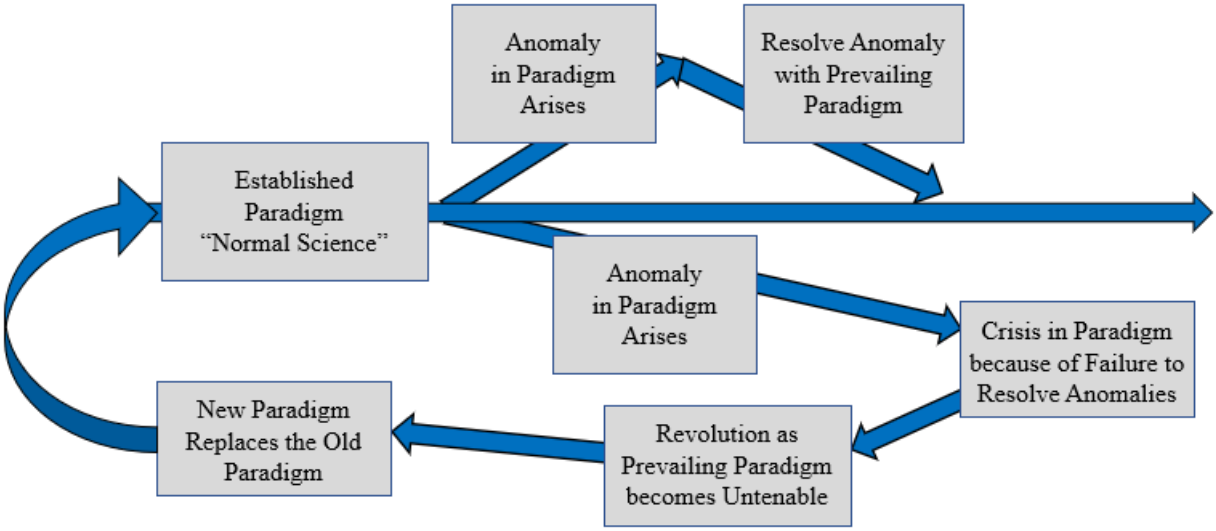

Figure 1. Paradigm Change. Created by the author using information from Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: The University of Chicago Press, 1996).

Key Definitions and Concepts

Definitions are critical when considering spacepower and the space domain. As will be shown, many of these definitions draw similarities to theories of the air and sea domains. Similarities to other theories are due to robust connections in many of the schools of thought for the space domain to other mediums.[50] However, per the literature review, many of these definitions are insufficient in the current form for analysis when applied to the case studies. The limitation of any of the proceeding terms is found in the emerging form of spacepower theory.

[49] Given the literature review and investigation of key definitions, spacepower theory may still be in an emergent phase.

[50] Klein, *Space Warfare*, 16.

Therefore, to analyze current US doctrine and concepts this study will review and expand upon a few current space-related concepts and definitions. These terms will be used throughout the monograph to illustrate where current grammatical and conceptual frameworks are insufficient.

Before establishing definitions, it useful to consider the predominant theories of spacepower. These schools of thought help to explain the direction and usage of the key terms in subsequent paragraphs. The four schools are sanctuary, survivability, high-ground, and control. Sanctuary holds that space should be war and weapons free.[51] The primary purpose of space technology is to monitor other nations.[52] The ability to monitor, the thinking goes, will inhibit the buildup of undisclosed military means. The ability to monitor other nations would, therefore, be a stabilizing force. The survivability school holds that space systems are more vulnerable than other assets or forces. There is nowhere to hide in space. Therefore, nations should not develop weapons in space as their ability to achieve effects is limited by their vulnerability.[53] The third school is high ground. This school is straightforward in explanation. The actor that holds space will have the advantage over their adversary.[54] However, multiple actors can act in space and still not have control over the domain. Control is the final school of spacepower thought. The control school argues to gain an advantage in space the United States must prevent hostile actors from gaining access to space while preserving its access to the domain.[55] Control has similarities to sea control and air superiority.[56] However, it is unclear whether control means regulating access to outer space as well as controlling the electromagnetic signals that move through space. The control school has gained many disciples in US military thinking because the belief is that

[51] Klein, *Space Warfare*, 17.

[52] Ibid.

[53] Ibid.

[54] Ibid.

[55] Ibid.

[56] Ibid.

whoever has the potential to exert control over space gains control over the air, land, and sea domains.[57] The control school recognizes the vital importance of space to American interests, as well as the impetus to defend the space domain.

The first critical definition to assess is spacepower. This monograph uses the definition of spacepower found in *Space Power 2010*, "Space power is the ability of a state or non-state actor to achieve its goals and objectives in the presence of other actors on the world stage through control and exploitation of the space environment."[58] *Space Power 2010* includes non-state actors who use spacepower. This is important because non-state actors are often overlooked as space powers. The *Space Power 2010* definition is also useful because other source documents lack a succinct definition. JP 1-02, *DOD Dictionary of Military and Associated Terms*, does not include the term *spacepower* as a term currently used by the Department of Defense (DOD). JP 1-02 does refer to space assets and space capabilities but these definitions refer to capability, not the ability to influence or gain an advantage from space. The USSF's capstone document, *Spacepower*, does not yet offer a concise definition of spacepower. Instead, the document uses aggregation of the activities by, with, and through space to show that which is spacepower.[59]

Spacepower does not have an official definition in the *DOD Dictionary of Military Terms*. However, the US military does categorize spacepower activities by establishing a space domain. The DOD uses the idea of domains to categorize areas that lend themselves to specific activities. The sea domain is geographic while the cyber domain is more conceptual. A domain may imply multiple functions. Domain can imply a sphere of specific activity or knowledge, or

[57] Ibid.

[58] James L. Hyatt, III, Paul L. Laugesen, Michael A. Rampino, Ronald R. Ricchi, and Joseph A. Schwarz, "Space Power 2010," (master's thesis, Air and Command Staff College Maxwell AFB, AL, 1995), 5.

[59] USSF, *Spacepower*, vi-vii.

domain may refer to an area of territory controlled by a sovereign entity.[60] However, the *DOD Dictionary of Military Terms* does not offer a specific definition for domain. Domains can be a bit deceiving as activities may be categorized into limitlessly discreet functions. Domains also have the appearance of being tautological. Activities belong to a specific domain because that is the realm in which those activities occur. Given this assessment of the definition of domain, the DOD dictionary does define space domain. The space domain is "the area above the altitude where atmospheric effects on airborne objects become negligible."[61] This definition creates a geographic sense of the space domain. However, for this study, space is both a physical space, like the land domain, and a more conceptual domain, like cyberspace. As the USSF capstone document, *Spacepower* points out, operations in the space domain require physical structures in the air, land, or sea domain, a structure in orbit, and an EMS link segment.[62] The implication is that ownership of all three segments constitutes spacepower; nonetheless, MNSA use these structures to conduct operations without ownership.

The lack of clarity between who owns and who can operate within the space domain necessitates elaboration on how to control the space domain. Space control relates to "operations to ensure freedom of action in space for the United States and its allies and deny an adversary freedom of action in space."[63] Controlling space draws parallels to sea control and air supremacy because of the categorization of space as a geographic medium where humans are unlikely to permanently inhabit. In his thesis, "Ten Propositions Regarding Space Power," M. V. Smith rightly argues that "space control is not optional."[64] Regardless, if the United States formally

---

[60] *Merriam-Webster*, s.v. "Domain," accessed November 12, 2020, https://www.merriam-webster.com/dictionary/domain.

[61] US Joint Staff, JP 1-02 (2020), 198.

[62] USAF, *Spacepower*, 36.

[63] US Joint Staff, JP 1-02 (2020), 198.

[64] Smith, "Ten Propositions, 86–91.

adopts the control school of military power, assured access to space is critical to national interests. With the advancement of near-peer competitors, China and Russia, to field anti-satellite weapons and advanced jamming techniques, there is a real threat to the United States' assured access and use of the space domain. Conducting space control is a more complicated matter. In "New Frontiers, Old Realties," Everett Dolman argues, "control is possible only from within the domain."[65] The concern is that adversaries can directly influence—kinetically or non-kinetically—the United States' space lines of communication. They can achieve these effects in and through space. An actor does not need to be in space to achieve control. The limitation of the idea of space control is it is primarily focused on the physical space segment. Space lines of communications consist of ground, space, and EMS links. Therefore, a more complete understanding of how space enhances military operations is necessary.

Author John J. Klein defines space lines of communications as "those lines of communications in and through space used for the movement of trade, material, supplies, personnel, spacecraft, electromagnetic transmissions, and some military effects."[66] The definition is useful but not sufficient. The definitions of the space domain, space control, and space lines of communication continue to point to the conclusion that space is primarily a physical domain that can be controlled by physical force. It can be accurately stated that kinetic and non-kinetic actions may exert some control over the space domain. However, what control can be effectively exerted when hostile actors are using space for their operations utilizing friendly space lines of communication? Examples may be using the Global Positioning System (GPS), Satellite-based communications and internet that is provided to millions of users, or publicly available satellite imagery found on the internet. The notion that an adversary can use friendly space-lines of

---

[65] Everett C. Dolman, "New Frontiers, Old Realities," *Strategic Studies Quarterly* 6, no. 1 (Spring 2012): 86, accessed September 12, 2020, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/dolman.pdf.

[66] Klein, *Space Warfare*, 51. Klein uses the term, "celestial lines of communication," to ensure differentiation between the acronyms of space lines of communication and sea lines of communication.

communications to achieve its ends draws out a few considerations. First, having spacepower is not predicated on control or ownership of all the space segments. The space domain cannot be fully isolated from other domains. A MNSA using GPS to navigate a ship or fly a UAV is relying on the space domain. Space control depends on control of the physical segments of space architecture as well as the control over access to the EMS. Finally, a lexicon is missing for actors, especially MNSA without ground stations or satellites, who use friendly or neutral space systems without interfering or degrading those space systems. These considerations are critical when assessing the case studies. Furthermore, the analysis will draw out potential definitions for adoption to help clarify current shortcomings in the spacepower grammar.

Case Studies

Hezbollah – Second Lebanese War 2006

The Israel-Hezbollah War of 2006 is a case study of a superior force, the Israeli Defense Force (IDF), executing operations against a MNSA. Hezbollah has membership within the Lebanese government while maintaining independent military forces.[67] These forces include traditionally organized units supported by thousands of rockets, missiles, and anti-tank guided missiles.[68] Hezbollah's organization and equipment imply a superior sophistication compared to most other MNSA. However, given the structure and technological advancement of the Israeli armed forces, the IDF should have easily outmatched Hezbollah. Yet, the 2006 war shows how a MNSA may achieve fundamental surprise and success by seeking gaps in their adversaries' doctrine, concepts, or technology.

[67] David E. Johnson, *Hard Fighting: Israel in Lebanon and Gaza* (Santa Monica, CA: RAND Corporation, 2011), 10.

[68] Russell W. Glenn, *All Glory is Fleeting: Insights from the Second Lebanon War* (Santa Monica, CA: RAND Corporation, 2012), 6, accessed November 10, 2020, https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG708-1.pdf.

A fundamental surprise is a sudden realization that there is a mismatch in one's perceived understanding and the reality of an operational environment.[69] Israel's fundamental surprise was the mismatch of its understanding of the IDF's asymmetric advantage over Hezbollah. The war, however, started with a situational surprise.[70] On July 12, Hezbollah conducted a cross-border raid attacking two IDF vehicles. The attack left three IDF soldiers dead and two captured. Israel's first response was to use air power to hit Hezbollah targets throughout Lebanon.[71] Hezbollah responded with the launch of hundreds of rockets over the following days.[72] Israel launched a ground offensive into Southern Lebanon starting on July 22, achieving minimal success.[73] The conflict lasted thirty-four days until the United Nations-brokered a ceasefire. The battlefield results are still unclear. The Israel-Lebanese border was reestablished by the ceasefire, but the war shook Israel's government.[74] Hezbollah had not expected the massive Israeli retaliation after the first attack.[75] Israel was accustomed to fighting in uncontested environments, including the air and the sea. The fundamental surprise was that Hezbollah was able to thwart a far superior military power. Part of the reason for their success was the integration of space capabilities into

[69] Zvi Lanir, *Fundamental Surprises* (Ramat Aviv, Israel: Center for Strategic Studies University of Tel Aviv, 1983), 25.

[70] Ibid., 25. Situational Surprise is the sudden discovery of an event. As opposed to the failure to understand the operational environment.

[71] Israeli Defense Forces, "The Second Lebanon War: A Timeline." July 07, 2016, accessed November 20, 2020, https://www.idf.il/en/articles/hezbollah/the-second-lebanon-war-a-timeline/.

[72] Ibid.

[73] Johnson. *Hard Fighting*, 67–69.

[74] Matt M. Matthews. "Hard Lessons Learned: A Comparison of the 2006 Hezbollah-Israeli War and Operation CAST LEAD: A Historical Overview," in *Back to the Basics: A Study of the Second Lebanon War and Operation CAST LEAD*, edited by Scott C. Farquhar (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), 21, accessed October 23, 2020, http://institutobrasilisrael.org/cms/assets/uploads/_BIBLIOTECA/_PDF/novos-conflitos-atualidades/948e1709b7c6e4fca1bb83fd4b45ca70.pdf.

[75] Andrew Chadwick, "The 2006 Lebanon War: A Short History," *Small Wars Journal*, September 11, 2012, accessed November 13, 2020, https://smallwarsjournal.com/jrnl/art/the-2006-lebanon-war-a-short-history.

their operations. Hezbollah's use of spacepower is an early example of the movement of MNSA to use once inaccessible domains to their advantage.

Hezbollah used three Iranian-produced Ababil unmanned aerial vehicles (UAV) during the war.[76] The Ababil drones were GPS guided and carried 85-110-pound explosives.[77] The Israeli Air Force was able to shoot down the UAV before they could reach their targets. Hezbollah also launched a fourth, unarmed UAV for reconnaissance during the war.[78] Although unable to hit their targets, they were able to evade IDF radars.[79] The IDF had to revamp and improve radar coverage to detect UAV near the northern border. The impact of these UAV on the 2006 battlefield was negligible. Yet these weapons stay germane to the use of space by MNSA. Battlefield success may have been limited, but they show the first stages of a trend to use space to counter an asymmetric disadvantage. Small UAV, especially used en masse, guided by GPS pose a growing threat.[80] Hezbollah's drones continue to be an immediate threat to Israel today.[81] Hezbollah successfully demonstrated how MNSA can use cross-domain capabilities, air, and space to begin countering an adversary's strength. Hezbollah also showed cross-domain capability in the information and space domains.

Hezbollah more effectively used information operations throughout the conflict than Israel. Hezbollah was able to capture the international narrative, claiming Israel caused senseless

[76] Hoeing, "Hezbollah and the Use of Drones."

[77] Ibid.

[78] Antebi, "Unmanned Aerial Vehicles," 84.

[79] Hoeing, "Hezbollah and the Use of Drones."

[80] Shaan Shaikh, "The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense," Center for Strategic and International Studies, December 8, 2020, accessed February 03, 2021, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense. The September 2020 conflict between Azerbaijan and Armenia saw the sophisticated use of drones including loitering drones that destroyed T-72s and S-300 ADA systems.

[81] Antebi, "Unmanned Aerial Vehicles," 88–89.

civilian casualties early in the war.[82] Despite early international support for Israel, Hezbollah used the IDF's ground and air campaign to show alleged catastrophic collateral damage. Hezbollah was able to achieve their information warfare success in part due to spacepower. Using satellite communications, Hezbollah's television network was able to broadcast its message to sympathetic viewers around the world.[83] The television station, al-Manar, broadcasted reports of successful fights against IDF as well as reports of civilian casualties.[84] The broadcast station became a symbolic method used to counter a superior foe. Israel targeted the al-Manar station but was never able to knock it off the air.[85] Israel faced multiple challenges when trying to counter the al-Manar information system. The IDF launched kinetic and non-kinetic strikes against the station. Using bombs, jamming, and cyber-attacks, the IDF was unable to achieve its goal.[86] Furthermore, Israel could not indiscriminately jam the satellite broadcasts because the station sent their broadcast signal through several third-party commercial satellites.[87] The role of spacepower, acknowledged or not, enabled Hezbollah to continue to push its narrative throughout the war. The evolving sophistication of space-enabled television and the use of the internet implies that MNSA will be able to push their narratives with growing influence into the future.

The 2006 Lebanese war was an early demonstration of the way space technologies enable MNSA. The Israel air campaign and follow-on ground offensive left the IDF's image in tatters.[88] Furthermore, Israel's conventional air and land power were unable to effectively shut down Hezbollah's information campaign. Space technology played a small, yet emerging, role for

---

[82] Marvin Kalb and Carol Saivetz, "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict" (research paper, Harvard Kennedy School of Government, Boston, MA, 2007), 8.

[83] Cochrane, "Bombs and Broadcasts."

[84] Kalb and Saivetz, "The Israeli-Hezbollah War of 2006," 8–9.

[85] Cochrane, "Bombs and Broadcasts."

[86] Ibid.

[87] Ibid.

[88] Glenn, *All Glory is Fleeting*, xi.

Hezbollah. These space technologies began to show how domains such as space can offer a counterbalance to advanced conventional forces.

Lashkar-e-Taiba – 2008 Mumbai Terrorist Attack

In 2008, Lashkar-e-Taiba (LeT) executed an attack within the city of Mumbai, India, resulting in over 160 deaths. LeT is a sophisticated terrorist organization that is analogous to al-Qaida in its scale and capability to conduct operations. The attack lasted four days as the terrorists attacked eight locations across Mumbai. The attackers struck the Chhatrapati Shivaji rail terminus, Mumbai Chabad House, Oberoi Trident Hotel, Taj Palace and Tower Hotel, Leopold Café, Cama Hospital, Nariman House, and the Metro Cinema. The attacks began on November 26 and culminated on November 29 when the Indian National Security Guards finally cleared the Taj Hotel. The attacks were carried out by ten gunmen with automatic weapons and grenades.[89] The tools and sophistication used to carry out these attacks exemplify what MNSA may achieve with meager resources.

LeT began the operation from Pakistan and chose to infiltrate India by crossing the Arabian Sea. The operatives navigated across the Arabian Sea to a preplanned debarkation point near Mumbai and moved rapidly to objectives across the city. The attackers kept constant contact with their handlers in Pakistan as the handlers watched the events unfold over television. The attack sent shock waves across Mumbai, India, and the world. The attack led to the death of 174 people and injuring over three hundred others. Only one LeT operative survived the attack. The lone surviving terrorist gave police vital information on the origins, tactics, and tools used to carry out the attack.[90] Those tools included many readily available space-enabled technologies.

[89] Rabasa et al., *The Lessons of Mumbai*, 4–5.

[90] Ibid., 4.

Figure 2. Mumbai Attack Sites. "Mumbai Attack Sites," *New York Times*, accessed December 12, 2020, https://archive.nytimes.com/www.nytimes.com/interactive/2008/11/26/world/asia/20081126-mumbai-attacks.html.

LeT began its operation by seizing a fishing trawler off the southern coast of Pakistan. The fishing trawl is where most of the operatives met for the first time.[91] LeT leadership kept the terrorists apart before the execution of the attack to maintain operational security. The consequence of operational security requirements necessitated extensive planning and continuous command and control during the attack. The LeT operatives maintained contact with their handlers using satellite phones during the preliminary stages of the operation. The terrorists left a satellite phone on the hijacked fishing trawler that held the records of phone calls to their handlers in Pakistan.[92] During the operation, the terrorists primarily communicated over cell phones using Voice Over Internet Protocol to mask their calls.[93] However, simple commercially available satellite phones were instrumental to provide initial direction during the transit across the Arabian Sea.

[91] Rabasa et al., *The Lessons of Mumbai*, 4.

[92] Kahn, "Mumbai Terrorists."

[93] Ibid.

Space technology was also instrumental while the terrorists transited the Arabian Sea. The terrorists did not have training or a background as sailors. The terrorists had GPS receivers with preprogrammed waypoints to navigate from Pakistan to Mumbai.[94] Numerous GPS devices found on the boat and attack sites included navigation points back to Pakistan and the locations of their attack sites.[95] The use of GPS receivers moved the water and through the city simple for the terrorists. LeT leadership understood that GPS tools could enable minimally trained and prepared operatives to execute a geographically dispersed and complex attack.

LeT leadership was also well prepared for when their operatives arrived in Mumbai. LeT conducted extensive reconnaissance on the ground in Mumbai.[96] They used commercially available satellite imagery to effectively create target packages for the terrorists.[97] Compact discs holding high-quality satellite imagery were found at the attack locations.[98] The satellite imagery, ground reconnaissance, and GPS receivers allowed for a simultaneous and dispersed attack across Mumbai.[99] The combination of reconnaissance assets and GPS enabled the execution of the operation comparable to the capability of a state actor. The handlers in Pakistan had designed a well-developed and prepared operation but were also able to watch the results of their efforts unfold on live television.

LeT leadership in Pakistan was in constant communication with the terrorists in Mumbai.[100] The leadership had a complete operating picture of the events in Mumbai because of

---

[94] Emily Wax, "Mumbai Attackers Made Sophisticated Use of Technology," *Washington Post*, December 3, 2008, accessed October 22, 2020, https://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html.

[95] Rabasa et al., *The Lessons of Mumbai*, 3.

[96] Ibid.

[97] Wax, "Mumbai Attackers."

[98] Ibid.

[99] Ibid.

[100] Kahn, "Mumbai Terrorists."

satellite television.[101] Satellite television broadcast the events throughout the globe as the world watched in shock. The Pakistani handlers were even able to inform their operatives at the Taj Hotel that Indian National Security Guards were about to storm the hotel on November 28 while LeT leadership watched.[102] Live satellite television played an unplanned role in the overall operation. Yet, the ability to broadcast and receive across the globe with other capabilities enabled the convergence of multiple domains to achieve outsized results.

The success of the LeT terrorists was due in large part to space-age technologies. GPS, SATCOM, satellite imagery, and satellite television allowed for the intricacy of the attack. Using these technologies, the terrorists launched the attack across a large body of water to precise preplanned attack points while keeping constant communication with their handlers. The results illustrate how space technologies allow unsophisticated actors to achieve disproportionate results. Space had created an operation that spanned the land, sea, space, cyberspace, and information domains, a result state actors spend significant resources trying to achieve.

Islamic State of Iraq and Syria – 2014-2016

The Islamic State of Iraq and Syria (ISIS) reemerged in Syria and Iraq when it splintered from al-Qaida in Iraq in 2011.[103] Their advent coincided with a viscous civil war in Syria and a fledgling Iraqi government that struggled to deal with the new organization.[104] ISIS was not so much of a terrorist organization as an insurgency that tried to seize territory and replace the state power within the regions they operated. ISIS effectively coupled its use of violence and social media with a call to potential members around the world to come to Syria and fight. This case

---

[101] Rabasa et al., *The Lessons of Mumbai*, 4.

[102] Kahn, "Mumbai Terrorists."

[103] "Timeline: The Rise, Spread, and Fall of the Islamic State," Wilson Center, October 28, 2019, accessed December 20, 2020, https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

[104] Fawaz A. Gerges, *A History of ISIS* (Princeton, NJ: Princeton University Press, 2016), 170–171.

study looks at ISIS between 2014 and 2016. This period captures the height of ISIS activity in the Middle East. ISIS was using primarily conventional arms—for an insurgent group—to achieve their aims as national governments had little ability to support local authorities.[105] Two areas of ISIS operations capture the way MNSA are using satellite supplied services to enhance their operations. These cases include satellite internet and GPS-capable drone systems.

ISIS has relied heavily on access to the internet. This access has allowed for extensive recruitment. Space relayed internet is prevalent in Syria and Iraq because of non-existent or destroyed infrastructure.[106] The internet allows ISIS the capability for the coordination of global operations and recruitment. This capability poses a major challenge for Western forces in the region. How were coalition forces to shut ISIS off from the internet? Shutting down internet access via space technologies, if possible, means shutting down access to potentially millions of users within a given region.[107] Satellite-based internet access provides services to approximately five million people in the region.[108] In addition to the numerous end users, there are over twelve commercial companies that have satellites providing coverage of the region.[109] Furthermore, the space-based internet service is provided by some European-based telecommunications companies such as Britain's Avanti, France's Eutelsat, and Belgium's GlobalTT.[110] These service providers

[105] Matthew F. Cancian, "Tactics, Techniques, and Procedures of the Islamic State Lessons for U.S. Forces," *Military Review* (March-April 2017), accessed September 25, 2020, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2017/ART-009/;Wilson Center, "Timeline."

[106] Nicolai Kwasniewski, "How Islamic State Takes Its Terror to the Web," *Spiegel International*, March 12, 2015, accessed October 15, 2020, https://www.spiegel.de/international/world/islamic-state-uses-satellite-internet-to-spread-message-a-1066190.html.

[107] Noah Shactman, "How Gadgets Helped Mumbai Attackers," *Wired*, December 01, 2008, accessed October 22, 2020, https://www.wired.com/2008/12/the-gagdets-of/.

[108] Matt Smith, "To silence propaganda, Iraq seeks to take Islamic State offline," *Reuters*, February 4, 2016, accessed October 17, 2020, https://www.reuters.com/article/us-mideast-crisis-iraq-internet-insight-idUSKCN0VD0LM.

[109] "Satellite Internet in the Middle East, " Satellite Signals, April 20, 2020, accessed December 2, 2020, https://www.satsig.net/ivsat2.htm.

[110] Smith, "To Silence Propaganda."

typically do not take ownership of who uses and what content is transmitted via their satellites.[111] Additionally, resellers buy and sell much of the bandwidth in the region rendering control of access even more difficult.[112] Internet services gave ISIS global reach and the capability to bypass the physical limitations placed on their operations within the region. Satellite internet was not the only space technology ISIS used. They made effective use of GPS-guided drones.

ISIS has pioneered the use of low-cost UAV to conduct its attacks. It has used drones on dozens of occasions with various levels of effectiveness.[113] The drones are used to launch bombing attacks and to conduct battlefield surveillance.[114] Drones have carried small explosives, grenades, RPG rounds, and built-in improvised explosive devices.[115] These drone operations are not possible without access to the GPS. GPS-guided armed drones gave ISIS access to the air domain to extend their operational reach, physically and psychologically.[116] Drones were also instrumental in creating complex dilemmas for coalition forces. Coalition forces began spending a considerable amount of time developing targeting packages for suspected UAV factories.[117] All the while, the airspace over coalition and Syrian forces was used by cheap MNSA drones as the coalition flew multi-million-dollar combat aircraft. Once the sphere of a select group of state actors, the use of GPS-guided UAV now allows for the capability of stand-off and reconnaissance.

---

[111] Ibid.

[112] Kwasniewski, "How Islamic State Takes Its Terror to the Web."

[113] Michael S. Schmidt and Eric Schmitt, "Pentagon Confronts a New Threat From ISIS: Exploding Drones," *New York Times*, October 11, 2016, accessed October 15, 2020, https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html.

[114] Watson, "The Drones of ISIS."

[115] Watson, "The Drones of ISIS."

[116] Archambault and Veilleux-Lepage, "Drone Imagery," 956–957.

[117] Watson, "The Drones of ISIS."

ISIS achieved stunning success in a region ripped asunder by sectarian strife and failed states. ISIS's major mistake was waging conventional war against the world's greatest conventional military forces. ISIS's use of satellite-based internet spread the Caliphate's propaganda throughout the world inspiring around 243 attacks between 2014 and 2018.[118] A regional terrorist organization achieved global reach within in a brief period. ISIS's use of drones has also revolutionized how future battlefields will look. Inexpensive, commercially available UAV allow MNSA access to the air domain in an unprecedented fashion. GPS has and will make these drones more capable. As drone technology continues to proliferate, UAV will reach longer ranges, loiter time, and payload capacity.[119] Access to space technologies gave ISIS access to the air, cyberspace, and information domains in a way that merits a reconsideration of the meaning of spacepower.

Analysis

MNSA demonstrated use of space poses multiple challenges to the development and implementation of effective US spacepower theory. These actors' use of the space domain also creates challenges for current doctrine and to the development of future doctrine. This monograph addresses these challenges by reviewing current doctrine and assessing the development and implementation of MDO. The challenge for current doctrine arises from an established capability and eagerness of MNSA to interface and use space technologies to achieve their aims. The current manual dealing primarily with MNSA is FM 3-24. *Insurgencies and Countering Insurgencies* has two areas of critical shortcomings as it pertains to MNSA use of space. The first shortcoming is that FM 3-24 includes the space domain in the information domain.[120] The inclusion of space in the information domain neglects the fact that MNSA use their space access

[118] Homeland Security Committee, *Terror Gone Viral*, 5–6.

[119] Watson, "The Drones of ISIS."

[120] US Army, FM 3-24, 7-18.

for operations other than information warfare. As shown in the case studies, MNSA are using space capabilities for planning and execution of operations as well as furthering their information campaigns. There are specific areas within *Insurgencies and Countering Insurgencies* that need to be reassessed considering MNSA use of spacepower. The second area of shortcomings is categorized into what FM 3-24 considers capabilities, activities, strengths, and weaknesses of MNSA.

The first of these issues is classified into what FM 3-24 considers conventional MNSA activities. For comparison, FM 3-24 does a reasonable job showing how MNSA may use the cyber domain to further their aims. However, the space domain should be addressed similarly. FM 3-24 illustrates how an MNSA may use the cyber domain to extend operations across borders and degrade friendly force capability.[121] These MNSA are also achieving cross-boundary operations and enhancing their weapons by using the space domain. The next problem in this area is that FM 3-24 does not address the actual significance the space domain creates for MNSA communication. FM 3-24 asserts MNSA cannot depend on traditional means of communication and therefore use ad hoc networks, including the internet, short-wave radio, and face-to-face messaging.[122] However, these ad hoc networks, especially communications over satellite-enabled internet or commercial SATCOM, are difficult to dismantle. These networks may prove vulnerable to friendly interception, but these space-enabled communications allow for global reach and resilient networks. MNSA can use these satellite communications networks without denying, infringing, or commandeering capability from the United States or coalition forces. The result is MNSA can operate in parallel to friendly forces on the same space architecture. Examples are MNSA purchasing SATCOM bandwidth from commercial resellers, ISIS using satellite internet that is also being used by millions of non-combatants, or using the same GPS

[121] Ibid., 5-3.

[122] US Army, FM 3-24, 5-25.

signal to fly UAVs. The last section of FM 3-24 that needs addressing is what the document considers a double-edged sword: decentralized networks. These decentralized networks offer operational security but become too resource-intensive or cause slow information dissemination because MNSA do not own or operate dedicated networks.[123] With the ever-increasing availability of SATCOM, access will not be a limitation in future conflict scenarios with MNSA. Decentralized networks are more capable with access to the space domain. As shown with ISIS and LeT, satellite communication-enabled decentralization creates more effective operations. Isolating parts of a MNSA network will only prove more difficult with the diffusion of space-capable communications equipment. Between third-party SATCOM bandwidth resellers and satellite phones that cost approximately $2,000, MNSA communications networks will only become more resilient.[124] The absence of assessing MNSA concerning the space domain is not only found in US counterinsurgency doctrine but also US space doctrine.

Current space doctrine does not address practical solutions for countering MNSA in the space domain. The doctrine available to US warfighters is JP 3-14, *Space Operations*, or FM 3-14, *Army Space Operations*. These documents are primarily designed to illustrate capabilities the force has at its disposal. These capabilities include space situational awareness; space control; position, navigation, timing (PNT); intelligence, surveillance, and reconnaissance (ISR); SATCOM; environmental monitoring; and missile warning.[125] These capabilities are critical to US military operations; however, these documents do not address the threat MNSA pose to the space domain and the capability the domain gives them.[126] JP 3-14 offers, as a general

[123] Ibid., 5-5.

[124] "Satellite Phones," SatPhone Shop, accessed February 13, 2021, https://www.satphone shop.com/products/satellite-phones?p=1.

[125] US Joint Staff, JP 3-14 (2018), II-7–8. JP 3-14, *Space Operations*, includes Nuclear Detonation Detection, Space lift, and Satellite Operations. These three functions are not Army missions and not included in FM 3-14.

[126] Ibid., I-6–7. These documents do not thoroughly address any threat in the operational environment. JP 3-14 offers a one-page synopsis of the general impacts of threats to US space forces.

summation of the operational environment, "Our adversaries' progress in space technology not only threatens the space environment and our space assets but could potentially deny us an advantage if we lose space superiority."[127] FM 3-14 offers a clearer picture of the operational environment, explaining that adversaries want to create a denied, degraded, and disrupted space operational environment (D3SOE). FM 3-14 states, "some threats which may contribute to a D3SOE include physical damage; signal jamming; signal spoofing; electronic interference with space-related assets, ground control nodes, control link, or on-orbit segments; and disabling or deceiving user equipment. The most likely risk to the US Army is signal jamming and spoofing directed against the ground user segments of SATCOM and PNT."[128] Both of these documents offer an incomplete picture of the space operational environment against an MNSA. The intent of this doctrine is intentionally broad to give unaccustomed individuals a cursory understanding of the ways space interfaces with traditional land warfare. However, FM 3-14 and JP 3-14 do not distinguish between near-peer, state, and non-state actors. This omission, when characterizing the threat environment, does not inform the reader of any nuance in adversary space capability.

Additionally, they do not address how an adversary may use the space domain to enhance their operations without necessarily degrading US space activities. The failure to discuss adversary space operations apart from attacks on US space capabilities misses the opportunity to consider how to attack an adversary's capabilities. The case studies show how MNSA use space assets to enhance their operations. MNSA do not always use space as a direct avenue to attack their adversaries. The divergence between US doctrine and MNSA space capabilities creates a gap in how MNSA space activities are threatening. Table 1 helps show how MNSA use space in relation to current US doctrine.

[127] Ibid., I-7.

[128] US Army, FM 3-14, 1-13.

Table 1. Malicious Non-State Actors in the Space Domain.

MNSA in the Space Domain			
	Offensive	**Defensive**	**Support**
Type of Activity	SATCOM and PNT Jamming, Attack UAVs, Information Warfare	Dispersion and Decentralization, PNT Jamming, UAV ISR	Commercial SAT Phone, SAT Imagery, and SAT Internet
US Doctrine Focus	Redundant Comms, Anti-UAV systems, Defensive Space Control	Redundant Comms, Anti-UAV systems, Offensive Space Control	Gap: Does not inherently attack, disrupt, or degrade US capabilities

Source: Created by author.

Space control may be the solution to this gap. Space control is those activities that may limit the access of MNSA to the space domain. Space control consists of offensive, prevent an adversary's use of space, and defensive, protecting US space assets, operations,[129] However, space control is highly classified and conveying to the overall force how to fight and win a war by, with, and through space is enormously challenging.

The deputy commander to US Space Command, LTG James Dickinson, articulated this problem during his confirmation hearing by explaining how over-classification leads to a gap in integration of capabilities and ignorance of threats in the space domain.[130] Furthermore, the fight against adversaries like ISIS and LeT is a daily occurrence for forces scattered across the CENTCOM AOR. The current doctrine does an insufficient job explaining to the warfighter how their adversary operates in the space domain. Unfortunately, many of the trends in FM 3-14 and JP 3-14 continue into the MDO concept.

[129] US Army, FM 3-14, 3-4.

[130] Beth Fidler, "Confirmation Testimony of New U.S. Space Force Commander Reiterates Concerns about Over-classification in Space, Calls for Review," National Archives, August 18, 2020, accessed December 14, 2020, https://transforming-classification.blogs.archives.gov/2020/08/18/confirmation-testimony-of-new-u-s-space-force-commander-reiterates-concerns-about-over-classification-in-space-calls-for-review/.

The second, more indirect, challenge arises from the way the US DOD conceptualizes and develops spacepower theory and doctrine. The US DOD's focus on near-peer competition, when framing the discussion and development of space doctrine, creates challenges that obscure the actual MNSA use of space. The current MDO solution is ill-designed for addressing an MNSA with space access or capabilities, essentially MNSA space powers. MDO focuses on near-peer competition. The development of MDO lies in the concern that the United States would be unable to compete or defeat a near-peer adversary without effective capability across all domains.[131]

This focus is reasonable for multiple reasons, including a protracted war in the Middle East the United States would like to put into the past and revanchist China and Russia. With the National Security Enterprise's focus turning from MNSA to powerful nation-states, a blind spot toward MNSA is emerging.[132] This appears similar to the same phenomena the United States faced during the first years of Operation Iraqi Freedom. The United States became focused on large-scale maneuver and forsook the lessons of counterinsurgency of Vietnam.[133] The United States found itself relearning the basic concepts of counterinsurgency in Iraq and Afghanistan.[134] The pivot toward counterinsurgency in 2006 and the change to MDO today appear to follow an established pattern of paradigm shifts. MNSA may maintain consistent patterns of warfare but a continual reassessment of counterinsurgency methods becomes imperative as the technology changes. Especially as space technologies play an ever-larger role in MNSA tactics. MDO may

---

[131] Andrew Feickert, IF11409, *Defense Primer: Army Multi-Domain Operations (MDO)* (Washington, DC: Congressional Research Service, December 8, 2020), 1, accessed January 04, 2020, https://fas.org/sgp/crs/natsec/IF11409.pdf.

[132] Stephen Tankel, "Making the U.S. Military's Counter-Terrorism Mission Sustainable," War on the Rocks, September 28, 2020, accessed January 03, 2021, https://warontherocks.com/2020/09/making-the-u-s-militarys-counter-terrorism-mission-sustainable/.

[133] Christopher Millson, "Comparing Counterinsurgency Tactics in Iraq and Vietnam," *Inquiries Journal* 3, no. 5 (2011): 1, accessed January 05, 2021, http://www.inquiriesjournal.com/articles/531/comparing-counterinsurgency-tactics-in-iraq-and-vietnam.

[134] Counterinsurgency, for simplicity, is used to encapsulate operations against less than non-state actors on under the threshold of large-scale combat operations.

be a solution to counter MNSA but the current MDO concept does not fully articulate that. The focus on near-peer competition is not the only limitation when assessing the use of MDO against MNSA.

MDO lays out penetration, disintegration, exploitation, and re-compete as the broad means of deterring and, if necessary, defeating a modern nation-state with significant anti-access and area denial capability. These MDO concepts are narrow in the sense that they are working against a system deliberately designed to prevent US capabilities from achieving success by denying access to specific areas across the named domains. However, what if the adversary's goal is not to create a system of denial? This may be the case with MNSA. They are using space technologies to carry out narrow operations and not necessarily to create a battlespace where the United States cannot operate. The focus of MDO on defeating anti-access and area denial systems is part of the concept's overall focus of large-scale combat operations along the conflict continuum.

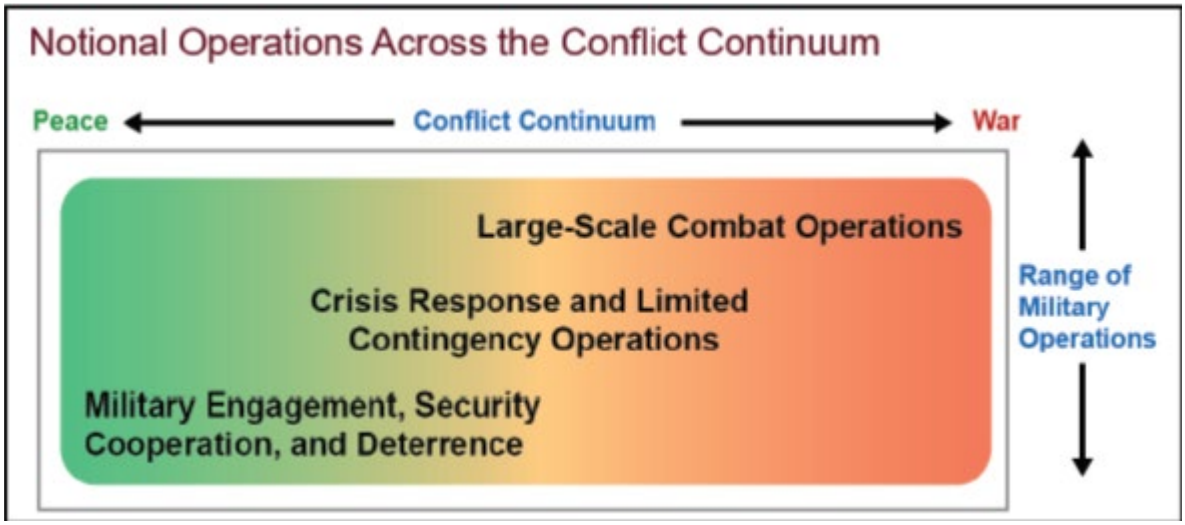

Figure 3. Notational Operations Across the Conflict Continuum. US Army, Field Manual (FM) 3-0, *Operations* (Washington, DC: Government Printing Office, 2008), 1-1.

Future war may occur anywhere along the conflict continuum or may occur at multiple places on the continuum at the same time (see Figure 3). The challenge regarding the conflict continuum is three-fold. First, what point along the continuum is the most dangerous? Second, at what point along the continuum are most conflicts going to occur? Lastly, what force structure is

necessary to meet the first two challenges? The United States has already answered the first challenge with a refocus on large-scale combat operations.[135] Policymakers want to ensure the US Army is prepared to fight an opponent that may pose an existential threat. A more cynical take is that large-scale combat merits the largest budgets. MDO is clearly a development to enhance established large-scale operations doctrine.[136]

The second challenge is less clear. There is potentially a limitless number of actors who could challenge American interests. There are more MNSA than nation-states that could challenge US interests militarily. MNSA may also be more inclined to challenge the United States because of factors stemming from their extremist ideologies.[137] That does not imply that conflict with MNSA will occur more often than nation-states. However, MDO is primarily a division and above framework.[138] Most of the assets and systems designed to deal with sophisticated adversaries will belong to the division and corps. The establishment of the multi-domain task force may be the bridge between the division and lower echelon units to counter hostile space actors.[139] However, while this organization may eventually possess the capabilities to effectively counter an MNSA spacepower on the battlefield, that capability appears to be held at the corps level. The US Army appears to be choosing between equipping brigades with more space capability or choose specialty brigades that are echelons above the MNSA fight.[140] This

---

[135] Feickert, *Defense Primer*, 1.

[136] US Army, TRADOC Pam 525-3-1, 33.

[137] Randy Borum, *Psychology of Terrorism* (Tampa, FL: University of South Florida, 2004), 4. Factors may include perceived injustice, socialization from the culture, or rigorous adherence to a belief system.

[138] US Army, TRADOC Pam 525-3-1, v.

[139] Dennis Wille, *The Army and Multi-Domain Operations: Moving Beyond AirLand Battle* (Washington, DC: New America, October 2019), 5, accessed November 02, 2020, https://www.newamerica.org/international-security/reports/army-and-multi-domain-operations-moving-beyond-airland-battle/dedicate-a-brigade-level-experimental-task-force-to-army-futures-command. The Multi-Domain Task Force is an experimental organization that incorporates a battalion that is dedicated to providing Intelligence, Information, Cyber, Electronic Warfare, and Space capability.

[140] Wille, *The Army and Multi-Domain Operations,* 6.

choice will affect future force structure and maintaining space capability at higher echelons will impact the ability of the US Army to fight in a low-intensity space conflict. Small unit operations primarily drove the Iraq and Afghanistan wars.[141] Organizationally, MDO is driving the US Army away from small unit operations to a force that is designed to fight at echelon. The focus of MDO on large-scale combat operations is not the only factor that will impact future operations against MNSA. The lexicon used to describe who are space actors and what activities they conduct presents a further challenge.

MDO will drive American doctrine over the next five to ten years. The United States needs to choose the language it includes carefully to avoid the pitfall of disregarding MNSA. First, US doctrine needs to include MNSA within the context of any definition of a spacepower. Utilizing a definition of spacepower that incorporates MNSA is the first step to correcting US doctrine. MNSA demonstrated use of space poses a real battlefield challenge to US forces. Therefore, space doctrine needs to highlight the vulnerability of the space domain against MNSA. Space control also needs to be expanded in doctrine and preferably move toward a lower classification. Lastly, space doctrine needs to include language that articulates the unique ways a MNSA may use space. MNSA propensity to use the GPS signal and acquire commercial SATCOM and satellite internet is not captured in doctrine. A grammar should be introduced that informs the warfighter of MNSA using friendly or third-party space assets., this study leverages the terms *concurrency* and *parallelism* from computer science to assess this phenomenon.

[141] Jerry Meyerle, Megan Katt, and Jim Gavrilis, *Counterinsurgency on the Ground in Afghanistan: How different units adapted to local conditions* (Alexandria, VA: CNA, 2010), 1, accessed December 26, 2020. https://apps.dtic.mil/dtic/tr/fulltext/u2/a533649.pdf.

Parallelism in computer science refers to a system that can run multiple subtasks at the same time.[142] Concurrency refers to a system that works on multiple tasks at the same time.[143] While no exact translation to the space domain is readily apparent, a few abstract examples will illustrate the usefulness of these terms. A GNSS constellation provides a PNT signal to customers around the globe. All users of GNSS receive simultaneously. Interrupting access to the signal would require shutting the GNSS signal to all users. Parallelism could be a term to illustrate the challenge of using and deny an EMS signal to friendly and adversary forces at the same time. Concurrency in connection to the space domain refers to the way a communications satellite operates. Generically speaking, a communications satellite processes calls from multiple users concurrently. Each call or signal is an independent task. Controlling or interrupting specific signals from or to a satellite is possible (legal and resource availability aside).[144] Adversaries may also use a more brute force approach to jamming. Describing some portion of the EMS space segment as concurrent or parallel tasks informs the warfighter what type of challenge they are facing. The introduction of these terms further helps demonstrate the limitations of controlling access to space.

MSNA use space in ways that are currently unaccounted for in doctrine. Furthermore, the development of MDO, which is unlikely to change the nature of JP 3-14 and FM 3-14, has shifted what focus the US had on MNSA to near-peer competitors. Additionally, there is a grammatical challenge when considering MNSA and spacepower. The accumulation of these three issues, current doctrine, MDO, and insufficient grammar, results in a blind spot to the true sophistication

---

[142] Logan Stafman, "Designing for Performance: Concurrency and Parallelism" (lecture, Department of Computer Science, Princeton, University, Princeton, NJ, Fall 2015), 2, accessed December 10, 2020, https://www.cs.princeton.edu/courses/archive/fall15/cos518/lectures/L7-concurrency-parallelism.pdf.

[143] Umut A. Acar, "Parallelism versus concurrency," in *Parallel Computing: Theory and Practice* (Pittsburgh, PA: Carnegie Mellon University, 2016), accessed November 20, 2020, http://www.cs.cmu.edu/afs/cs/academic/class/15210f15/www/tapp.html#_parallelism_versus_concurrency.

[144] Harrison, Johnson, and Roberts, "Others: Kinetic Physical," 24.

of MNSA in the space domain. Future conflicts against MNSA will be space wars. Those wars may be limited to the surface and the airspace above the surface, but MNSA will use space to increasingly improve their operational reach as well as develop cross-domain capabilities to hinder or attack US forces.

Conclusion and Recommendations

This monograph set out to investigate the potential that US conceptualization, theory, and grammar of spacepower is inadequate to prepare for future conflicts with MNSA. The first research question in support of the thesis investigated whether the contemporary descriptions of spacepower theory are sufficient to constitute a comprehensive framework for the development of effective concepts and doctrine. The answer is no. Spacepower theory is still in the initial stages of development. There are multiple definitions of spacepower but there is a general failure to link those theories effectively with military doctrine.

The second question investigated if MNSAs have already demonstrated sufficient activity within and through the space domain to constitute being called space powers. The answer to this question is clearly yes. MNSA have access to SATCOM, PNT, and satellite imagery combined with a history of using these technologies. Spacepower is no longer the purview of the nation-state. Any entity with sufficient capital and technical capability can use space to its advantage. MNSA have and will use space even though the prospect of an organization like ISIS launching a satellite is negligible. Non-state actors may not be on the cusp of fighting a war in space, but they are already fighting wars through space.

The third question asked if current US doctrine and concepts use the proper grammar to account for MNSA actions in the space domain. The answer to this question is also no. Current doctrine including JP 3-14, FM 3-14, and FM 3-24 have sufficient gaps in them to create the possibility of a fundamental surprise in the space domain perpetrated by a MNSA. These documents offer either a broad overview of military spacepower as is the case in FM 3-14 and JP

3-14, or these documents do not properly account for an MNSA with spacepower, as is the case in all three documents. There is a significant enough gap in these doctrinal manuals to allow for MNSA to develop further capabilities beyond current conceptions. Furthermore, MDO, in its current form, continues this trend. MDO fully acknowledges the space domain as a critical warfighting domain. However, MDO ignores the development of MNSA as space powers. MDO is also driving organizational restructuring to the point where capability that can counter MNSA space activity will be used at organizations that are not the primary echelon fighting a low-intensity conflict. Space is no longer the domain of superpowers. The US is turning its focus away from MNSA as they accelerate their access to sophisticated space-enabled technologies that will further degrade the United States' ability to counter them.

The purpose of this monograph is to develop a clearer idea of the potential futures and trendlines in the development of MNSA use of space. Therefore, this study's secondary aim is to draw out recommendations within the DOTMLPF-F framework. These recommendations are not all-inclusive but are, in the author's view, necessary to avoid a fundamental surprise in the future. Given this goal, there are two primary recommendations for the future force. The recommendations fall within the doctrine and training and leader development categories. However, organizational changes may be needed in the future as well. As this monograph discussed in the analysis section, the MDO force structure is focused on echelons at the division level and above. In future low-intensity conflict against MNSA, brigades will need the capability to effectively counter space threats. However, organizational changes take considerable time and resources to affect. Therefore, a more immediate recommendation is to make doctrinal changes.

The first recommendation is to reevaluate the FM 3-24, *Insurgencies and Countering Insurgencies*; FM 3-14, *Army Space Operations;* and the implementation of the MDO concept.[145]

[145] For simplicity, this recommendation will focus on FM 3-14 and not JP 3-14. There is minimal distinction between joint and army space doctrine in its current formulation.

FM 3-24 needs updates to reflect the growing use of space by MNSA. MNSA are using space communications, satellite imagery, and GPS to achieve their aims on the battlefield. As the battlefield becomes more ill-defined, MNSA seek out weaknesses in the space and cyber domains, US forces must understand the space domain sophistication of these organizations. FM 3-24 must add a space domain focus when dealing with MNSA. FM 3-14 needs to be developed in tandem with FM 3-24 to address the threat of MNSA. These documents need to speak to who the various actors in space are and the way they may uniquely operate in those domains. Vignettes of historical case studies would be useful for this. Additionally, space doctrine needs to build a comprehensive picture of the ways MNSA and US forces may interact in the space domain. Adversaries will use the space domain to attack as well as to enhance their operations. Their use of space in parallel to the United States creates a nuanced challenge where the threat of MNSA's spacepower may not be readily apparent to US ground forces.

Regarding MDO, many of the limitations of the current doctrine persist. The MDO approach focuses on the US military's conceptual framework to the challenges of actors using sophisticated cross and multi-domain attacks. In addition to the recommendations for current doctrine, MDO needs to better acknowledge what MDO looks like at multiple points along the conflict continuum. The current design is a one size fits all approach. MDO should reflect low-intensity conflict as well. Updating FM 3-24 to incorporate MDO concepts would be a major step in the direction of avoiding the pitfall of ignoring MNSA with spacepower.

The second recommendation is to continue to develop training regimes that incorporate D3SOE. The first step in enhancing any training regime will be leader development. Educating leaders on the space domain must incorporate at least three components. These components include current space capabilities and how to employ them; how near-peer competitors will use space; and finally, the way existing space technologies are enabling MNSA operations. Leadership development is a necessary prerequisite for the development of any training regime. Leaders, who understand the integral nature of the space domain in warfighting as well as the

way adversaries may harness space to defeat US forces, can begin to develop training that tests current readiness.

A D3SOE space training regime provides US forces with experience when they are denied the GPS signal or SATCOM access. Training environments that incorporate these elements are effective for simulating a conflict against a near-peer competitor or a MNSA. Training should also focus on historical tactics, techniques, and procedures of MNSA space activities. This training should focus on situations where MNSA are accessing third-party satellites, the use of commercial satellite imagery for operations, and the proliferation of commercially available drones. MNSA will use these capabilities to operate in a geographically dispersed manner leveraging the dependence of US forces on space technology against the United States. Training regimes will be instrumental in identifying and closing the conceptual gaps in current doctrine to enhance future doctrine.

The current conceptualization of spacepower theory does not adequately incorporate MNSA as space powers. Any definition of spacepower must be sufficiently broad to incorporate the historic and future capabilities of MNSA. MNSA may not currently compete directly in space with the United States. However, MNSA are competing with the United States through space. MNSA's use of space capabilities to enhance their operational reach in the land, air, sea, cyber, and information domains is already occurring. The use of space by MNSA will only increase US operational problems in the future as US adversaries exploit spacepower to the United States' detriment.

Bibliography

Acar, Umut A. *Parallel Computing: Theory and Practice.* Pittsburgh, PA: Carnegie Mellon University, 2016. Accessed November 20, 2020. http://www.cs.cmu.edu/afs/cs/academic/class/15210-f15/www/tapp.html#_administrative_matters.

Antebi, Liran. "Unmanned Aerial Vehicles in Asymmetric Warfare: Maintain the Advantage of the State Actor." In *The Quiet Decade: In the Aftermath of the Second Lebanon War, 2006-2016*, 83-94. Tel Aviv, Israel: Institute for National Security Studies, 2017.

Arbatov, Alexi G., and Vladimir Dvorkin. *Outer Space: Weapons, Diplomacy, and Security*. Washington, DC: Carnegie Endowment, 2014.

Archambault, Emily, and Yannick Veilleux-Lepage. "Drone Imagery in Islamic State Propaganda: Flying like a State." *International Affairs* 96, no. 4 (July 2020): 955-973. Accessed October 20, 2020. https://academic.oup.com/ia/article/96/4/955/5813533.

Borum, Randy. *Psychology of Terrorism*. Tampa, FL: University of South Florida, 2004.

Burt, Kelly. D. "Space Power in Small Wars: The End of Asymmetric Advantage?" Master's thesis, School for Advanced Air and Space Studies, Maxwell Airforce Base, AL, 2020. Accessed August 1, 2020. https://apps.dtic.mil/dtic/tr/fulltext/u2/1019213.pdf.

Cancian, Matthew F. "Tactics, Techniques, and Procedures of the Islamic State Lessons for U.S. Forces" *Military Review* (March-April 2017). Accessed September 25, 2020. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2017/ART-009/.

Chadwick, Andrew. "The 2006 Lebanon War: A Short History." *Small Wars Journal* (September 11, 2012). Accessed November 13, 2020. https://smallwarsjournal.com/jrnl/art/the-2006-lebanon-war-a-short-history.

Chulov, Martin. "The rise and fall of the Isis 'caliphate'" *The Guardian*, March 24, 2019. Accessed October 22, 2020. https://www.theguardian.com/world/2019/mar/23/the-rise-and-fall-of-the-isis-caliphate.

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

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Cochrane, Paul. "Bombs and Broadcasts: Al Manar's Battle to Stay on Air." Arab Media & Society, March 7, 2007. Accessed November 22, 2020. https://www.arabmediasociety.com/bombs-and-broadcasts-al-manars-battle-to-stay-on-air/.

Cordesman, Anthony H. “The Lessons of the Israel-Hezbollah War: A Briefing.” Center for Strategic and International Studies, March 12, 2008. Accessed 1 November 2020. https://www.csis.org/analysis/lessons-israel-hezbollah-war.

Defense Intelligence Agency. *Challenges to Security in Space*. Washington, DC: Government Publishing Agency, 2019.

Dolman, Everett C. “New Frontiers, Old Realities.” *Strategic Studies Quarterly* 6, no. 1 (Spring 2012): 78-96. Accessed September 12, 2020. https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-06_Issue-1/dolman.pdf.

———. *Pure Strategy Power and Principle in the Space and Information Age*. New York, NY: Frank Cass, 2005.

Dudney, Robert S. Douhet. “The Legendary and Controversial Airpower Theorist is Debated to this Day.” *Air Force Magazine*, April 2011. Accessed November 12, 2020. https://www.airforcemag.com/PDF/MagazineArchive/Documents/2011/April%202011/0411douhet.pdf.

Ebrahim, Ebrahim K. “Thuraya Telecom Services Affected by Intentional Jamming in Libya.” Thuraya Telecommunications, February 25, 2011. Accessed July 15, 2020. https://www.thuraya.com/content/thuraya-telecom-services-affected-intentional-jamming-libya.

Eisler, Peter. “Google Earth Helps yet Worries Government.” ABC News, November 7, 2008. Accessed July 19, 2020. https://abcnews.go.com/Technology/story?id=6208093.

Federation of American Scientists. “Mumbai Terrorist Attacks.” Accessed October 20, 2020. https://fas.org/irp/eprint/mumbai.pdf.

Feickert, Andrew. IF11409. *Defense Primer: Army Multi-Domain Operations (MDO).* Washington, DC: Congressional Research Service, December 8, 2020. Accessed January 04, 2020. https://fas.org/sgp/crs/natsec/IF11409.pdf.

Feng, Emily. “ISIS use of Hobby Drone as Weapons Tests Chinese Makers.” *Financial Times*, December 15, 2020. Accessed October 17, 2020. https://www.ft.com/content/82a29f96-c9e7-11e7-ab18-7a9fb7d6163e.

Fidler, Beth. “Confirmation Testimony of New U.S. Space Force Commander Reiterates Concerns about Over-classification in Space, Calls for Review.” National Archives, August 18, 2020. Accessed December 14, 2020. https://transforming-classification.blogs.archives.gov/2020/08/18/confirmation-testimony-of-new-u-s-space-force-commander-reiterates-concerns-about-over-classification-in-space-calls-for-review/.

Finley, Klint. “It’d be Great to Kick ISIS Offline-If It Were Possible.” *Wired*, March 30, 2016. Accessed October 16, 2020. https://www.wired.com/2016/03/how-is-isis-online/.

Gabriel, Rachel A., and Barnett S. Coven. “Malicious Non-state Actors and Contested Space Operations.” NSI Inc., February 2018. Accessed August 2, 2020. https://nsiteam.com/malicious-non-state-actors-and-contested-space-operations/.

Gerges, Fawaz A. *A History of ISIS*. Princeton, NJ: Princeton University Press, 2016.

Glenn, Russell W. *All Glory is Fleeting: Insights from the Second Lebanon War*. Santa Monica, CA: RAND Corporation, 2012. Accessed November 10, 2020. https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG708-1.pdf.

Greenenmeier, Larry. "GPS and the World's First 'Space War.'" *Scientific American*, February 8, 2016. Accessed September 12, 2020. https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/.

Harrison, Todd, Kaitlyn Johnson, and Thomas G. Roberts. "Others: Kinetic Physical." In *Space Threat Assessment 2018*, 22. Washington, DC: Center for Strategic and International Studies, April 2018. Accessed September 20, 2020. https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf#page=28.

Harvey, Brian, Henk H. F. Smid, and Theo Pirard. *Emerging Space Powers the New Space Programs of Asia, the Middle East and South-America*. New York, NY: Springer, 2010.

Headquarters, United States Space Force (USSF). US Space Force Capstone Publication, *Spacepower*. Washington, DC: Government Printing Office, 2020.

Hoeing, Milton. "Hezbollah and the Use of Drones as a Weapon of Terrorism." Federation of American Scientists, June 5, 2014. Accessed October 16, 2020. https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism/.

Homeland Security Committee. *Terror Gone Viral: Overview of the 243 ISIS-Linked Incidents Targeting the West: House Homeland Security Committee Majority Staff Report 2014-2018*. Version 2.0. Washington, DC: Department of Homeland Security, 2018. Accessed October 20, 2020. https://www.hsdl.org/?view&did=817196.

Hyatt, James L., III, Paul L. Laugesen, Michael A. Rampino, Ronald R. Ricchi, and Joseph A. Schwarz. "Space Power 2010." Master's thesis, Air and Command Staff College Maxwell AFB, AL, 1995.

Israeli Defense Forces. "The Second Lebanon War: A Timeline." July 07, 2016. Accessed November 20, 2020. https://www.idf.il/en/articles/hezbollah/the-second-lebanon-war-a-timeline/.

Jenkov, Jackob. "Concurrency vs. Parallelism" Jenkov.com, November 17, 2020. Accessed November 27, 2020. http://tutorials.jenkov.com/java-concurrency/concurrency-vs-parallelism.html.

Johnson, David E. *Hard Fighting: Israel in Lebanon and Gaza*. Santa Monica, CA: RAND Corporation, 2011.

Johnson-Freese, Joan. *Space as a Strategic Asset*. New York: Columbia University Press, 2007.

———. *Space Warfare in the 21st Century: Arming the Heavens.* London: Routledge Taylor, 2017.

Kahn, Jeremy. “Mumbai Terrorists Relied on New Technology for Attacks.” *New York Times*, December 09, 2008. Accessed July 15, 2020. https://www.nytimes.com/2008/12/09/world/asia/09mumbai.html.

Kalb, Marvin, and Carol Saivetz. “The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict.” Research paper, Harvard Kennedy School of Government, Boston, MA, 2007.

Klein, John J. *Space Warfare: Strategy, Principles, and Policy*. London, UK: Routledge, 2006.

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Chicago, IL: The University of Chicago Press, 1996.

Kwasniewski, Nicolai. “How Islamic State Takes Its Terror to the Web.” *Spiegel International*, March 12, 2015. Accessed October 15, 2020. https://www.spiegel.de/international/world/islamic-state-uses-satellite-internet-to-spread-message-a-1066190.html.

Lambakis, Steven. *On the Edge of Earth: Future of American Space Power*. Lexington, KY: University Press of Kentucky, 2001.

Lanir, Zvi. *Fundamental Surprises*. Ramat Aviv, Israel: Center for Strategic Studies University of Tel Aviv, 1983.

Matthews, Matt M. “Hard Lessons Learned: A Comparison of the 2006 Hezbollah-Israeli War and Operation CAST LEAD: A Historical Overview.” In *Back to the Basics: A Study of the Second Lebanon War and Operation CAST LEAD.* Edited by Scott C. Farquhar, 5-44. Fort Leavenworth, KS: Combat Studies Institute Press, 2008. Accessed October 23, 2020. http://institutobrasilisrael.org/cms/assets/uploads/_BIBLIOTECA/_PDF/novos-conflitos-atualidades/948e1709b7c6e4fca1bb83fd4b45ca70.pdf.

Matthews, Matt M. *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*. Fort Leavenworth, KS: Combat Studies Institute Press, 2008. Accessed October 13, 2020. https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf.

Meyerle, Jerry, Megan Katt, and Jim Gavrilis. *Counterinsurgency on the Ground in Afghanistan: How different units adapted to local conditions.* Alexandria, VA: CNA, 2010. Accessed December 26, 2020. https://apps.dtic.mil/dtic/tr/fulltext/u2/a533649.pdf.

Miller, Gregory D. “Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists: Nonstate Threats in Space.” *Air & Space Power Journal* 33, no. 3 (Fall 2019): 33-51. Accessed September 12, 2020. https://search.proquest.com/openview/3555c15671f813f1a75817ced0a5f2d1/1?pq-origsite=gscholar&cbl=26498.

Millson, Christopher. “Comparing Counterinsurgency Tactics in Iraq and Vietnam.” *Inquiries Journal* 3, no. 5 (2011): 1. Accessed January 05, 2021. http://www.inquiriesjournal.com/articles/531/comparing-counterinsurgency-tactics-in-iraq-and-vietnam.

Nettis, Kimber. “Multi-Domain Operations: Bridging the Gaps for Dominance.” Sixteenth Air Force (Air Force Cyber), March 16, 2020. Accessed 20 October 2020. https://www.16af.af.mil/News/Article/2112873/multi-domain-operations-bridging-the-gaps-for-dominance/.

New York Times. “Mumbai Attack Sites,” Accessed December 12, 2020. https://archive.nytimes.com/www.nytimes.com/interactive/2008/11/26/world/asia/20081126-mumbai-attacks.html.

Opall-Rome, Barbara. “Inability to Jam Hezbollah Satellite TV Signal Spurs Israeli Research.” Space News, June 29, 2005. Accessed November 12, 2020. https://spacenews.com/inability-jam-hezbollah-satellite-tv-signal-spurs-israeli-research/.

Osinga, Frans P. B. *Science Strategy and War: The Strategic Theory of John Boyd*. New York, NY: Routledge, 2007.

Preston, Bob, Dana J. Johnson, Sean J. A. Edwards, Michael D. Miller, Calvin Shipbaugh, *Space Weapons: Earth Wars*. Santa Monica, CA: RAND Corporation, 2002.

Rabasa, Angel, Robert D. Blackwill, Peter Chalk, Kim Cragin, C. Christine Fair, Brian A. Jackson, Brian Michael Jenkins, Seth G. Jones, Nathaniel Shestak, and Ashley J. Tellis. *The Lessons of Mumbai*. Santa Monica, CA: RAND Corporation, 2009. Accessed October 18, 2020. https://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP249.pdf.

Rajagopalan, Rajeswari Pillai. “Managing New Actors in the Space Domain.” The Diplomat, June 29, 2019. Accessed September 23, 2020. https://thediplomat.com/2019/06/managing-new-actors-in-the-space-domain/.

Satellite Signals. “Satellite Internet in the Middle East.” April 20, 2020. Accessed December 2, 2020. https://www.satsig.net/ivsat2.htm.

SatPhone Shop. "Satellite Phones." Accessed February 13, 2021. https://www.satphoneshop.com/products/satellite-phones?p=1.

Schmidt, Michael S., and Eric Schmitt. “Pentagon Confronts a New Threat From ISIS: Exploding Drones.” *New York Times*, October 11, 2016. Accessed October 15, 2020. https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html.

Shactman, Noah. “How Gadgets Helped Mumbai Attackers.” *Wired*, December 01, 2008. Accessed October 22, 2020. https://www.wired.com/2008/12/the-gagdets-of/.

Shaikh, Shaan “The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense.” Center for Strategic and International Studies, December 8, 2020. Accessed February 03, 2021. https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense.

Smith, M. V. “Ten Propositions Regarding Space.” Ann Arbor, MI: Nimble Books LLC, 2011.

Smith, Matt. “To silence propaganda, Iraq seeks to take Islamic State offline.” *Reuters*, February 4, 2016. Accessed October 17, 2020. https://www.reuters.com/article/us-mideast-crisis-iraq-internet-insight-idUSKCN0VD0LM.

Stafman, Logan. “Designing for Performance: Concurrency and Parallelism.” Lecture, Department of Computer Science, Princeton, University, Princeton, NJ, Fall 2015. Accessed December 10, 2020. https://www.cs.princeton.edu/courses/archive/fall15/cos518/lectures/L7-concurrency-parallelism.pdf.

Tankel, Stephen. "Making the U.S. Military’s Counter-Terrorism Mission Sustainable." War on the Rocks, September 28, 2020. Accessed January 03, 2021. https://warontherocks.com/2020/09/making-the-u-s-militarys-counter-terrorism-mission-sustainable/.

Times of India. “How Google Earth Helped Mumbai Attackers.” December 19, 2009. Accessed July 15, 2020. https://timesofindia.indiatimes.com/india/How-Google-Earth-helped-Mumbai-attackers/articleshow/3862879.cms.

Tucker, Patrick. "The NSA Is Studying Satellite Hacking." Defense One, September 19, 2019. Accessed September 20, 2020. https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/.

United Nations Security Council. *Security Council Calls for end to Hostilities between Hizbollah, Israel, Unanimously Adopting Resolution 1701 (2006)*. 5511th Meeting (Night). August 11, 2006.

US Army. Field Manual (FM) 3-0, *Operations*. Washington, DC: Government Printing Office, 2008.

———. Field Manual (FM) 3-14, *US Army Space Operations*. Washington, DC: Government Publishing Office, 2019.

———. Field Manual (FM) 3-24, *Insurgencies and Countering Insurgencies*. Washington, DC: Government Publishing Office, May 13, 2014.

US Congress, Senate, *Lessons from the Mumbai Terrorist Attacks: Hearings before the Committee on Homeland Security and Governmental Affairs*. 111th Cong., 1st sess., January 8 and 28, 2009.

US Department of Defense, Joint Staff. Joint Publication (JP) 1-02, *DOD Dictionary of Military and Associated Terms.* Washington, DC: Government Publishing Office, 2020.

———, Joint Staff. Joint Publication (JP) 3-14, *Space Operations*. Washington, DC: Government Printing Office, 2018.

US Department of the Air Force. Doctrine Annex 3-99, *Department of the Air Force Role in Joint All-Domain Operations (JADO)*. Washington, DC: Government Publishing Office, 2020.

US Department of the Army. US Army Training and Doctrine Command Pamphlet (TRADOC Pam) 525-3-1, *The U.S. Army in Multi-Domain Operations, 2028.* Washington, DC: Government Printing Office, 2018.

Watson, Ben. “The Drones of ISIS.” Defense One, January 12, 2017. Accessed October 15, 2020. https://www.defenseone.com/technology/2017/01/drones-isis/134542/.

Wax, Emily. “Mumbai Attackers Made Sophisticated Use of Technology.” *Washington Post*, 3, December 2008. Accessed October 22, 2020. https://www.washingtonpost.com/wp-dyn/content/article/2008/12/02/AR2008120203519.html.

Wille, Dennis. *The Army and Multi-Domain Operations: Moving Beyond AirLand Battle*. Washington, DC: New America, October 2019. Accessed November 02, 2020. https://www.newamerica.org/international-security/reports/army-and-multi-domain-operations-moving-beyond-airland-battle/dedicate-a-brigade-level-experimental-task-force-to-army-futures-command.

Wilson Center. “Timeline: The Rise, Spread, and Fall of the Islamic State.” October 28, 2019. Accessed December 20, 2020. https://www.wilsoncenter.org/article/timeline-the-rise-spread-and-fall-the-islamic-state.

Wong, Wilson W. S., and James G. Fergusson. *Military Space Power: A Guide to the Issues*. Santa Barbara, CA: Praeger, 2010.

Zilber, Neri. “To Target Israel, Iran's 'Suitcase' GPS Kits Turn Hezbollah Rockets into Guided Missiles.” *The Daily Beast*, February 21, 2019. Accessed July 15, 2020. https://www.thedailybeast.com/to-target-israel-irans-suitcase-gps-kits-turn-hezbollah-rockets-into-guided-missiles.