UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

THE LAND, SPACE, AND CYBERSPACE NEXUS: EVOLUTION OF THE OLDEST MILITARY OPERATIONS IN THE NEWEST MILITARY DOMAINS

Jeffrey L. Caton

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

THE LAND, SPACE, AND CYBERSPACE NEXUS: EVOLUTION OF THE OLDEST MILITARY OPERATIONS IN THE NEWEST MILITARY DOMAINS

Jeffrey L. Caton

March 2018

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

*****

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *ssi.armywarcollege.edu*, at the Opportunities tab.

*****

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of certain reports may also be obtained free of charge while supplies last by placing an order on the SSI website. Check the website for availability. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *ssi.armywarcollege.edu*.

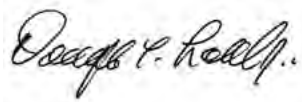
*****

The Strategic Studies Institute and U.S. Army War College Press publishes a quarterly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at the following address: *ssi.armywarcollege.edu/newsletter/*.

ISBN 1-58487-779-0

FOREWORD

The *Capstone Concept for Joint Operations* predicts that space and cyberspace will become increasingly important to joint operations and "will become both a precursor to and integral part of armed combat in the land, maritime and air domains."[1] How are U.S. military operations in the newest domains of space and cyberspace being integrated with operations in the traditional domain of land? In this monograph, Mr. Jeffrey Caton explores various aspects of this question by examining existing doctrine, operations in multiple domains, and future operations. His work was completed before the April 2017 release of the U.S. Army Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations*. He argues that the current state of military doctrine in the relatively new domains of space and cyberspace includes adequate means to support land-based joint operations. Further, he contends that knowledge of the nature of these new domains is not intuitive and understanding their unique characteristics and capabilities is still a challenge for the military force writ large. To address some of the challenges facing cross-domain operations, Mr. Caton provides recommendations in the areas of domain definitions, command relationships, and military theory. This monograph should inform the current work of the Army and Marine Corps in their exploration of the multi-domain battle concept.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ENDNOTES - FOREWORD

1. Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, Washington, DC: Department of Defense, September 10, 2012, p. 2.

ABOUT THE AUTHOR

JEFFREY L. CATON is President of Kepler Strategies LLC, Carlisle, Pennsylvania, a veteran-owned small business specializing in national security, cyberspace theory, and aerospace technology. He is also an Intermittent Professor of Program Management with Defense Acquisition University. From 2007 to 2012, Mr. Caton served on the U.S. Army War College (USAWC) faculty, including Associate Professor of Cyberspace Operations and Defense Transformation Chair. Over the past 7 years, he has presented lectures on cyberspace and space issues related to international security in the United States, Sweden, the United Kingdom, Estonia, Kazakhstan, and the Czech Republic, supporting programs such as the Partnership for Peace Consortium and the North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence. His current work includes research on the nexus of cyberspace, space, and landpower doctrine issues as part of the External Research Associates Program of the Strategic Studies Institute (SSI). Mr. Caton is also a member of the Editorial Board for *Parameters* magazine. He served 28 years in the U.S. Air Force working in engineering, space operations, joint operations, and foreign military sales including command at the squadron and group level. Mr. Caton holds a bachelor's degree in chemical engineering from the University of Virginia, a master's degree in aeronautical engineering from the Air Force Institute of Technology, and a master's degree in strategic studies from the Air War College.

SUMMARY

Over the last century, the domains of air, space, and cyberspace have joined the traditional warfighting domains of land and sea. While the doctrine for land operations is relatively mature, the doctrine for space and cyberspace continue to evolve, often in an unstructured manner. This monograph examines the relationships among these domains and how they apply to U.S. Army and joint warfighting. It concentrates on the central question: How are U.S. military operations in the newest domains of space and cyberspace being integrated with operations in the traditional domain of land? This inquiry is divided into three major sections:

- **Existing Doctrine**: This section explores the current state of joint and U.S. Army doctrinal development for each of the domains of land, space, and cyberspace. The discussion assumes the reader is familiar with the doctrine of land operations, and thus it focuses more on the newer and lesser-known domains of space and cyberspace.
- **Operations in Multiple Domains**: This section explores the concept of cross-domain synergy and its ability to enhance globally integrated operations. It also examines the existing processes and entities defined in doctrine that provide expertise and support to joint force commanders.
- **Future Operations**: This section explores probable future operating environments as well as the resulting implications for U.S. Army and joint force development. It also identifies operational challenges that cut across all domains. It includes recommendations for policymakers

and senior leaders regarding the future development and integration of space and cyberspace doctrine.

The scope of this monograph extends from current doctrine toward the anticipated operational environment over the next 20 years. Material considered and presented here is limited to unclassified and open source information; therefore, any classified discussion must occur via another venue. This monograph provides cursory summaries and observations of over a thousand pages of official joint and service documentation. Thus, it serves as a synopsis with analysis of the important issues related to joint operations in land, space, and cyberspace. This information should allow senior policymakers, decision makers, military leaders, and their respective staffs to gain common understanding and professional appreciation for the wide array of frameworks and concepts as well as their interconnections. Of course, the reader should always defer to the full text for details and context.

THE LAND, SPACE, AND CYBERSPACE NEXUS: EVOLUTION OF THE OLDEST MILITARY OPERATIONS IN THE NEWEST MILITARY DOMAINS

Over the last century, the domains of air, space, and cyberspace have joined the traditional warfighting domains of land and sea. While the doctrine for land operations is relatively mature, the doctrine for space and cyberspace continue to evolve, often in an unstructured manner. This monograph examines the relationships among these domains and how they apply to U.S. Army and joint warfighting. It concentrates on the central question: How are U.S. military operations in the newest domains of space and cyberspace being integrated with operations in the traditional domain of land? This inquiry is divided into three major sections: examination of existing doctrine in the three domains; analysis of operations in multiple domains; and analysis of the anticipated future joint operating environment (JOE) and the resulting implications for Army and joint operations and force development.

EXISTING DOCTRINE

> **joint doctrine**—Fundamental principles that guide the employment of United States military forces in coordinated action toward a common objective and may include terms, tactics, techniques, and procedures [emphasis added].[1]

In January 2012, President Barack Obama and Secretary of Defense Leon Panetta endorsed new strategic guidance for 21st-century defense priorities. Operations in cyberspace and space were among the 10 mission areas explicitly identified for additional

investment as the guidance asserted: "Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space."[2]

Put simply, doctrine documents the best way to conduct military operations based on experience of the past, capabilities of the present, and expectations of the future. This section explores the current state of doctrinal development for each of the domains of land, space, and cyberspace. First, it identifies the foundations for current joint operational doctrine. Next, it focuses on the domain-specific joint doctrine publications, and finally, it considers U.S. Army doctrine for the domains. The discussion assumes the reader is familiar with the doctrine of land operations, and thus it focuses more content and details on the newer and lesser-known domains of space and cyberspace. Let us begin with a look at the overarching tenets of joint doctrine.

Joint Doctrine for Operations in Traditional Domains

> **Joint operations** are military actions conducted by joint forces and those Service forces employed in specified command relationships with each other, which of themselves do not establish joint forces [emphasis in original].[3]

Military doctrine has been evolving for centuries. During most of this time military forces consisted of armies and navies, but within the last century U.S. military forces have formally adopted a construct that added three new domains—air, space, and cyberspace—to those of land and sea. With the establishment of the Joint Chiefs of Staff following World War II,

doctrine has become increasingly complex to address coordinated operations in multiple domains that may include actions from other U.S. Government entities as well as those of other nations.[4]

At the top of the current doctrine hierarchy is the capstone document Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States*, which provides the theory and foundation for subsequent doctrine publication.[5] Inspired by scholars such as Carl von Clausewitz and Sun Tzu, JP 1 places joint operations within the larger context of the nature of war that involves many potential instruments of national power as well as introduces the enduring principles of war and joint functions that are covered in greater detail in capstone publications.[6] It also introduces the joint force structure with dedicated components for land, air, maritime, and special operations components as well as outlines command and control (C2) structures and authorities.[7] As its title implies, the final chapter of JP 1 addresses joint force development, which includes the fundamentals of joint concepts, doctrine, education, and training. It is interesting to note that in JP 1 cyberspace is not listed as a domain, but rather as part of the information environment. In fact, JP 1 refers to "physical domain(s)" only three times, and it fails to explicitly identify these domains in the document.[8]

The next level in the joint doctrine hierarchy is the keystone publications that include JP 3-0, *Joint Operations*. In addition to describing the fundamentals and art of joint operations, it devotes a chapter to the six functions:

> **grouped together to help JFCs** [joint force commanders] **integrate, synchronize, and direct joint operations**. . . . **C2, intelligence, fires, movement and maneuver, protection, and sustainment** [emphasis in original].[9]

JP 3-0 also discusses the nine enduring principles of war identified in JP 1—objective, offensive, mass, maneuver, economy of force, unity of command, security, surprise, and simplicity—plus the three additional ones of restraint, perseverance, and legitimacy.[10] Like JP 1, JP 3-0 lists cyberspace as part of the information environment rather than in the list of domains, which it specifies as "air, land, maritime, and space."[11] Potentially adding to the confusion in discussing joint operations is the fact that "domain" is not defined in joint doctrine.

Doctrine publications comprise the final level of the joint hierarchy and these include documents that address the C2 for the joint operations of land, maritime, and air forces.[12] These are the most mature doctrine in terms of compiled experience, and they each have firm foundations in military theory, such as those of Clausewitz and Antoine-Henri Jomini for land; Alfred Thayer Mahan and Julian Stafford Corbett for maritime; and Hugh Trenchard and William Mitchell for air. Space and cyberspace operations (CO) each have joint publications as well, but generally lack the benefit of developed military theory as their foundation and often devolve to technical descriptions of their operation. Let us now examine how well space and cyberspace are incorporated into the current doctrine for land operations.

Joint Doctrine for Operations in the Land Domain

> **land domain.** The area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals [emphasis in original].[13]

JP 3-31, *Command and Control for Joint Land Operations* is centered on the concept of the joint force land component commander (JFLCC) as key link between the JFC and the C2 of joint land operations. Assigning a JFLCC provides the JFC with "**the ability to enhance synchronization of operations not only between US ground and component forces, but also with multinational land forces** [emphasis in original]."[14] The current JP 3-31 (February 2014) identifies five major forms of land operations that the JFLCC may accomplish: offensive, defensive, stability, homeland defense, and defense support to civil authorities. It also discusses how the six joint functions apply to land operations. JP 3-31 finishes with three appendices that provide additional details on the organization and planning of a JFLCC.[15]

To tackle complex operational and threat environments, JP 3-31 states up front "commanders at all levels should consider how space, cyberspace, and EMS [electromagnetic spectrum] capabilities enhance the effectiveness and execution of joint land operations."[16] Appendix I of this monograph provides verbatim excerpts of space- and cyberspace-related material contained in JP 3-31, but several items merit discussion here. Space operations can provide the JFLCC with "ISR [intelligence, surveillance, and reconnaissance]; missile tracking; launch detection; environmental monitoring; satellite communications [SATCOM]; position, navigation, and timing; and navigation warfare."[17] JP 3-31 emphasizes the benefits of global positioning system (GPS) and satellite imagery that provide valuable terrain information and personnel situational awareness for land-based operations as well as the communications that "may provide a critical link in the C2 architecture."[18] It is interesting to note that the JFLCC may also serve as the space

coordinating authority (SCA), but would most likely delegate this responsibility to the senior space officer on their staff.[19] The SCA will be covered in more detail under space doctrine discussions.

With regard to CO, JP 3-31 asserts that many advances in joint land operations "have been realized through the use of cyberspace and the electromagnetic spectrum (EMS), which has enabled the US military and allies to communicate and reach across geographic and geopolitical boundaries."[20] The JP advises the JFLCC to fully integrate CO capabilities into their plans with the purpose to "conduct CO to retain freedom of maneuver in cyberspace, accomplish objectives, deny freedom of action to adversaries, and enable other operational activities."[21] The C2 for such CO is accomplished via the JFC's Joint Cyberspace Center (JCC), which should include a JFLCC representative. In its chapter on operations, JP 3-31 explicitly distinguishes between CO, information operations (IO), and communications synchronization.

The inclusion of space and CO into JFLCC doctrine thus far appears to be appropriate, especially considering how recent the joint doctrine was introduced for cyberspace (12 months prior) and updated for space (8 months prior). The JFLCC notional headquarters includes both space and cyberspace sections aligned under the J-33 current operations. Also, the notional joint land operation plan explicitly includes these capabilities in its annexes—appendix 16 to annex C (Operations) covers CO; annex K (Communication Systems) includes cyberspace defense; and annex N focuses on space operations. Finally, a cursory review of the current doctrine for the joint force air and maritime component commanders (joint force air component commander via JP 3-30 and joint force maritime component commander via 3-32) reveals that they contain

much less detail when compared to JFLCC doctrine with regard to how space and CO are integrated in the other traditional domains. The joint doctrine for special operations (JP 3-05), which includes details on the C2 accomplished by the joint force special operations component commander's incorporation of space and CO, is on par with that of JP 3-31.

Joint Doctrine for Operations in the Space Domain

> Space is a domain enabling many joint force-essential capabilities. These capabilities derive from exploitation of the unique characteristics of space, among which include a global perspective and lack of overflight restrictions, as well as the speed and persistence afforded by satellites.[22]

JP 3-14, *Space Operations* was first released in August 2002, and it addressed space operations focused on the combatant command (CCMD) of U.S. Space Command (USSPACECOM) that was established in 1985. Ironically, after 17 years of waiting for joint space doctrine, large portions of JP 3-14 were obsolete only months later when USSPACECOM was disestablished and its missions moved under the new U.S. Strategic Command (USSTRATCOM) under changes mandated by the 2002 Unified Command Plan (UCP).[23] JP 3-14 was updated in 2009 to reflect the new organization of space forces under USSTRATCOM and updated to its current version in May 2013.

From the start, the JP 3-14 portrays space as a domain to support operations in the terrestrial domains, noting, "space capabilities have proven to be **significant force multipliers** when integrated into military operations [emphasis added]."[24] It emphasizes that space capabilities are sought by friendly nations and adversaries as well as commercial entities, making the space domain a "congested, contested, and competitive environment."[25] JP 3-14 asserts four unique characteristics of

the space domain: no geographical boundaries; orbital mechanics; environmental considerations of space weather and orbital debris; and EMS dependency. While it claims "international law does not extend a nation's territorial sovereignty up to Earth orbit," JP 3-14 also includes a section on critical legal considerations regarding obligations to international law for U.S. space operations.[26] However, the publication does not mention the crucial role of the United Nation's (UN) International Telecommunication Union (ITU) in allocating SATCOM orbits and radio spectrum.[27]

The current JP 3-14 identifies five joint space mission areas: space situational awareness (added in this revision); space force enhancement; space support; space control; and space force application. The mission of space force enhancement provides the most direct benefits to forces in other domains by providing intelligence, surveillance, and reconnaissance; missile tracking; launch detection; environmental monitoring; SATCOM; positioning, navigation, and timing; and navigation warfare.[28] Since the 2002 UCP change, joint space operations are conducted by USSTRATCOM, with the bulk of daily activities managed by the Joint Functional Component Commander for Space (JFCC SPACE), who provides "unity of command and unity of effort in the unimpeded delivery of joint space capabilities to supported commanders and, when directed, to deny the benefits of space to adversaries."[29] Two other authorities of interest in JP 3-14 are the designation of U.S. Cyber Command (USCYBERCOM) as the supported command for SATCOM and Defense Information Systems Agency (DISA) as the only authorized provider of SATCOM for the Department of Defense (DoD).[30]

For joint operations, the space coordinating authority (SCA) has the responsibility for planning and integrating space capabilities. The SCA may be delegated to the JFC for a specific operation who in turn may designate a component command or other individual to serve as the SCA.[31] For land operations, JP 3-14 states that the U.S. Army integrates space capabilities into their units using space support elements (SSEs), which coordinate with the SCA.[32] All space operations integration into joint planning includes the use of Annex N of a standard operational plan to describe space forces and capabilities relevant to the specific nature of the plan. JP 3-14 emphasizes that planners need to grasp the high-demand/low-density nature of some space capabilities as well as the challenges of space force augmentation or reconstitution.[33]

To provide overt connections to the joint tenets, JP 3-14 includes an overview of the 12 principles of joint operations from the perspectives of employing and enabling operations in the space domain, offering examples but no in-depth discussion.[34] Finally, to improve awareness of these limited resources, almost one-third of JP 3-14 is in the form of appendices that provide further detail into certain space capabilities as well as the technical "rocket science" nature of space operations.[35]

Although it got off to a slow start, the publication of joint space doctrine has evolved steadily since its introduction in 2002. However, there is still no widely accepted theory for military space operations and no definition for the space domain codified in joint doctrine. Both of these situations will be addressed in more detail later in this monograph.

Joint Doctrine for Operations in the Cyberspace Domain

> **cyberspace**. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [emphasis in original].[36]

Although military operations in cyberspace have been occurring for decades, it was not until 2010 that the DoD publicly codified cyberspace "as relevant a [man-made] domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[37] In July 2011, this pronouncement was further clarified as the inaugural DoD cyberspace strategy made its first of five strategic initiatives to "treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential."[38] This strategy followed 6 months after the establishment of the initial operational capability of USCYBERCOM.

Initially released in February 2013 as a secret document, JP 3-12, *Cyberspace Operations* was published in its current unclassified format as JP 3-12 (R) in October 2014.[39] The publication establishes a conceptual framework of cyberspace as three layers: a physical network layer that enables a logical network layer upon which operations are initiated by entities in the cyber-persona layer.[40] The intent of CO is to:

> enhance operational effectiveness and leverage various capabilities from physical domains to create effects, which may span multiple geographic combatant commanders' (GCCs') AOR [area of responsibility].[41]

As with space operations, the Commander, U.S. Strategic Command (CDRUSSTRATCOM), has overall responsibility for CO, most of which are carried out by the sub-unified USCYBERCOM. The JP identifies three types of CO missions: offensive CO (OCO), defensive CO (DCO), and DoD Information Network (DODIN) operations; it also defines related cyberspace actions that may be employed to accomplish the CO missions.[42] To help clarify these missions and actions, JP 3-14 (R) discusses in considerable detail how the six joint functions apply to CO.[43]

With regard to authorities, roles, and responsibilities, JP 3-12 (R) includes not only the U.S. Code Title 10 duties for joint cyberspace forces, but also potential support to other U.S. Government departments for national responses to cyberspace incidents as well as the protection of critical infrastructure and key resources (CIKR).[44] The publication identifies cyberspace support elements (CSEs) as the deployed units that integrate USCYBERCOM capabilities to CCMDs. CSEs help to achieve situational awareness in cyberspace as well as to develop target lists and synchronize joint fires in part through their coordination with the CCMD JCC (see Appendix II of this monograph for depiction of cyberspace C2 structure).[45]

Finally, JP 3-12 (R) considers how joint operations in cyberspace should mesh with joint, interorganizational, and international planning and coordination. It makes a crucial caveat regarding the complexity of cyberspace, noting, "second and higher order effects in and through cyberspace can be more difficult to predict, necessitating more branches and sequels in plans."[46] For the integration and synchronization of joint fires, use of cyberspace capabilities will follow an existing coordination apparatus, such as working

groups and prioritized target lists. Importantly, the JP clarifies that cyberspace capabilities may be not only a viable option for engaging joint targets, but also may be the best choice.[47]

Compared to joint space doctrine, the publication of the first joint cyberspace doctrine came soon after its designation as a warfighting domain. As with space, there is no widely accepted theory for military CO yet, and there remain significant uncertainties regarding how CO relates (or should relate) to IO and EMS constructs.[48]

Table 1 summarizes the major missions areas identified in joint publications for land, space, and CO. It also indicates whether a joint publication addressed the joint functions and principle of joint operations. Given this basic understanding of the key elements of the joint doctrine for these domains, let us now examine how U.S. Army doctrine treats them.

Domain	Joint Doctrine and Operational Missions Specified Therein	Joint Functions Addressed?	Principles of War/ Joint Operations Addressed?
Land	JP 3-31 (February 2014) • Offensive operations • Defensive operations • Stability operations • Homeland defense • Defense support of civil authorities	Yes	No
Space	JP 3-14 (May 2013) • Space situational awareness • Space force enhancement • Space support • Space control • Space force application	No	Yes
Cyberspace	JP 3-12 (February 2013) • OCO • DCO • DODIN operations	Yes	No

Table 1. Comparison of Land, Space, and Cyberspace Joint Operations Doctrine.[49]

Army Land Operations Doctrine

Following the establishment of the Army Training and Doctrine Command (TRADOC), doctrine for Landpower has evolved from the venerable Field Manual (FM) 100-5, *Operations* (1976, 1982, 1986, 1993 versions), to the new designation of FM 3-0, *Operations* (2001, 2008 versions), and finally to the current Army Doctrine Publication (ADP) No. 3-0, *Unified Land Operations*.[50] Published in October 2011 as part of the Doctrine 2015 initiative, ADP 3-0 is the latest evolution of the capstone document that provides a

common operational concept for U.S. Army forces that must "operate across the range of military operations, integrating their actions with joint, interagency, and multinational partners as part of a larger effort."[51] The main focus of U.S. Army units in this team effort is to "seize, retain, and exploit the initiative to gain and maintain a position of relative advantage in sustained land operations to create conditions for favorable conflict resolution."[52]

ADP 3-0 recognizes that the dynamic operational environment includes interactions with other domains. It identifies the foundations of unified land operations as initiative, decisive action, U.S. Army core competencies (combined arms maneuver and wide area security), and mission command. It also presents the tenets of unified land operations as flexibility, integration, lethality, adaptability, depth, and synchronization. ADP 3-0 discusses six warfighting functions consistent with those of joint doctrine, except that the U.S. Army replaces C2 with mission command. A concise document by design, ADP 3-0 refers to space and cyberspace as domains in the operational environment, but does not include any other specific details with regard to how the domains affect land operations.[53]

Army Space Operations Doctrine

In 2006, TRADOC published Pamphlet 525-7-4, *Space Operations Concept Capability Plan* (CCP), in part to "Systematically and deliberately evolve Army space support operations over time to provide dedicated, responsive theater focused support to operational and tactical commanders."[54] The CCP stresses the joint interdependency of military operations, and asserts that "space operations are inherently joint, and joint interdependence is essential for the conduct of

all space operations."[55] Pamphlet 525-7-4 identifies the Army Space and Missile Defense Command/Army Forces Strategic Command as the Army Service component to joint space operations that provides support for SATCOM, theater missile warning, blue force tracking, and situational awareness.[56] The CCP uses a detailed operational vignette to demonstrate how space capabilities would support the Army Modular Force construct and concludes, "space power must be viewed in the larger construct of joint operations. Army space operations depend on the successful Army and joint transformation and exploitation of the space domain."[57]

The U.S. Army published the first FM 3-14, *Space Support to Army Operations in 2005*, which superseded FM 100-18 (1995) under the older doctrine system. FM 3-14 was updated in 2010 and again updated in August 2014 to its current version, *Army Space Operations*.[58] This latest version added a distribution restriction, therefore its content cannot be discussed in detail herein.[59] In general terms, FM 3-14 remains very consistent with the content of JP 3-14, echoing the five joint mission areas for space. FM 3-14 also discusses how the foundations and tenets of unified land operations from ADP 3-0 apply to space operations. It then provides details regarding how the U.S. Army organizes space units as well as how SSEs support different U.S. Army echelons. For practical application, FM 3-14 includes an appendix that provides a detailed template for Annex N to joint plans and orders.

U.S. Army Cyberspace Operations (CO) Doctrine

In February 2010, TRADOC released the *Cyberspace Operations Concept Capabilities Plan* (Pamphlet 525-7-8), with its central idea of:

> prevailing in the cyber-electromagnetic contest means making progress at the same time along three lines of effort: gaining advantage, protecting that advantage, and placing adversaries at a disadvantage.[60]

Pamphlet 525-7-8 emphasizes the interrelated nature of cyberspace operations (CyberOps or CO), electronic warfare (EW), and IO, and proposes that the U.S. Army address these complex notions at three levels: a psychological contest of wills, a strategic engagement, and a cyber-electromagnetic contest.[61] The Cyberspace Operations CCP offers a CyberOps framework comprised of four components: cyber situational awareness (CyberSA), cyber network operations (CyNetOps), cyber warfare (CyWar), and cyber support (CySpt).[62] The pamphlet appendices use three operational vignettes to help identify and propose many required capabilities for CyberOps. As intended, the CCP provides the conceptual foundation upon which subsequent U.S. Army cyberspace doctrine—FM 3-38 and FM 3-12—is built.

Published in February 2014, FM 3-38, *Cyber Electromagnetic Activities*, is the first attempt by the U.S. Army to produce an FM focused on integration and synchronizing of the new concept of cyber electromagnetic activities (CEMA).[63] FM 3-38 provides an overview of the CEMA concept and the commander's role in CEMA operations (see Appendix III of this monograph for a graphic depiction of the CEMA concept). It then dedicates a chapter to the tactics and procedures for three areas: CO, EW, and spectrum management operations. The FM closes with discussion on how CEMA is planned, integrated, and executed in unified land operations.

FM 3-38 was released a year after the release of the classified JP 3-12, and its description of CO are consistent with details of the releasable version of JP 3-12

(R) that followed 8 months later. The FM echoes the three-layer depiction of cyberspace (physical, logical, cyber-persona) as well as the three missions of cyberspace forces (OCO, DCO, and DODIN) and Cyberspace Operational Preparation of the Environment (C-OPE). It also provides details on the interfaces between CEMA and LandWarNet (the U.S. Army's portion of the DODIN) in CO and DODIN planning and operations.

There are many favorable aspects of the content in FM 3-38. First, the FM embraces the cross-domain nature of cyberspace. Next, it explicitly spells out the soldier's role in CEMA to help them better "understand the relationship between cyberspace and the EMS and maintain the necessary protection measures when using devices that leverage this relationship between capabilities."[64] The FM presents the CEMA element as the part of a commander's staff that "integrates CEMA into the operations process from theater Army through brigade"[65] as well as a CEMA working group to coordinate with internal and external units and centers.[66] Finally, FM 3-38 provides a practical and detailed template for documenting CEMA as appendix 12 to annex C (Operations) in a standard joint operations plan or order.

Attempts to develop U.S. Army cyberspace doctrine have been in work for years, but the proposed FM 3-12, *Cyberspace and Electronic Warfare Operations* had not yet been published at the conclusion of the research for this monograph.[67] Despite the delay in the completion of this FM, the U.S. Army is doing well with incorporating space and cyberspace into traditional land operations. To apply this information to the education of its senior leaders, the U.S. Army War College's Center for Strategic Leadership released a *Strategic Cyberspace Operations Guide* in June 2016.[68] However, there

remains much to do as land-based operations adapt to space and cyberspace domains that continue to evolve and grow in their significance to operations across multiple domains.

OPERATIONS IN MULTIPLE DOMAINS

Having reviewed the basic joint and U.S. Army doctrine for land, space, and cyberspace, let us now explore how operations in the domains interact. This section explores the concept of cross-domain synergy and its ability to enhance globally integrated operations. It also examines the existing processes and entities defined in doctrine that provide expertise and support to JFCs. Do joint forces in these three domains have existing means available to facilitate cross-domain synergy?

Capstone Concept for Joint Operations (CCJO)

To support the President's and Secretary of Defense's 21st-century defense priorities, the Joint Chiefs of Staff published the new *Capstone Concept for Joint Operations for Joint Force 2020* (CCJO) in September 2014. Its central concept is globally integrated operations that embody eight key elements.[69] The CCJO predicts that space and cyberspace will become increasingly important to joint operations and "will become both a precursor to and integral part of armed combat in the land, maritime and air domains."[70] Space and cyberspace forces also present "flexible, low-signature or small-footprint capabilities" that are:

> rapidly deployable, largely able to operate independently from logistically intensive forces, have operational reach, and can be persistent. Perhaps most significantly, their

> use does not always constitute an irreversible policy commitment.[71]

The CCJO also asserts that cyberspace capabilities enable global agility necessary to support "swift and adaptable military responses."[72] Further, it considers that adversaries may also find such operational advantages attractive and opt to attack exclusively in cyberspace.[73]

In its prognosis of future threat environments, the CCJO expects adversaries to obtain advanced capabilities that can be applied across multiple domains. To help posture joint forces for success, the globally integrated operations concept includes the key element of cross-domain synergy that will allow an integrated joint force "to exploit even small advantages in one domain to create or increase advantages in others, compounding those mutually reinforcing advantages until they overwhelm an enemy."[74]

Cross-Domain Operations

In January 2016, the Joint Staff J-7 published the *Cross-Domain Synergy in Joint Operations Planner's Guide* in part to address this element of the CCJO's goal of globally integrated operations. The guide defines cross-domain synergy as "the complementary vice merely additive employment of capabilities in different domains such that each enhances the effectiveness and compensates for the vulnerabilities of others."[75] The *Planner's Guide* stresses that cross-domain synergy "is not an end in itself, but a by-product of effective joint planning."[76] It avers that the major challenge of achieving such synergy is for the JFC to access and utilize diverse domain expertise; hence, the guide provides a brief primer of how existing support and liaison elements can provide support within the joint

operation planning process (JOPP).[77] In turn, effective joint planning is dependent in part upon the planners' knowledge of each domain's strengths and vulnerabilities. While cross-domain operations have been an integral part of U.S. military operations for decades, the incorporation by planners of capabilities from the new domains of space and cyberspace is in its infancy.

Unique Domain Characteristics and Capabilities

The *Planner's Guide* provides an overview of capabilities, characteristics, and operations for each of the traditional domains, plus space and cyberspace. It is useful to explore how the guide views the individual domains before looking at how it discusses cross-domain operations. Much of the guide's material appears in joint doctrine, but it includes some new commentary as well. Let us examine how the guide portrays the domains for land, space, and cyberspace.

Land Domain. Table 2 presents an analysis of aspects of the land domain presented as unique by the *Planner's Guide*. Although the proposed traits may be consistent with joint doctrine, collectively they are misleading. Certainly, land is not the only domain to have significant operational environment variations—all domains have such factors that help define the domain itself. Also, noncombatants are present in all physical domains, and their safety must be a consideration in joint operations. The two most distinctive characteristics of the land domain are: the ability to assemble large supply stores for sustained operations, and the slower movement of forces across land when compared to movement in other domains.

Land Domain	
Proposed Unique Characteristic or Capability*	**Critical Assessment**
(a) Extreme variations in climate and terrain—urban, forest, desert, jungle, mountain, and arctic—present dramatically different operational environments.	**(a) Not unique**. Climate and topography also have significant implications for the design and operation of maritime, air, and space forces.
(b) Presence of people, especially non-combatants, effects options for use of military force.	**(b) Not unique**. Although the vast majority of Earth's population lives on land, people are present in the sea domain for extended periods of time as well. Also, the presence of non-combatants must be considered in all domains.
(c) The ability to sustain operations over long periods of time.	**(c) Unique**. One can argue that extended sea and air operations ultimately depend upon land-based assets through ports and airfields for long-duration sustainment.
(d) The speed and duration of movement on land is slower and more arduous than movement by air and sea.	**(d) Unique** (on average). Movement of large land forces over unfamiliar terrain may be a limiting factor of a given operation.
(e) With respect to non-lethal effects, only land forces have directly useful capability that can be precisely applied in complex, human terrain. Non-lethal effects work through example and the potential threat of violence rather than the execution of that threat. Although all services have the ability to affect their counterparts through security assistance activities, only land forces can achieve the position (close to the population dispersed in complex land clutter) and duration (persistence) that permits sustained non-lethal effect.	**(e) Inaccurate**. The topic of this paragraph is unclear, but it contains several elements that are not necessarily tied to land. One can argue that cyberspace can also have long-term and persistent contact with dispersed populations to achieve non-lethal effects using means such as social media.

Note: *The text from this column is from the *Cross-Domain Synergy in Joint Operations: Planner's Guide*.[78]

Table 2. Assessment of Land Characteristics and Capabilities.

Space Domain. Table 3 shows the assessment of how the space domain is depicted in the *Planner's Guide*. Upon examination, none of the characteristics or capabilities listed is truly unique. Indeed, operations in all domains must consider the environment, utilize EMS, and obey the laws of physics. The *Planner's Guide* defines space as "a medium like the land, sea, and air within which military activities shall be conducted to achieve US national security objectives,"[79] however, this definition in not included in official joint doctrine. Despite the lack of a clear demarcation for space by the United States and many other countries, there are still many international treaties and conventions that attempt to govern its use.[80]

Space Domain	
Proposed Unique Characteristic or Capability*	**Critical Assessment**
(a) There are no geographical boundaries in space. As a **Global Commons**, space overcomes the international law aspect of a nation's territorial sovereignty [emphasis in original].	**(a) Not unique**. One can argue that geosynchronous orbit spots have some equivalence to sovereignty based on the location and frequency use of the satellite.**
(b) Satellites are subject to the laws of orbital mechanics. Adjustments to orbits expend fuel and reduce asset life span.	**(b) Not unique**. All physical domains are subject to the laws of physics.
(c) Environmental considerations place demands on satellites' characteristics to include size, weight, and power, further hindering the spacecraft's performance and life span.	**(c) Not unique**. Recall that the land domain section also tried to claim the environment as its unique trait (see Table 2). Again, each domain must consider environmental factors in operational planning.
(d) Though space is infinite in expanse, certain altitudes and orbital patterns are advantageous. These portions of space are becoming crowded.	**(d) Not a characteristic or capability**. The statement is an observation about the current construct and population of space objects.

Table 3. Assessment of Space Characteristics and Capabilities.

(e) Electromagnetic spectrum access is vital to space operations because it is the sole medium for space-based assets to transmit and receive information and/or signals [emphasis in original]. Therefore, JFCs must sufficiently control the EMS to interact with space systems.	**(e) Not unique**. Certainly use of the EMS enables space operations, but the EMS supports operations in all domains (this will be discussed in more detail in the implications section of this monograph).
(f) Space is no longer a domain exclusively transited by state actors. Many non-state actors maintain assets in orbit and often military capabilities (Iridium satellite phones, Virgin space tourism, etc.) employ these non-state assets.	**(f) Not unique**. Space has been used by nonstate actors since 1961, 4 years after Sputnik 1. The evolution and proliferation of commercial and other nonstate space assets has evolved with military use.

Notes: *The text from this column is from the *Cross-Domain Synergy in Joint Operations: Planner's Guide*.[81]
**For more on this topic, see Iulia-Diana Galeriu's "'Paper satellites' and the free use of outer space."[82]

Table 3. Assessment of Space Characteristics and Capabilities. (cont.)

Cyberspace Domain. Table 4 summarizes the analysis of how the cyberspace domain is described in the *Planner's Guide*. Like the descriptions of land and space, the portrayal of cyberspace is fraught with inaccuracies, the most egregious of which are those that infer that activities in cyberspace are almost magic in that they are not subject to the limitations of time and space. In fact, the transmission of information must comply with the laws of physics, albeit on a much smaller scale than those of the traditional domains. The *Planner's Guide* includes a table taken from a scholarly work that compares "Cyberspace vs. Traditional Warfare Domain Characteristic," but the table contents do not match those in the guide's text.[83] Curiously, the guide omits the one unique aspect of cyberspace

explicitly noted in the 2010 *Quadrennial Defense Review Report*:

> The man-made nature of cyberspace distinguishes it from other domains in which the U.S. armed forces operate. The Administration will continue to explore the implications of cyberspace's unique attributes for policies regarding operations within it.[84]

FM 3-38 provides a much better rendering of cyberspace for those unfamiliar with the domain. The manual's discussion on the characteristics of the cyberspace domain includes many concepts that merit attention, such as cyberspace as a system of systems; its dynamic and evolving nature; its lack of confinement to a physical site; and the continued maintenance required for its existence.[85] FM 3-38 also includes an alternative definition that may provide better insight to planners: "Cyberspace is an environment created and maintained for the purpose of facilitating the use and exploitation of information, human interaction, and intercommunication."[86]

Cyberspace Domain	
Proposed Unique Characteristic or Capability*	**Critical Assessment**
(a) Cyberspace is a **global** enabler for expedient, dynamic information exchange impacting all aspects of life [emphasis in original]. It allows instantaneous information flow across the globe for financial transactions as well as the movement and tracking of products and goods. However, it also allows adversaries to access this information and disrupt vital operations from any location. Cyberspace is difficult to regulate due to ease of accessibility. From a military perspective, cyberspace activities rarely require movement of forces, allowing engagement from extended stand-off ranges. It also enables the influence of populations that are inaccessible through the other domains.	**(a) Inaccurate**. These characteristics appear to be more appropriate for describing a commons rather than a domain. Also, the use of "instantaneous information flow" is misleading since transmission of data through cyberspace takes a finite amount of time that has great relevance on the scale of timing for CO.**
(b) ***Can be reverse engineered:*** Unlike munitions, which are normally destroyed upon use, cyberspace activities include code that can be saved, analyzed, and recoded for use against allies or friendly nations [emphasis in original]. Planners must account for the possibility of a "boomerang effect" in which cyber activities are turned against the originator through reverse engineering.	**(b) Inaccurate**. This proposed trait confuses the domain of cyberspace with the potential weapons used therein. It may not be possible to recreate all aspects of cyberspace for forensics or reserve engineering due to the nature of complex adaptive systems. Also, physical weapons may not detonate as intended and may be used in an improvised manner by an adversary or may leave behind remnants that are subject to forensics.
(c) ***No Single National/International Ownership:*** While someone owns each physical component of cyberspace, the whole of cyberspace is not under any single nations' or entities' complete control [emphasis in original]. The infrastructure is a disparate combination of public and private networks without standardized security or access controls. This arrangement enables free information flow, but the lack of controls hinders global accountability, standardization, and security.	**(c) Not unique**. No single nation or entity owns all of the land, maritime, air, or space domains either.

Table 4. Assessment of Cyberspace Characteristics and Capabilities.

Cyberspace Domain	
(d) ***Lack of Cooperation/Collaboration:*** The lack of international laws and regulations governing the environment complicates responses to actions in this domain [emphasis in original]. The difficulty in tracing the source of a cyberattack makes them easily deniable, especially if conducted by individual "hackers." Further hindering collaboration is the tendency to deny that a cyberspace attack has occurred to prevent loss of trust in an organization's cyber security measures.	**(d) Inaccurate**. While the processes are far from perfect, there is significant cooperation and collaboration in cyberspace through such organizations as the UN, European Union, International Criminal Police Organization, and the North Atlantic Treaty Organization (NATO).*** In fact, one could argue that the Internet would not exist and function without ongoing cooperation and collaboration in cyberspace.
(e) ***Low Cost:*** Cyberspace is the most affordable domain through which to attack the United States [emphasis in original]. Viruses, malicious code, and training are readily available over the Internet at no cost. Adversaries can develop, edit, and reuse current tools for network attacks. Inexpensive tools and training allow an adversary to compete without costly ships, aircraft, or missiles. Furthermore, an adversary can impose significant financial burdens on nations that rely heavily on cyberspace by forcing them to invest in cyberspace defense. Currently, "military-grade" cyberspace capabilities remain too expensive for most malign actors, but they can buy relatively inexpensive services of professional hackers.	**(e) Inaccurate**. This characteristic would benefit from a more complete context. As stated, it reflects popular beliefs that readily available computer code can rival the power of sophisticated weapons systems. The concept of affordability here is misleading in that low-cost access to cyberspace does not equal capabilities of a nation state. One could argue that, given the same analogy, perhaps an assassin's rifle is equal to the power of an army.
(f) ***Volatile:*** Successful cyberspace attacks depend on vulnerabilities within the adversary's network [emphasis in original]. Identifying these vulnerabilities and creating cyberspace capabilities sometimes require great expense. If an adversary discovers the targeted network's vulnerability and closes it, the cyberspace attack technique is rendered immediately and unexpectedly useless despite the development expense. For this reason, great care must be taken to prevent alerting adversaries to vulnerabilities in their networks.	**(f) Inaccurate**. The term "volatile" may apply to activities in cyberspace, but one can argue that such volatility also exists in land operations (e.g., the fog and friction of war). Perhaps a more useful characterization would be to model cyberspace as a complex adaptive system. It is interesting to note that there seems to be conflicting perspectives promulgated within this entry "(f)"and previous entry "(e)" regarding the cost of cyberspace attacks.

Table 4. Assessment of Cyberspace Characteristics and Capabilities. (cont.)

Cyberspace Domain	
(g) ***Speed:*** Cyberspace operations [CO] occur quickly [emphasis in original]. However, preparation for those operations is often extensive. An intense study of the adversary's network may be required to learn system specifications and understand patterns of life. Therefore, a cyberspace unit operating on one adversary's networks may not be able to shift focus to another target without substantial preparation.	**(g) Inaccurate and not unique**. This entry mingles speed of operations, operations tempo, and C-OPE. Operations in other domains may also occur quickly after extended ISR and planning. As with characteristic entry "(a)," use of the word "quickly" is vague and of little use without a time scale for CO.
(h) ***Unintentional cascading effects:*** Another unique characteristic of cyberspace is the potential for unintended cascading effects [emphasis in original]. Capabilities and munitions in the natural domains lose momentum the greater distance from impact. However, physical distance means very little in cyberspace. While cyberspace capabilities are developed and evaluated in computer labs and cyberspace ranges, there can never be complete assurances as to how a capability will behave or where it might spread when introduced to the great expanse of cyberspace.	**(h) Not unique and inaccurate**. Physical weapons may also experience "unintended cascading effects." Also, the assertion that "physical distance in cyberspace means very little" propagates an ignorance of the timescales of cyberspace activity. Information traveling through cyberspace is still subject to finite speeds that may affect their integration and synchronization with other operations.
(i) ***Layers:*** Cyberspace consists of three layers: Physical Network, Logical Network, and Cyber-Persona [emphasis in original].**** **Adversaries might attack any of these layers to disrupt, degrade, or destroy cyberspace capability. Conversely, each of these layers presents a means to attack adversaries' use of cyberspace** [emphasis in original].	**(i) Inaccurate.** While this is useful information, it is one of many artificial constructs used to analyze cyberspace rather than an intrinsic characteristic.

Notes: *The text from this column is from the *Cross-Domain Synergy in Joint Operations: Planner's Guide*.[87]
**For more on this topic, see the *Internet Traffic Report*.[88]
***For more on this topic, see the U.S. Government Accountability Office (GAO) Report 10-606.[89]
****For more on this topic, see the *Planner's Guide*.[90]

Table 4. Assessment of Cyberspace Characteristics and Capabilities. (cont.)

Some readers may find the assessments in Tables 2 to 4 to be a bit pedantic; however, accuracy matters in the quest to equip joint planners with a full and common understanding of what a domain of military operations comprises. As an inaugural document to encourage cross-domain synergy, the *Planner's Guide* has considerable merit. It is reasonable to assume that the sections for specific domains were written or influenced by practitioners who may unwittingly advocate their domain vice merely describe it. Perhaps such bias may be addressed in future versions by comparing an impartial set of characteristics amongst the domains vice trying to argue for "unique" attributes. Surely, the development and acknowledgment of basic theory for military operations in space and cyberspace could provide the necessary foundation upon which to build better doctrine.

Support Relationships Among Domains

Having assessed the individual domain interpretations for land, space, and cyberspace, let us now consider how doctrine incorporates the means advocated in the *Planner's Guide* to achieve cross-domain synergy. Table 5 is a composite of excerpts from doctrine covered in the first section of this monograph that are organized to illustrate how these three domains support each other's missions. Note that this is not to be confused with a discussion of roles for supported versus supporting commanders. Clearly, there are ample examples in existing doctrine to demonstrate how the domains enable or enhance joint operations. Most of these examples would remain the same if sea or air substituted for land.

Domain with Supporting Capabilities	Domain with Supported Capabilities		
	Land	**Space**	**Cyberspace**
Land		Plan for and provide force protection for space infrastructure and forces assigned, deployed, and operating in their [CCMD] AOR.[91]	Operations in cyberspace rely on the links and nodes that exist in the natural domains. . . . Operations in the other domains create effects in and through cyberspace by affecting the EMS, the data, or the physical infrastructure.[92]
Space	GPS plays a key role in military operations by enabling precise location and navigation in all four physical domains (land, maritime, air, and space).[94]		Space provides a key global connectivity option for CO.[93]
	The inherent precision of GPS allows precise site surveys, emplacement of artillery, target acquisition, and navigation. GPS establishes a "common reference grid" within the operational area, enables a "common time," helps establish "common direction," and facilitates synchronized operations.[96]		[T]he linkages between space and cyberspace are of particular importance as space provides a global connectivity option for CO.[95]
	The space support element [SSE] . . . Supports the G-2 (S-2) during intelligence preparation of the battlefield.[98]		Space capabilities provide cyberspace with a global reach.[97]
			GPS plays a key role in military operations . . . by providing precise timing in cyberspace.[99]
			The space support element [SSE] . . . Provides space-based expertise and services that enhance CEMA. . . . Integrates space-related capabilities into CEMA planning. . . . Analyzes and recommends the potential employment of additional space-related capabilities to support CEMA.[100]

Table 5. Mutual Support Relationships Among Land, Space, and Cyberspace.

Cyberspace	The physical domains (air, land, maritime, and space) and information environment rely on cyberspace for instant communications.[102]	CO provide a means by which space support is executed.[101]	
	[O]perations in cyberspace enable freedom of action for operations in the four natural domains and the EMS.[103]	[C]yberspace provides the means by which space control and transmission of space sensor data are conducted.[104]	
	Using OCO, commanders can mass effects through the employment of lethal and nonlethal actions leveraging all capabilities available to gain advantages in cyberspace that support objectives on land.[106]	Operations in the space domain depend on cyberspace and the EMS to execute space support.[105]	
Mutual Space and Cyberspace		The relationship between space and cyberspace is unique in that virtually all space operations depend on cyberspace, and a critical portion of cyberspace can only be provided via space operations. . . . These interrelationships are important considerations across the spectrum of CO, and particularly when conducting targeting in cyberspace.[107]	
		These interrelationships are critical, and the linkages must be addressed during all phases of joint operation planning.[108]	
		The cyberspace and space domains are uniquely interrelated primarily because of their current role in telecommunications and networks. . . .These interrelationships are important considerations when planning for CEMA.[109]	
		CO produces NAVWAR [navigation warfare] effects by assuring friendly access and/or denying enemy access to positioning, navigation, and timing information transmitted by global navigation satellite system (GNSS) or other radio navigation aid signals. Creation of global and theater NAVWAR effects is attained through the coordinated employment of CO, EW, and space operations.[110]	

Table 5. Mutual Support Relationships Among Land, Space, and Cyberspace. (cont.)

The bottom portion of Table 5 focuses on areas of operational interdependence between space and cyberspace, most of which deal with signal transmission. Further, JP 3-12 (R) provides insight into the complex interactions between space, cyberspace, and the EMS, as well as the effects they can collectively realize:

> **Domain Overlap.** CO enhance operational effectiveness and leverage various capabilities from physical domains to create effects, which may span multiple GCCs AOR. Some of the capabilities the JFC may employ in conjunction with, or to enable CO, include significant portions of electronic warfare (EW), EMS management, C2, intelligence, surveillance, and reconnaissance (ISR), navigation warfare (NAVWAR), and some space mission areas. Advancements in technology have created an increasingly complex OE [operational environment]. CO, space operations, and EW operations can be conducted against targets using portions of the EMS. They can be integrated with other information related capabilities as part of IO. CO, space operations, and EW operations are often conducted under specific authorities. Likewise, some information-related capabilities supported by CO, such as MISO [military information support operations], MILDEC [military deception], and special technical operations (STO), have their own execution approval process [emphasis in original].[111]

The evolving interplay of space, cyberspace, information, and EMS operations at times resembles a doctrinal Gordian Knot that can frustrate planners and warfighters pursuing mission command necessary to conduct unified land operations.[112] What support elements are available to help the JFLCC cope with this situation?

Domain Support to JFLCC

Table 6 recaps the key elements of space and cyberspace forces from joint doctrine and organizes them by the type of integration they may provide for the JFLCC to achieve cross-domain synergy. If properly implemented, the existing arrangements appear to provide an acceptable framework for integrating and synchronizing space and CO into the JFLCC. As per the routine development of doctrine, the tactical details from actual experience should be captured and documented

in media such as joint and service lessons learned and tactics, techniques, and procedures.

Integration Means	Space	Cyberspace
Depiction of notional organizational structure?	No	Yes (JP 3-12 (R) Figure IV-1)
Link to JOPP plans and orders?	Annex N	Annex C (Appendix 16) and Annex K
Enduring support element?	SSE	CSE
Operational support elements?	• Space Operations Section in J-33 Current Operations • Space Tasking Order • Missile Warning Support Request*	• Cyberspace Operations Section in J-33 Current Operations • Cyberspace Cell in J-5 • Joint Cyberspace Center (JCC) • Cyberspace Effects Request Form**

Notes: *The Missile Warning Support Request.[113]
**Cyberspace Effects Request Form.[114]

Table 6. Space and Cyberspace Cross-Domain Elements in JFLCC Doctrine.

Joint force development and the refinement of doctrine also require the consideration of new concepts driven by strategic insights from DoD and the joint staff.[115] Having now explored the cross-domain tenets and nominal applications of land, space, and cyberspace means to achieve synergy in JFLCC operations, let us now investigate two derivative documents of

the CCJO that further address the future challenges of operational access to domains.

Operational Access

In January 2012, the DoD released the *Joint Operational Access Concept* (JOAC) to describe "how joint forces will operate in response to emerging antiaccess and area-denial security challenges."[116] It focuses on a central theme of cross-domain synergy and it "envisions a greater degree and more flexible integration of space and cyberspace operations [CO] into traditional air-sea-land battlespace than ever before."[117] The concept argues that one of the three key trends affecting future joint force projection is "the emergence of space and cyberspace as increasingly important and contested domains."[118] The JOAC supposes that operations in these new domains will precede those in the traditional domains, perhaps even to the degree that "even in the absence of open conflict, operations to gain and maintain cyberspace superiority and space control will be continuous requirements."[119]

To guide the planning of joint access operations, the JOAC proposes 11 Operational Access Precepts, the last of which is to "protect friendly space and cyber assets while attacking the enemy's space and cyber capabilities" since these domains "are now essential to all joint force projection."[120] Further, the JOAC infers that the success of space and CO may leverage the combat power from the traditional domains.[121] In general, this shift to focus on space and cyberspace is a theme throughout the JOAC. Several of the precepts favor reduced use of land forces that is offset in many cases by increased space and CO. One precept specifically cautions against over-committing forces into

hostile territory, especially major land forces.[122] The precept to "seize the initiative by deploying and operating on multiple, independent lines of operations," predicts a reduced presence in the land domain, as it "suggests smaller units and platforms that are rapidly deployable yet lethal."[123] Also, the precept aimed at disrupting enemy anti-access/area denial (A2/AD) capabilities notes that "large land forces generally will be the last to penetrate within range of an enemy's antiaccess and area-denial weapons because of the potential for catastrophic loss."[124] Finally, with regard to basing options, the JOAC suggests a minimized dependence on forward bases with more dependence on capabilities such as long-range strike, cyberspace, space, and EW.[125] The JOAC avers that space and cyberspace capabilities may be used in advance of other forces to facilitate operational access.[126] In addition, the JOAC alleges that cyberspace capabilities may help to maximize operational surprise and complicate enemy targeting processes.[127]

Entry Operations

In April 2014, Chairman of the Joint Chiefs of Staff Martin Dempsey released the *Joint Concept for Entry Operations* (JCEO) as his "vision for how joint forces will enter onto foreign territory and immediately employ capabilities to accomplish assigned missions."[128] The JCEO was written to support the JOAC with a central idea of "full integration of force capabilities across domains."[129] The concept calls for the use of "mission-tailored joint forces that are organized, trained, and equipped with unique capabilities."[130] The JCEO lists seven operational characteristics that are mostly enduring considerations with the exception of the relatively new characteristic of "social media,

cultural factors, and commercial capabilities" which has ties to CO and IO.[131]

Consistent with JOAC, the JCEO calls for earlier use of cyberspace capabilities, and explicitly calls for pre-crisis activities to include C-OPE that is "clearly integrated and synchronized with operations in other domains."[132] Cyberspace may also be used to enable operational deception efforts to gain surprise, complicate the enemy's targeting process, and reduce collateral damage.[133] Also, space and cyberspace can enable joint fires as well as enhance joint and allied C2 interoperability for cyberspace.[134] Finally, the JCEO contends that properly integrated cyberspace and space capabilities may enhance land maneuver.[135]

It appears that the inculcation of cross-domain synergy into the joint force remains a work in progress. Fortunately, existing concepts and doctrine provide the necessary foundation upon which to build and hone joint capabilities that span domains as required by circumstance. Joint concepts such as the CCJO, JOAC, and JCEO anticipate increased contributions from capabilities in the space and cyberspace domain to enable the success of future military operations, especially those faced with A2/AD challenges. How will this future unfold for the joint force?

FUTURE OPERATIONS

Armed with knowledge of how activities in the individual domains of land, space, and cyberspace may intersect and integrate to enhance joint force operations, let us now explore how such operations may change in the future. This section explores probable future operating environments as well as the resulting implications for the U.S. Army and joint force

development. It also identifies operational challenges that cut across all domains and makes recommendations to help prepare for the envisioned future.

Future Environment

Joint Operating Environment (JOE)

In July 2016, the joint staff released *Joint Operating Environment, JOE 2035: The Joint Force in a Contested and Disordered World*, to convey future security contexts and implications to aid the joint force development. In its view of the evolving world order, *JOE 2035* contends that regional powers will pursue competitive space and cyberspace capabilities that enable their global reach.[136] These capabilities may be enhanced by the proliferation of technologies, such as high-powered radio frequency (HPRF) weapons and non-nuclear electromagnetic pulse (EMP) weapons that may counter U.S. strengths in space and cyberspace.[137] *JOE 2035* weaves this trend into two of its six Contexts of Future Conflict. The context of "Disrupted Global Commons" centers on the "denial or compulsion in spaces and places available to all but owned by none."[138] The context assumes an enduring land-centric nature of conflict, noting that much of the conflict in commons is intended to influence events on land.[139] Also, this context predicts very intense rivalry for EMS usage as well as increasingly fierce military activities in the space domain that may include intentional interference from other satellites or ground-based systems as well as anti-satellite weapons (ASAT).[140]

The *JOE 2035* purposefully excludes cyberspace from the global commons context, instead giving it an exclusive context on "A Conflict for Cyberspace,"

where it suggests, "conflict and war are likely to occur as states struggle to define and credibly protect sovereignty in cyberspace."[141] In addition to direct military conflict at the tactical and operational levels as well as attacks on homeland critical infrastructure, *JOE 2035* foresees the conflict expanding to all elements of national power, noting that "the competition may involve disrupting data, networks, and the physical systems of competitors to gain economic, military, and political advantages."[142] Finally, this context infers that cyberspace capabilities are paradoxical in that the strengths provided by the vast and complex connectivity of the domain may also introduce substantial weaknesses:

> Where land and naval power intersect in two dimensions, air and space in three, cyberspace intersects with other domains in thousands, or even millions of ways. This presents many new vulnerable points through which weapons systems, and the circuitry and software upon which they rely, will be directly engaged.[143]

To address such threats and challenges, *JOE 2035* proposes a series of 24 evolving joint missions organized by 4 groups of enduring military tasks. While all of these missions may utilize support from space and cyberspace capabilities, the missions connected with the two contexts described above have explicit and significant expectations for space and cyberspace forces. Table 7 provides some excerpts from *JOE 2035* in each of these mission areas to provide the reader with an appreciation for the depth and diversity of capabilities required for the joint force should these projections come to fruition.

Enduring Military Tasks	Space and Cyberspace-Related Missions
Shape or *contain* to assist the United States with coping and adapting to changed international security conditions [emphasis in original].	*Freedom of Navigation and Overflight*. . . . Specifically, the Joint Force may conduct ambiguous actions and deception operations with low-signature assets to avoid direct confrontation with a competitor, while still demonstrating U.S. resolve to use and keep open the commons for military and civilian purposes [emphasis in original]. *Military Support to Cyber Resiliency*. This mission will require cyber support to U.S. Government and civilian organizations, allied nations, and other international partners that credibly reinforces the resilience of cyber-dependent systems and infrastructure. This includes a capacity to reliably communicate, compute, store, and retrieve critical data that outpaces adversary efforts to deny these capabilities [emphasis in original].
Deter or *deny* to manage the antagonistic behavior of competitors or to impose costs on competitors or adversaries taking aggressive action [emphasis in original].	*Global Commons Stabilization*. . . . Joint Force must be capable of protecting national objectives in the global commons despite the use of asymmetric, unconventional, and hybrid approaches by competitors to assert new claims and exercise more control in the commons. This will require operations that impose costs on adversaries who impede free use of the commons, such as targeted electromagnetic and space denial measures, the enforcement of sanctions, or the establishment of electromagnetic exclusion zones [emphasis in original]. *Network Defense*. These missions will require steady-state information operations [IO] in support of national cyber deterrence strategies that communicate the resiliency of critical U.S. systems and infrastructure, while protecting their vulnerabilities. Key actions may include the development of a Department of Defense [DoD] cyber umbrella; the creation of a national 'cyber border patrol;' more comprehensive intelligence sharing efforts; contributions to national level cyber exercises; the development of hardened networks; and reinforced coordination with domestic law enforcement [emphasis in original].

Table 7. Evolving Joint Missions for Space and Cyberspace from *JOE 2035*.[144]

Enduring Military Tasks	Space and Cyberspace-Related Missions
Disrupt or *degrade* to punish aggressive action by an adversary or to force an adversary to retreat from previous gains [emphasis in original].	*Global Commons Defense*. . . . the Joint Force must maintain the ability to conduct targeted command and control [C2] warfare, counter ISR operations, and discriminate sensor interdiction and spoofing in all commons. Furthermore, the Joint Force should be capable of responding to the threat of adversaries creating debris fields in important orbits [emphasis in original]. *Cyberspace Disruption*. . . . Additionally, the Joint Force may conduct proportional cross-domain operations to physically damage an adversary's cyber infrastructure, using weapons operating in other domains to suppress enemy cyber defenses and specifically strike their critical cyber infrastructure. Furthermore, these operations should be coupled with defensive cyber efforts to block adversary responses, and might include the use of autonomous or semi-autonomous cyber defense systems or the activation of war reserve networks when peacetime networks are unavailable [emphasis in original].
Compel or *destroy* to impose desired changes to the international security environment and subsequently enforce those outcomes [emphasis in original].	*Global Commons Exclusion*. . . . This will likely include multi-domain offensive operations using coordinated and simultaneous electronic, cyber, space, and kinetic actions to eradicate adversary capabilities that can influence or affect the commons [emphasis in original]. *Cyberspace Control*. . . . Cyberspace control operations will frequently integrate cyber and non-cyber capabilities. In coordination with law enforcement agencies, offensive operations may be required to identify, target, and capture or kill adversary cyber operatives. Offensive operations will also be used to eradicate an adversary's cyber infrastructure and capabilities, which might include an array of kinetic strikes combined with simultaneous electronic, cyber, and space warfare actions [emphasis in original].

Table 7. Evolving Joint Missions for Space and Cyberspace from *JOE 2035*. (cont.)

A complete evaluation of *JOE 2035* is beyond the scope of this monograph, but clearly in it the joint staff foresees military roles and cross-domain operations for the space and cyberspace domains that far exceed those of the present day. But is this view shared by other similar examinations of the future?[145]

Global Risks 2035

The Atlantic Council report *Global Risks 2035: The Search for a New Normal* echoes many of the themes of the *JOE 2035,* also through the perspective of changing demographics, international governance, and technology advancement.[146] For the global commons of space, the commentary envisions increased dependence and competition for space systems that may tempt state and nonstate actors to disrupt space operations. Escalation of conflict may occur and:

> if an arms race in space does get under way among the United States, China, Russia, India, Brazil, Japan, and other countries, these countries are likely to employ symmetric and asymmetric measures to counter the threats in space and coming from space.[147]

The study treats cyberspace issues with more imminent concern. The author lists the task to "Stop the slide towards a segmented internet. There is [sic] needs to be rules governing offensive cyber" as part of 11 items in a recommended "100-Day Checklist for the New Administration."[148] From a global commons framework, the report projects that cybersecurity costs may eventually outweigh the benefits for advanced economic countries like the United States.[149] From a domain framework, the author asserts, "Cyber is now transforming the nature of conflict and war."[150] Expanding on this theme, the study warns against possible disruption by cyberattacks without warning

from a variety of state and nonstate actors. However, the discussion focuses on critical infrastructure attacks and crime in cyberspace; the report does not address any roles of cyberspace in warfare.

Implications for the Army and the Joint Force

Anticipated future trends favor the decreased emphasis on traditional large-scale land operations and increased frequency and intensity of conflict in space and cyberspace. What are the implications and challenges that may result from these trends?

LandCyber

The U.S. Army's concept for achieving its cross-domain synergy is LandCyber, a transformational convergence of land and CO similar to the U.S. Army's AirLand Battle concepts to address challenges in the European theater in the 1980s. The central idea of LandCyber is for the U.S. Army to:

> think globally and act locally in the cyberspace domain in conjunction with land forces to shape the physical and virtual security-related behavior of humans and their machines to gain opportunity and advantage.[151]

The path to achieve LandCyber is described in a September 2013 white paper from the Army Cyber Proponent of U.S. Army Cyber Command (ARCY)/2nd U.S. Army. It identifies eight aspects of convergence and nine guiding principles as the foundation for LandCyber.[152] The white paper provides an overview of the U.S. Army roles and responsibilities in cyberspace that include C-OPE, critical infrastructure protection, integration into exercises, and CCMD support. It also gives near, mid, and long-term projections of cyberspace

evolution.[153] Although it discusses emerging CO similar to joint cyberspace doctrine, the LandCyber white paper lists U.S. Army mission areas as cyberspace control; cyberspace forces enhancement; cyberspace support; and cyberspace force application—a mission set similar to that in joint space doctrine.[154] The white paper includes an insightful discussion of how the LandCyber capabilities are related to the traditional warfighting functions.[155] Overall, the LandCyber concept adopts an approach that is holistic and forward leaning in scope.

FM 3-38 appears to embody many of the tenets of LandCyber, although there the FM contains no reference to the concept. At the conclusion of the research for this monograph, the highly anticipated U.S. Army document FM 3-12, *Cyberspace and EW Operations*, was not complete.[156] Recent status briefings indicate that FM 3-12 will include fundamentals of cyberspace and EW operations as well as CEMA considerations. It may also tackle the issue of addressing the relationships that cyberspace operations have on space operations, IO, intelligence, and targeting. Finally, it should include appendices that cover organization for CO, cyberspace information required for operations orders, and standard formats for cyber effects or EA requests.[157]

Joint Force Development

When considering the type of cross-domain operations that the United States may encounter in the near future, it is important to note that potential adversaries may be working along similar lines of effort. Although a detailed exploration of potential adversaries is beyond the scope of this monograph, the vignette from the cross-domain *Planner's Guide* on Russian actions

in Georgia (August 2008) captures the realm of the possible:

> The war between Georgia, Russia, and the Russian-backed self-proclaimed republics of South Ossetia and Abkhazia saw some 35,000-40,000 Russian and allied forces, augmented by significant air and naval forces, confront some 12,000-15,000 Georgian forces with little air and minimal naval capability. Although a short and limited conflict, it was historic and precedent setting. This appears to be the first coordinated cyberspace attacks synchronized with major combat actions in the other warfighting domains, primarily land and air. . . . In summary, Russian planners tightly integrated CO with their kinetic, diplomatic, and strategic messaging operations. The Russo-Georgian war provides a case study for joint planners preparing for a future conflict, involving the new domain of cyberspace.[158]

The CCJO identifies 23 explicit force development implications to enable globally integrated operations. Five of these implications directly address force development required for space and cyberspace forces in the joint functional areas of C2, fires, movement and maneuver, and protection (see Table 8). The JOAC and JCEO provide more detailed force development goals focused on capabilities to enhance entry operations; these include significant requirements for space and cyberspace capabilities (see Appendix IV of this monograph).

Command and Control:	***Enhance our ability to operate effectively in*** a degraded ***environment***. Given dramatic increases in the ability of adversaries to disrupt, degrade or destroy cyberspace and space systems, it is essential that Joint Forces be able to operate effectively despite degradation to those systems. Greater resilience must be built in to technical architectures, and the force must regularly train to operate in "worst case" degraded environments [emphasis in original].
Fires:	***Provide*** a fire support coordination capability ***that integrates all fires, including cyber.*** Key to maximizing cross-domain synergy will be fielding a system for planning, requesting and directing all available fires so any element of a Joint Force can access the most appropriate supporting arm. In particular, realizing the global potential of Joint Forces will require that previously niche capabilities, such as offensive cyber weapons, are available to Joint Force commanders [emphasis in original].
Movement and Maneuver:	***Rapidly employable on a global scale***. As a nation with global responsibilities, the forces of the United States must be able to operate effectively anywhere in the world on short notice. This can be achieved through multiple means. Massed force, deployed to the scene, is certainly one way. Low-signature and low-footprint capabilities, such as cyber and global strike, can also project force quickly. Versatility, too, plays a role. Forces suitable for a variety of missions, if smartly positioned, maximize the chance of being prepared for a crisis [emphasis in original].
Protection:	***Improve cyber defense capabilities***. Given the heavy reliance of Joint Forces on military computer networks and civilian critical infrastructure, it is essential that Joint Forces be able to defend key systems and ensure the continuity of critical network functions in the face of disruption [emphasis in original]. ***Continue to improve defensive space capabilities***. Given the heavy reliance of Joint Forces on space systems and the rapidly increasing proliferation of counterspace systems, it is essential that Joint Forces be able to protect friendly space capabilities, including defensive space control and space situational awareness capabilities [emphasis in original].

Table 8. Force Development Priorities for Space and Cyberspace from CCJO.[159]

The efforts described in Table 8 reflect the premise that space and cyberspace will be hotly contested domains, and thus their defenses must be improved. Also, the CCJO makes it clear that other force development efforts should carefully deliberate over their dependence on space and cyberspace capabilities as well as ponder how to compensate for disruption of activities in these domains. Finally, some of these force development efforts may push beyond the limits of technical feasibility and affordability.[160]

Other Operational Challenges

There are several themes of operational challenges common to many of the documents examined in this monograph. While beyond the scope herein to explore these themes, they merit serious study and incorporation into the general dialogue of future joint forces.

Dealing with Disruption. The CCJO and *JOE 2035* stress that commanders should be prepared to deal with disrupted and degraded space and cyberspace capabilities that may be attacked using advanced weapons (HPRF and EMP). Such disruptions should be studied not only for tactical and operational impacts, but also for strategic implications. For example, interfering with certain on-orbit assets, such as GPS and missile warning satellites, may evoke greater consequences than the local SATCOM jamming.

Cross-domain Deterrence. The refinement of cross-domain synergy can help to clarify the intentions of deterrence measures as well as enhance their effectiveness. The traditional strategic deterrence anchored with nuclear weapons may evolve to incorporate space and cyberspace means due to their growing utility and value.[161]

The Leadership Dimension. Concepts such as LandCyber that are enabled by space and cyberspace means hope to provide unprecedented situational awareness and connectivity at the lowest echelons. While such a construct offers great promise for enhancing unified land operations, it also creates challenges for effective mission command such as the increased potential for commanders to micromanage their troops.[162]

Autonomous Systems. The *JOE 2035* addresses the evolution of autonomous and robotic technologies and weapon systems. Such capabilities have the potential to enhance joint operations, but they will likely be used by adversaries as well for applications in the battlespace and against the U.S. homeland.[163] For current operations, the legality and ethics surrounding remotely-operated weapon systems are contentious issues in international venues such as the UN.[164]

Electromagnetic Spectrum. Within U.S. military doctrine, EMS is generally viewed as a critical enabler to operations in all domains.[165] Current U.S. Army doctrine provides useful codification of EMS within its CEMA construct. However, the status of EMS within the body of doctrine remains muddled as do related terms such as EW and EA.[166] Many practitioners and scholars argue that EMS is worthy of being named as the sixth warfighting domain; this remains an open dialogue.[167]

Recommendations

Physical Limitations in Cyberspace

Time and Distance in Cyberspace. Recommend that the parameters of time and distance be considered as significant parameters for CO, and that the transfer

of information never be characterized as being instantaneous. Rather, they are governed by the laws of physics and, therefore, cyberspace capabilities are affected by the distance that they traverse (despite to JOAC's assertion to the contrary).[168] Many large U.S. brokerage firms have applied this fact to their economic advantage by locating their servers as close as possible to the Wall Street servers to reduce the transmission times of their high-speed trading. In addition to the distance traveled, planners should note the existence and potential effects of "cyberspace weather/traffic" in the commons that may impede the delivery of "cyber payloads." Like terrestrial weather, these phenomena may be difficult to predict in such cases as the flood of social media surrounding unforeseen events such as the death of Michael Jackson or Prince.

Limits of Human Cognition in Cyberspace. Current concepts and doctrine infer that human operations can exercise effective C2 in the cyberspace domain. However, much of the activity in cyberspace occurs at speeds well beyond the human ability to comprehend. Recommend that the joint community add the realm of "ultra-tactical operations" to the traditional tactical-operational-strategic spectrum.[169] This concept could also be of great utility for applications of artificial intelligence and autonomous weapon systems.

Command Relationships

USCYBERCOM as CCMD. Recommend that USCYBERCOM remain as a sub-unified command. The vision of future operations articulated in the JOAC and *JOE 2035* support the wisdom of consolidating the global-reaching capabilities, such as strategic nuclear strike, missile defense forces, and cyberspace forces, under the unified command of USSTRATCOM.

Historians will recall the push in the late 20th century for the unified command of space to be elevated to its own service. Its reduction from CCMD to the JFCC under USSTRATCOM did not significantly hamper joint space operations.

Space C2 Structure. Recommend that the next version of JP 3-14, *Space Operations*, clarify the notional C2 relationships between USSTRATCOM, CCMD and its service components, and combat support agencies by adding a diagram and supporting text. Figure IV-1 of JP 3-12 (R) should serve as the model, thus enhancing cohesion between the two JPs.

Domain Definitions

Define Domain. Recommend that the DoD and the joint staff develop an official definition of military domain. Common usage in joint doctrine may infer the ability to apply sovereignty or the ability to achieve dominance or local superiority; or it may merely refer to physical characteristics. Regardless, theory and doctrine should include the establishment of precise language that can eliminate pedantic arguments and facilitate intellectual dialogue on such topics. The definition could include a set of parameters common in concept but not in application. For example, domain parameters such as boundaries, seams with other domains, and environmental disruptors may be useful for comparison and enhancing cross-domain operations. Also, representation of land, space, and cyberspace domains should be refined in future versions of the *Cross-Domain Planner's Guide* to address issues identified in Tables 2 through 4 of this monograph.

Domain versus Commons. In many joint documents the term "commons" (or "global commons") is

used interchangeably with certain domains. In addition to codifying a definition for domain, recommend that the DoD and the joint staff not only provide a definition for commons (or global commons) but also provide discussion for when it is appropriate to use the term. A starting point may be the JOAC description of a global commons as "areas of air, sea, space, and cyberspace that belong to no one state."[170]

A suggested distinction to consider and refine is for "domain" to be used for applications focused on military activities (e.g., organize, train, equip, and operate) and for "commons" to be used for applications that explicitly include other instruments of national power (e.g., diplomatic and economic).

Define the Space Domain. Recommend that the DoD and the joint staff develop an official definition for the space domain. Granted, the seam between air and space domains may not be significant to current cross-domain operations. However, future space operations may include more routine traversing of vehicles to and from space as well as more airborne systems operating at extremely high altitudes.

Discuss Domain-Specific Terrain. Recommend future versions of domain-specific joint doctrine publications include a discussion on the notion of "key terrain" in the domain. Such discussion could address whether the terrain is transient, enduring, or a mixture; how it can be influenced by blue or red forces; what lines of communication and choke points exist; and what factors influence movement in and through the given domain.

Supported and Supporting Roles

Space and Cyberspace in the Lead. Current joint doctrine makes mention of the possibility that space or CO may be designated as the supported activities, but does not address how this might occur. Recommend future joint doctrine include examples of how the supporting efforts in traditional domains may support main efforts in the space or cyberspace domains.

Priorities for Cyberspace Resources. The CCJO and *JOE 2035* set high expectations for future U.S. military cyberspace forces with little regard of the feasibility of these forces to be able to cover all the tasks. In turn, this may foster unrealistic expectations for U.S. Government, commercial, and international entities with regard to the support they may receive for "cyber resiliency" efforts.[171] Recommend that future DoD and joint staff publications strive to emphasize the high-demand/low-density aspects of cyberspace capabilities as well as a realistic evaluation of military cyberspace support outside of military operations during periods of intense and widespread conflict.

Enduring Military Theory

Discussion of Joint Functions and Principles. Recommend that future versions of joint doctrine publications for domain operations include a brief discussion on the 12 principles of joint operations as well as the 8 joint functions. This will enhance understanding of how common theories and principles of military operations apply to specific domains as well as provide a common lexicon and topics for comparison amongst domains. The use of vignettes in these discussions may enhance understanding for the joint community.

Military Theory for Space and Cyberspace. One can argue that military activities in space and

cyberspace are the least intuitive to comprehend and the least understood by military planners and operators. Recommend that the DoD and the joint staff actively support the development of military theory to help provide a foundation for increased knowledge in the joint force. Such efforts should be promulgated throughout the spectrum of military professional education.

Summary

By their very nature, military doctrine and operations are works in progress. In general, the current state of military doctrine in the relatively new domains of space and cyberspace include adequate means to support land-based joint operations. However, knowledge of the nature of these new domains is not intuitive, and understanding their unique characteristics and capabilities is still a challenge for the military force writ large. Anticipated future trends favor the decreased emphasis on traditional large-scale land operations and increased frequency and intensity of conflict in space and cyberspace, perhaps even where these newer domains may become preeminent for a given operation. The joint staff's pursuit of achieving cross-domain synergy in planning and operations offers a credible method to face some of the challenges of the future joint force, but this will likely remain an evolutionary vice revolutionary endeavor.

ENDNOTES

1 Joint Chiefs of Staff, Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, Washington, DC: Joint Chiefs of Staff, as of August 2017, p. 123, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf*, accessed February 12, 2018.

2 Department of Defense (DoD), *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Washington, DC: U.S. Department of Defense, January 2012, p. 5, available from *http://archive.defense.gov/news/Defense_Strategic_Guidance.pdf*, accessed November 7, 2016. The full text regarding this mission area is:

> **Operate Effectively in Cyberspace and Space**. Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space. Today space systems and their supporting infrastructure face a range of threats that may degrade, disrupt, or destroy assets. *Accordingly, DoD will continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space* [emphasis in original].

3 Joint Chiefs of Staff, JP 3-0, *Joint Operations*, Washington, DC: Joint Chiefs of Staff, January 17, 2011, p. I-1, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_20170117.pdf*, accessed September 19, 2016.

4 Joint Chiefs of Staff, *Joint Military Operations Historical Collection*, Washington, DC: Joint Chiefs of Staff, July 15, 1997, p. v-vi, available from *http://www.jcs.mil/Portals/36/Documents/History/Monographs/JMO.pdf*, accessed November 3, 2016.

5 Joint Chiefs of Staff, "Joint Doctrine Hierarchy Chart," February 6, 2016, Washington, DC: Joint Chiefs of Staff, available from *http://www.jcs.mil/Doctrine/Hierarchy-Chart/*, accessed February 12, 2018.

6 Joint Chiefs of Staff, JP 1, *Doctrine for the Armed Forces of the United States*, Washington, DC: Joint Chiefs of Staff, March 25, 2013, Incorp. Change 1, July 12, 2017, pp. I-3, I-17–I-19, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2017-12-23-160207-587*, accessed September 19, 2016.

7 Ibid., p. IV-3. In JP 1, Figure IV-1, "Possible Components in a Joint Force," depicts the notional relation of the joint force components to the joint force commander (JFC). Chapter V describes in detail the command relationships and command and control (C2) of joint forces.

8 Ibid., pp. x, I-5, and IV-4.

9 Joint Chiefs of Staff, JP 3-0, p. III-1.

10 Ibid., Appendix A.

11 Ibid., p. IV-1.

12 The following joint publications are available on the Joint Electronic Library: Joint Chiefs of Staff, JP 3-30, *Command and Control of Joint Air Operations*, Washington, DC: Joint Chiefs of Staff, February 10, 2014, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_30.pdf*; Joint Chiefs of Staff, JP 3-31, *Command and Control for Joint Land Operations*, Washington, DC: Joint Chiefs of Staff, February 24, 2014, p. GL-6, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_31.pdf*; Joint Chiefs of Staff, JP 3-32, *Command and Control for Joint Maritime Operations*, Washington, DC: Joint Chiefs of Staff, August 7, 2013, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32.pdf*.

13 Joint Chiefs of Staff, JP 3-31, p. GL-6.

14 Ibid., p. II-1.

15 Ibid. JP 3-31 Chapter IV describes the forms of land operations as well as the six joint functions that apply to them. The topics of the appendices are: Appendix A: Notional Headquarters Organization; Appendix B: Theater-Level Land Component Planning Considerations; and, Appendix C: Joint Land Operation Plan and Order Development.

16 Ibid., p. I-4.

17 Ibid., p. IV-10.

18 Ibid., pp. IV-10–V-11.

19 Ibid., p. II-3.

20 Ibid., p. I-3–I-4.

21 Ibid., p. IV-28.

22 Joint Chiefs of Staff, JP 3-14, *Space Operations*, Washington, DC: Joint Chiefs of Staff, May 29, 2013, p. G-1, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_14.pdf*.

23 DoD, *Department of Defense Key Officials 1947-2014*, Washington, DC: Historical Office, Office of the Secretary of Defense, June 2014, pp. 22, 106. USSPACECOM was disestablished on October 1, 2002.

24 Joint Chiefs of Staff, JP 3-14, p. I-1.

25 Ibid., p. I-1. See also DoD, *National Security Space Strategy: Unclassified Summary*, Washington, DC: Department of Defense and Office of the Director of National Intelligence, January 2011, p. 1. The description of space as "congested, contested, and competitive" first appeared in this document.

26 Ibid., p. I-8.

27 International Telecommunication Union (ITU), "About International Telecommunication Union (ITU)," n.d., available from *https://www.itu.int/en/about/Pages/default.aspx*. The website describes ITU as:

> **ITU is the United Nations [UNs] specialized agency for information and communication technologies—ICTs** [emphasis in original]**.**
>
> We allocate global radio spectrum and satellite orbits, develop the technical standards that ensure networks and technologies seamlessly interconnect, and strive to improve access to ICTs to underserved communities worldwide.
>
> ITU is **committed to connecting all the world's people**—wherever they live and whatever their means [emphasis in original]. Through our work, we protect and support everyone's fundamental right to communicate.

28 Joint Chiefs of Staff, JP 3-14, p. II-6.

29 Ibid., p. IV-3.

30 Ibid., pp. IV-4, IV-9.

31 Ibid., p. III-2. Per this joint publication, the space coordinating authority (SCA) roles and responsibilities are:

(1) Integrating space capabilities.

(2) Planning, coordinating, and synchronizing space operations in the operational area and ensuring inputs from the joint force staff and components are incorporated.

(3) Maintaining situational awareness of theater space operations, and coordinating with the CCMD [combatant command] SCA or Commander, JFCC SPACE [Joint Functional Component Commander for Space], to integrate theater space operations into DOD space operations.

(4) Providing consolidated space requirements through the JFC for coordination as required.

32 Ibid., pp. III-3-III-4. The joint publication's description of the space support elements (SSEs) follows:

The Army integrates space capabilities at the army, corps, division, special forces groups, and fires brigade levels using space support elements (SSEs). SSE organic space experts are resident on the headquarters . . . staff as an integral part of the staff and are directly involved in the staff planning process from the beginning. The element is responsible for identifying opportunities to employ space force enhancement or space control, and then coordinating the required support. When deployed, the SSE establishes and maintains contact with the SCA. It also coordinates with the SCA on procedures for space support requests and reachback support. The SSE participates in the conduct of mission analysis to determine which space-based capabilities are applicable to the particular operation and then coordinates and makes recommendations for the allocation and use of space services and capabilities. The mission analysis performed by the SSE forms the basis of the staff's space running estimate, as well as annex N (Space Operations), for all orders and plans.

33 Ibid., p. V-5. Challenges facing the space planner include:

Space presents unique planning and operational considerations that affect friendly, adversary, and neutral space forces alike. Space capabilities require extensive and advanced planning. Space assets are sufficiently capable and robust; however, operational planners must understand the limited number of resources available and the distinct challenges with space force reconstitution. Numerous resource and

legal considerations impact planning and affect mission success.

34 Ibid., pp. I-3–I-6.

35 Ibid., pp. A-1–G-8. The subjects of the seven appendices are: A: Space-Based Intelligence, Surveillance, and Reconnaissance; B: Missile Warning; C: Space-Based Environmental Monitoring Capability; D: Satellite Communications [SATCOM]; E: Space-Based Positioning, Navigation, and Timing; F: Operationally Responsive Space; and, G: Space Fundamentals.

36 Joint Chiefs of Staff, JP 3-12 (R), *Cyberspace Operations*, Washington, DC: Joint Chiefs of Staff, original release February 5, 2013, updated (unclassified) October 21, 2014, p. GL-4, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf*, accessed February 14, 2018.

37 DoD, *Quadrennial Defense Review Report*, Washington, DC: U.S. Government Printing Office, February 2010, p. 37.

38 DoD, *Department of Defense Strategy for Operating in Cyberspace*, Washington, DC: Department of Defense, July 2011, p. 37.

39 Joint Doctrine Analysis Division, *Compendium of Key Joint Doctrine Publications*, Washington, DC: Deputy Directorate, Joint Staff, J-7, January 3, 2014, p. iii.

40 Joint Chiefs of Staff, JP 3-12 (R), pp. v-vi and I-2–I-4 states that, "Cyberspace can be described in terms of three layers: physical network, logical network, and cyber-persona" and is summarized as:

> The **physical network** layer of cyberspace is comprised of the geographic component and the physical network components. It is the medium where the data travel. . . . The **logical network** layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network, i.e., the form or relationships are not tied to an individual, specific path, or node. A simple example is any Web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator. . . . The **cyber-persona** layer represents yet a higher level of

abstraction of the logical network in cyberspace; it uses the rules that apply in the logical network layer to develop a digital representation of an individual or entity identity in cyberspace. The cyber-persona layer consists of the people actually on the network [emphasis in original].

41 Ibid., p. vii.

42 Ibid., pp. II-2–II-5. JP 3-12 (R) distinguishes between cyberspace operations (CO) missions and cyberspace actions as follows:

e. **Cyberspace Actions**. While the JFC's military missions in cyberspace (OCO [offensive CO], DCO [defensive CO], and DODIN [DoD Information Network] operations) are categorized by intent, as described above, these missions will require the employment of various capabilities to create specific effects in cyberspace. To plan for, authorize, and assess these actions, it is important the JFC and staff understand how they are distinguished from one another.

Cyberspace actions include cyberspace defense, cyberspace intelligence, surveillance, and reconnaissance (ISR), cyberspace operational preparation of the environment [C-OPE], and cyberspace attack.

43 Ibid., pp. II-6–II-12.

44 Ibid., p. III-3. Figure III-1 of this publication summarizes the roles in cyberspace for six major sections of U.S. law as follows:

Title 6 . . . *Domestic Security* . . . [Role] Security of US cyberspace . . . Title 10 . . . *Armed Forces* . . .[Role] Man, train, and equip US forces for military operations in cyberspace . . . Title 18 *Crimes and Criminal Procedure* . . . [Role] Crime prevention, apprehension, and prosecution of criminals operating in cyberspace . . . Title 32 . . . *National Guard* . . . [Role] Domestic consequence management (if activated for federal service, the National Guard is integrated into Title 10 . . . [U.S. Code], *Armed Forces*) . . . Title 40, *Public Buildings, Property, and Works*, [Role] Establish and enforce standards for acquisition and security of information technologies . . . Title 50 . . . *War and National Defense* . . . [Role] Secure US interests by conducting military and foreign intelligence operations in cyberspace [emphasis in original].

45 Ibid., p. III-6. Cyberspace support element (CSE) deployed to CCMDs provide the following:

> CSEs are organized from USCYBERCOM forces and deployed to CCMDs for full integration into their staffs. CSEs resources are provided by USCYBERCOM to provide the CCMDs with joint CO planners and other subject matter experts on CO. These personnel facilitate development of cyberspace requirements and coordinate, integrate, and deconflict CO into the command's planning process.
>
> 1. The CSE provides CCMDs an interface and reachback capability to USCYBERCOM to synchronize cyberspace fires with the commander's scheme of maneuver, develop SA, and facilitate acquiring timely threat information.
>
> 2. USCYBERCOM retains operational control [OPCON] of the CSE, and the CSE is in direct support to the JCC [Joint Cyberspace Center].

46 Ibid., p. IV-1.

47 Ibid., p. IV-3. With regard to joint targeting, the publication notes that:

> However, three aspects of CO should be included in the JFC's targeting processes: recognizing that cyberspace capabilities are a viable option for engaging designated joint targets; understanding that a CO option may be preferable in some cases; and first, second, and third order effects on joint targets may involve or affect elements of the DODIN.

48 For a discussion of potential elements of a military cyberspace theory, including how the principles of joint operations apply to cyberspace, see Jeffrey L. Caton, "On the Theory of Cyberspace," in J. Boone Bartholomees, Jr., ed., *U.S. Army War College Guide to National Security Issues, Volume I: Theory of War and Strategy*, 5th Ed., Carlisle, PA: Strategic Studies Institute, U.S. Army War College, June 2012, pp. 325-343.

49 For the land domain, see Joint Chiefs of Staff, JP 3-31, pp. IV-1–IV-7. For the space domain, see Joint Chiefs of Staff, JP 3-14. In this publication, Chapter I includes a discussion of how the principles of joint operations apply to the space domain; Chapter

II addresses the Space Mission Areas. For the cyberspace domain, see Joint Chiefs of Staff, JP 3-12 (R).

50 Benjamin King, *Victory Starts Here: A Short 40-Year History of the US Army Training and Doctrine Command*, Fort Leavenworth, KS: Combat Studies Institute Press, May 2013, pp. 31-37, available from *https://usacac.army.mil/Cac2/cgsc/carl/download/csipubs/VictoryStartsHere_40yr.pdf*, accessed November 11, 2016.

51 Department of the Army, Army Doctrine Publication (ADP) No. 3-0, *Unified Land Operations*, Washington, DC: Headquarters, Department of the Army, October 2011, Foreword, available from *https://www.army.mil/e2/rv5_downloads/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf*, accessed February 13, 2018.

52 Ibid., p. iii.

53 Ibid., p. 2.

54 Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet 525-7-4, *The United States Army's Concept Capability Plan (CCP): Space Operations 2015-2024*, Version 1.0, Fort Monroe, VA: Training and Doctrine Command, Headquarters, Department of the Army, November 15, 2006, p. ii. The other imperatives of this CCP are:

- Facilitate the integration of space capabilities across the full spectrum of Army and joint operations.
- Improve the Army's ability to exploit existing space capabilities.
- Deliver space capabilities that address Army needs (capability requirements) and priorities by influencing the design of space-based systems and payloads.

55 Ibid., p. 15.

56 Ibid., p. 16.

57 Ibid., p. 37.

58 Headquarters, Department of the Army, Field Manual (FM) 3-14, *Army Space Operations*, Washington, DC: Department of the Army, August 2014. Although this document is unclassified, its distribution is limited to DoD and DoD contractors in

order to protect certain technical data. Thus, details of its contents are not included in this monograph.

59 For a detailed examination of Army space capabilities, see Jeffrey L. Caton, *Evolving Army Needs for Space-Based Support*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, April 2015. See also Institute of Land Warfare, *U.S. Army Space Capabilities: Enabling the Force of Decisive Action,* Torchbearer National Security Report, Arlington, VA: Association of the United States Army, May 2012, available from *https://www.ausa.org/sites/default/files/TBNSR-2012-US-Army-Space-Capabilities-Enabling-the-Force-of-Decisive-Action.pdf*.

60 Department of the Army, TRADOC Pamphlet 525-7-8, *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, Fort Monroe, VA: Training and Doctrine Command, Headquarters, Department of the Army, February 22, 2010, p. 16.

61 Ibid., pp. 15-18. The three dimensions of cyber electronic warfare (EW) and information operations (IO) are described as:

> (a) First dimension. The first dimension is the psychological contest of wills against implacable foes, warring factions, criminal groups, and potential adversaries. This dimension involves influencing desperate and creative people "to do what they really don't want to do" and requires an acute understanding of human behavior.
>
> (b) Second dimension. The second dimension is strategic engagement and involves keeping friends at home, gaining allies abroad, and generating support or empathy for the mission in the area of operations. This dimension includes the general public, key actors, and third party validators who are the ultimate arbiters of success or failure of military operations in the current operational environment. Gaining and maintaining their support or empathy for the mission is an imperative of 21st century operations.
>
> (c) Third dimension. The third dimension is the cyber-electromagnetic contest. Trends in wired, wireless, and optical technologies are setting conditions for the convergence

of computer and telecommunication networks. A significant advantage will go to the side that is able to gain, protect, and exploit advantages in the highly contested cyberspace and electromagnetic spectrums [EMS]. [Footnote for this paragraph: The use of the term cyber-electromagnetic is not meant to equate the terms cyberspace and EMS, but rather to highlight there is significant overlap between the two and future technological development is likely to increase this convergence.]

62 Ibid. Descriptions of the four elements of CyberOps include:

> CyberSA is the immediate knowledge of friendly, adversary and other relevant information regarding activities in and through cyberspace and the EMS [electromagnetic spectrum]. It is gained from a combination of intelligence and operational activity in cyberspace, the EMS, and in the other domains, both unilaterally and through collaboration with unified action and public-private partners. Discrimination between natural and manmade threats is a critical piece of this analysis. (p. 18)

> CyNetOps is the component of CyberOps that establishes, operates, manages, protects, defends, and commands and controls the LandWarNet, critical infrastructure and key resources (CIKR), and other specified cyberspace. CyNetOps consists of three core elements: Cyber enterprise management (CyEM), cyber content management (CyCM), and cyber defense (CyD), including information assurance, computer network defense (to include response actions), and critical infrastructure protection. CyNetOps uses CyEM, CyCM, and CyD in a mutually supporting and supported relationship with CyberWar and CyberSpt. (p. 19)

> CyberWar is the component of CyberOps that extends cyber power beyond the defensive boundaries of the GIG [global information grid] to detect, deter, deny, and defeat adversaries. CyberWar capabilities target computer and telecommunication networks and embedded processors and controllers in equipment, systems and infrastructure. CyberWar uses cyber exploitation (CyE), cyber attack (CyA), and dynamic cyber defense (DCyD) in a mutually supporting and supported relationship with CyNetOps and CyberSpt. (p. 21)

> CyberSpt is a diverse collection of supporting activities which are generated and employed to specifically enable both CyNetOps and CyberWar . . . These activities are called-out in this unifying category due to their unique and expensive nature as high-skilled, low-density, time-sensitive/intensive activities requiring specialized training, processes, and policy. Additionally, several of these activities also require specialized coordination, synchronization, and integration to address legal and operational considerations. It is because of these considerations and their overall importance that these activities are addressed as a CyberOps core component. (p. 22)

63 Department of Army, FM 3-38, *Cyber Electromagnetic Activities*, Washington, DC: Headquarters, Department of Army, February 2014, p. v. For additional background and history of the U.S. Army CO, see Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, January 2015.

64 Department of Army, FM 3-38, pp. 2-8–2-9. The full context of the Soldier's role in cyber electromagnetic activities (CEMA) is:

> Routine uses of cyberspace, such as sending e-mail, using the Internet to complete an online training course, and developing a briefing document, may occur in cyberspace, but they do not amount to what is defined as CO. However, it is through these routine uses of cyberspace that most of the vulnerabilities on U.S. networks are exposed to, and exploited by, adversaries. This includes communications that enter the EMS. By following accepted operations security procedures, every Soldier contributes to CEMA. Commanders, leaders, and non-commissioned officers educate Soldiers on threats in cyberspace and the EMS. Soldiers understand the relationship between cyberspace and the EMS and maintain the necessary protection measures when using devices that leverage this relationship between capabilities.

65 Ibid., p. 2-2.

66 Ibid., p. 2-7. With regard to CEMA coordination, FM 3-38 notes:

> The CEMA element collaborates internally with subordinate units and externally with supported, supporting, and adjacent units and centers. The CEMA element neither owns nor controls any of the unit's CO or EW assets, but it must coordinate with many who do. Therefore, CEMA staff personnel cannot support the element's mission by themselves. To plan, integrate, and synchronize successfully, the CEMA element, in coordination with the G-2 (S-2), collaborates via several means both internally to its unit and externally to its supporting units. The organization's knowledge management section can assist in establishing mechanisms to facilitate collaboration and reachback. (See table 2-1 on page 2-8.) [Note: table 2-1 is titled "Functions of the cyber electromagnetic activities working group."]

67 The new version of FM 3-12 was released 5 months after the research for this monograph was concluded. See Headquarters, Department of the Army, FM 3-12, *Cyberspace and Electronic Warfare Operations*, Washington, DC: Headquarters, Department of Army, April 11, 2017, available from *http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN3089_FM%203-12%20FINAL%20WEB%201.pdf*, accessed February 19, 2018.

68 U.S. Army War College, *Strategic Cyberspace Operations Guide*, Carlisle Barracks, PA: Center for Strategic Leadership, U.S. Army War College, June 1, 2016, available from *https://archive.org/details/USAWCStrategicCyberOpsGuide*, accessed November 14, 2016.

69 Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020*, Washington, DC: Joint Chiefs of Staff, September 10, 2012, p. 4. The elements of globally integrated operations are:

- Mission command
- Seize, retain and exploit the initiative
- Global agility
- Partnering
- Flexibility in establishing Joint Forces
- Cross-domain synergy
- Use of flexible, low-signature capabilities
- Increasingly discriminate to minimize unintended consequences

70 Ibid., p. 2.

71 Ibid., p. 7. The *Capstone Concept for Joint Operations* (CCJO) includes special operations, global strike, and ISR as part of flexible, low-signature or small-footprint capabilities.

72 Ibid., p. 5.

73 Ibid., p. 2.

74 Ibid., p. 7.

75 Joint Staff Joint Force Development (J7), *Cross-Domain Synergy in Joint Operations: Planner's Guide*, Washington, DC: Joint Chiefs of Staff, January 14, 2016, p. 1, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230*, accessed February 14, 2018.

76 Ibid., p. 1.

77 Ibid., Chapters 2 and 3.

78 Ibid., pp. 37-38. The text for Proposed Unique Characteristics and Capabilities in Table 2 are verbatim from this reference.

79 Ibid., p. 5. The *Planner's Guide* cites JP 1-02 as the source for its definition of space, but there is no definition of "space" in the current version (August 2017) of JP 1-02.

80 See Air Command and Staff College, Space Research Electives Seminars, *AU-18 Space Primer*, 2nd Ed., Maxwell Air Force Base, AL: Air Command and Staff College, September 2009. Chapter 3 addresses Current Space Law and Policy.

81 Joint Staff Joint Force Development (J7), pp. 46-47. The text for Proposed Unique Characteristics and Capabilities in Table 3 are verbatim from this reference.

82 Iulia-Diana Galeriu, "'Paper satellites' and the free use of outer space," New York: New York University School of Law, January/February 2015, available from *http://www.nyulawglobal.org/globalex/Paper_satellites_free_use_outer_space.html,* accessed February 14, 2018. This paper examines the claims by nations and commercial entities for specific space orbit positions:

Abstract: The International Telecommunication Union [herein after: ITU] is the United Nations [UNs] specialized agency for information and communications technologies, that allocates global radio spectrum and satellites orbits and develops the technical standards which ensure that networks and technologies seamlessly interconnect. [1] As the satellite industry is the most profitable space business at the moment, the demand for slots in the geostationary orbit [herein after: GSO] has been growing and the mandated institution to allocate these slots amongst States is the ITU. Due to the high value of the orbital positions and their scarcity, the GSO is slowly becoming saturated, despite the fact that many States have not yet placed a satellite into orbit due to technological or economic constrictions. This impairment of the States in their capability to participate has triggered a speculative phenomenon known as 'overfiling'. Overfiling consists of registering unneeded uses of orbit resources and has the effect of foreclosing others, who have near-term needs, from achieving access and conflict-free registrations. As a consequence of this practice, some States risk being denied their right to use outer space freely, a right which has been generally recognized in the international space legislation.

83 Joint Staff Joint Force Development (J7), p. 52. Table TIV-2 of the *Planner's Guide* is taken from Table 1 of Sean Brandes, "The Newest Warfighting Domain: Cyberspace," *Synesis: A Journal of Science, Technology, Ethics, and Policy*, Vol. 4, 2013, pp. G:90-G:95.

84 DoD, *Quadrennial Defense Review Report*, p. 37.

85 Department of Army, FM 3-38, p. 1-5. FM 3-38 lists the characteristics of the cyberspace domain as:

1-13. Cyberspace has characteristics that significantly differ from the land, air, maritime, and space domains. Cyberspace is a system of systems in that many small and diverse systems comprise the structure as a whole. These systems exist throughout each of the four natural domains. Changes in cyberspace are often driven by private industry research and development, making the domain dynamic and continually evolving as information technology capabilities continue to expand and evolve. Because cyberspace is man-made, it is only through continued attention and maintenance that cyberspace persists.

1-14. Cyberspace reinforces the fact that an operational framework is not confined to a physical place. Traditional battlefields were confined to physical space. While the repercussions of what happens on the traditional battlefield can create social and political effects around the world, the actual physical impact is limited to the physical battlefield. The inclusion of cyberspace and the EMS greatly expands and complicates the operational framework, transforming a limited physical battlefield to a global battlefield. A computer virus executed in cyberspace may strike its intended target and also indiscriminately strike other systems in several nations around the world, including the United States (U.S.). Collateral damage from this type of attack is not always predictable.

1-15. Cyberspace is an environment created and maintained for the purpose of facilitating the use and exploitation of information, human interaction, and intercommunication. This domain co-exists with the EMS through telecommunications systems. These systems utilize the EMS and have converged into a worldwide network to create cyberspace. Effective CO holistically address the physical infrastructure, data networks, and the EMS.

86 Ibid., p. 1-5.

87 Joint Staff Joint Force Development (J7), pp. 50-51. The text for Unique Characteristics and Capabilities in Table 4 are verbatim for this reference.

88 "Internet Traffic Report," continuously updating, available from *http://internettrafficreport.com/*, accessed November 28, 2016. This website "monitors the flow of data around the world. It then displays a value between zero and 100. Higher values indicate faster and more reliable connections." It also provides statistics on the average response times for information package to traverse servers in the continents of Asia, Australia, Europe, North America, and South America. These values varied between 39 to 137 milliseconds on the day of access for this endnote. For more discussion on physical factors in cyberspace, see Caton, in Bartholomees, Jr., ed., pp. 333-334.

89 U.S. Government Accountability Office (GAO), *United States Faces Challenges in Addressing Global Cybersecurity and*

Governance, GAO Report 10-606, Washington, DC: U.S. Government Accountability Office, July 2010. Figure 1 of this report, "U.S. Government Involvement in Key Entities and Efforts Addressing Global Cyberspace Security and Governance," includes 24 different fora with which U.S. Government departments participate (e.g., Departments of State, Defense, Homeland Security, Justice, and Commerce).

90 Joint Staff Joint Force Development (J7), The description of the three layers of cyberspace in the *Planner's Guide*—originally from Joint Chiefs of Staff, JP 3-12 (R)—is included on p. 52.

> The **physical layer** includes all hardware assets—computers, servers, routers, satellite links, etc.—enabling the movement of information in and through cyberspace. Related to the physical layer is cyberspace's reliance on the electromagnetic spectrum (EMS), where much of cyberspace's code moves and is, therefore, vulnerable to jamming or manipulation. The **logical layer** is the abstract portion of the physical layer. This layer reflects information represented and accessible in multiple locations through Internet Protocol and uniform resource locator (URLs). The **cyber-persona** layer is an extension of the logical layer and represents the users, entities, and organizations on the network. This layer applies the same rules that govern the logical layer [emphasis in original].

91 Joint Chiefs of Staff, JP 3-14, p. IV-2.

92 Department of Army, FM 3-38, pp. 1-4–1-5.

93 Joint Chiefs of Staff, JP 3-12 (R), p. I-2.

94 Joint Chiefs of Staff, JP 3-14, p. E-2.

95 Ibid., p. IV-18.

96 Ibid., p. E-1.

97 Department of Army, FM 3-38, p. 1-5.

98 Ibid., p. 2-7.

99 Joint Chiefs of Staff, JP 3-14, p. E-2.

100 Department of Army, FM 3-38, p. 2-7.

101 Joint Chiefs of Staff, JP 3-12 (R), p. I-2.

102 Joint Chiefs of Staff, JP 3-14, p. IV-18.

103 Department of Army, FM 3-38, pp. 1-4–1-5.

104 Joint Chiefs of Staff, JP 3-14, p. IV-18.

105 Department of Army, FM 3-38, p. 1-5.

106 Ibid., p. 3-3. FM 3-38 provides an example of CO support to opposing land commanders:

> For example, cyberspace capabilities and other information-related capabilities may be directed at an enemy weapons system consisting of the targeted platform and its operators. The cyberspace capability could create degrading effects on the platform while an information-related capability influences, disrupts, corrupts, or usurps the decisionmaking of the operator.

107 Joint Chiefs of Staff, JP 3-12 (R), p. I-2.

108 Joint Chiefs of Staff, JP 3-14, p. IV-18.

109 Department of Army, FM 3-38, p. 1-5.

110 Joint Chiefs of Staff, JP 3-12 (R), p. IV-12.

111 Ibid., p. II-1.

112 Department of the Army, ADP No. 3-0, p. 13. Mission Command is described as:

> 62. The mission command warfighting function develops and integrates those activities enabling a commander to balance the art of command and the science of control. This fundamental philosophy of command places people, rather than technology or systems, at the center. Under this philosophy, commanders drive the operations process through their activities of understand, visualize, describe, direct, lead, and assess.

113 For details, see Joint Chiefs of Staff, JP 3-14, p. B-2, Figure B-1 "Missile Warning and Support Request Procedures."

114 Department of Army, FM 3-38, p. 3-12. The Cyberspace Effects Request Form is described as follows:

> 3-50. The cyber effects request format is a format used to request effects in support of CO. The cyber effects request format contains baseline information for coordinating and integrating cyberspace capabilities and associated authorities to create effects outside and inside of the DODIN including LandWarNet. Commanders and staffs ensure cyber effects request formats are developed and submitted throughout the operations process to facilitate planning. Also, the cyber effects request format facilitates the achievement of operational and tactical objectives by leveraging the employment of cyberspace capabilities.

115 Chairman of the Joint Chiefs of Staff Instruction 3010.02D, *Guidance for Development and Implementation of Joint Concepts*, Washington, DC: Joint Chiefs of Staff, November 22, 2013, p. A-3.

> While concepts indirectly guide the other elements of force development, the relationship between concepts and doctrine is more direct: both concepts and doctrine focus on ideas for how the Joint Force should operate. As concepts gain institutional acceptance and requisite capabilities are developed, validated elements of the concepts may be incorporated in doctrine.

116 DoD, *Joint Operational Access Concept (JOAC)*, Version 1.0, Washington, DC: U.S. Department of Defense, January 17, 2012, Foreword, available from *https://www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf*, accessed November 3, 2016.

117 Ibid., Foreword.

118 Ibid., p. 12. The other two trends are "dramatic improvement and proliferation of weapons and other technologies capable of denying access to or freedom of action within an operational area" (p. 9) and "**the changing U.S. overseas defense posture** [emphasis in original]" resulting from decreased support abroad, severely contracting resources, and force protection.

119 Ibid., p. 12.

120 Ibid., p. 26.

121 Ibid., p. 27. The JOAC vision includes the use of traditional domain forces to support space and CO:

> Gaining space and cyberspace superiority when and where needed is not necessarily a symmetrical effort—that is, cyberspace operations [CO] to gain cyberspace superiority and space operations to gain space superiority—but often can be achieved more effectively, like superiority in the other domains, through the cross-domain application of combat power.

122 Ibid., p. 18. Operational Access Precept number 1, "Conduct operations to gain access based on the requirements of the broader mission, while also designing subsequent operations to lessen access challenges" considers a reduced use of land forces:

> Since operational access does not exist for its own sake, joint forces should conduct access operations in accordance with the broader objectives and ideally in conjunction with the other elements of national power. Importantly, a joint force commander [JFC] should avoid over-committing forces or projecting combat power deeper into hostile territory than is required by the objective. This is especially true of major land forces, which can be difficult to withdraw once committed.

123 Ibid., pp. 20-21.

124 Ibid., p. 22.

125 Ibid., pp. 19-20. Operational Access Precept number 3, "**Consider a variety of basing options** [emphasis in original]," includes use of space and cyberspace capabilities to help offset forward-based forces:

> One other option is to emphasize capabilities with minimal dependence on forward bases, such as amphibious, long-range strike, cyber, electronic, or space capabilities, either in primary or supporting roles.

126 Ibid., pp. 18-19. Operational Access Precept number 2, "**Prepare the operational area in advance to facilitate access**

[emphasis in original]," emphasizes the early use of operations in the space and cyberspace domains:

> Operations in space, cyberspace, and across the electromagnetic spectrum [EMS] likewise will be continuous to ensure that support to navigation, command and control [C2], targeting, sustainment, and intelligence are in place when needed. Moreover, computer network operations [NETOPS], both offensive and defensive, likely will commence long before lethal combat begins and even before combat forces begin to deploy.

Operational Access Precept number 5, "**Exploit advantages in one or more domains to disrupt enemy antiaccess/area-denial capabilities in others** [emphasis in original]," (pp. 21-22) also calls early space and CO:

> The decision on which domains to operate in initially will depend on the mission and the enemy's capabilities and vulnerabilities in the various domains; there is no universal sequence. That said, joint force projection almost always will include the early conduct of information operations [IO] and operations in space and cyberspace, since freedom of action in those latter domains is increasingly important to all joint operations. Moreover, those operations rarely require the additional risks incurred in deploying forces to the operational area. In fact, information, space, and cyberspace operations [CO] generally should commence well before the need for combat, as part of efforts to shape the operational area.

127 Ibid., p. 25. Operational Access Precept number 10, "**Maximize surprise through deception, stealth, and ambiguity to complicate enemy targeting** [emphasis in original]," includes:

> In the context of future opposed access, forms of deception that could prove especially useful include electromagnetic deception and cyber deception, which could provide intentionally erroneous information on the location and activities of deploying joint forces to enemy intelligence networks.

128 Joint Chiefs of Staff, *Joint Concept for Entry Operations*, Washington, DC: Joint Chiefs of Staff, April 7, 2014, p. iii, available

from *http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jceo.pdf?ver=2017-12-28-162000-837*, accessed February 13, 2018.

129 Ibid., p. vi. The purpose of the *Joint Concept for Entry Operations* (JCEO) is summarized in this passage as:

> The idea is to employ opportunistic, unpredictable maneuver, in and across multiple domains, in conjunction with the ability to attain local superiority at multiple entry points to gain entry and achieve desired objectives.

130 Ibid., p. vii.

131 Ibid., p. 6. The other six operational characteristics are:

- Purposes for entry operations
- Geographic and infrastructure challenges
- Capacity for entry operations
- Evolving threats
- Whole-of-government approach
- Multinational and coalition interface and interoperability

132 Ibid., pp. 11-12.

133 Ibid., pp. 12-13. Regarding the use of cyberspace and space to support military deception (MILDEC) operations against enemy forces, the JCEO includes:

> One method the Joint Force may use to confound the enemy is to create either a dearth or overabundance of targets for the enemy to process. Social media and other cyber-enabled deception methods may be valuable contributors to gaining surprise. Where surprise is not possible due to the nature of the operating area or the duration of the operation, the Joint Force will seek to overwhelm the enemy's targeting capability. This could be done, for example, through a combination of cyberspace efforts and the use of numerous autonomous decoys employed in one or more of the other domains.

Regarding the use of cyberspace and space support of MILDEC operation to reduce collateral damage, the JCEO states:

> Additionally, information operations, [IO] including those enabled by cyberspace employed in either a clandestine or overt manner, may be able to move populations away from potential points of entry in order to minimize collateral damage concerns.

134 Ibid., pp. 13, 15. With regard to joint fires, the JCEO suggests:

> In a hostile environment, fires will be mutually supporting across all domains to develop local superiority by suppressing threats to air and maritime operations. For example, information operations [IO], cyberspace, and space operations may be used to help a special operations unit to target, track, and conduct a direct action strike on an adversary's anti-ship system, permitting naval surface fires to engage enemy air defense assets. In turn, this engagement would allow global strike assets to eliminate key short range area denial assets that would otherwise impede the entry force.

135 Ibid., p. 20. The JCEO notes how maneuver is enhanced by space and cyberspace capabilities:

> Regardless of the type of maneuver, mobility and flexibility are critical and enhanced when fully integrated with cyberspace and space capabilities. Entry operations require the ability to build up capabilities as quickly as possible. Forces must be able to disperse to seize key terrain or for self-preservation, and to concentrate rapidly to exploit opportunity.

136 Joint Chiefs of Staff, *Joint Operating Environment, JOE 2035: The Joint Force in a Contested and Disordered World*, Washington, DC: Joint Chiefs of Staff, July 14, 2016, p. 7, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joe_2035_july16.pdf?ver=2017-12-28-162059-917*, accessed September 19, 2016. The *Joint Operating Environment* (JOE) suggests regional power trends that include:

> Emergence of new spacefaring nations and military competition in space. Many capabilities previously reserved to superpowers are now available to other states on a commercial basis, to include Earth observation, optical

sensing, space-based Internet, and communications services. A range of anti-satellite weapons (ASAT) able to disrupt or destroy the space, electromagnetic, and ground segments of these constellations will also become more common.

Growth of state-sponsored cyber forces and capabilities. The next decades will see the further emergence of state-sponsored actors and associated organizations with more advanced cyber warfare capabilities. Like strategic airpower before it, state-based cyber advocates will develop strategies that attempt to "leap over" traditional U.S. military forces and directly influence the decision calculations of political and military leadership.

137 Ibid., p. 17.

138 Ibid., pp. 21, 30-33.

139 Ibid., pp. 30, 33.

140 Ibid., pp. 32-33. *JOE 2035* predicts a potentially hostile space domain:

Competition in orbit (even during peacetime) will be intense, highlighted by satellites maneuvering to hinder the operations of other satellites, co-orbital jamming, and the use of ground-based lasers to dazzle or destroy imaging sensors. Future adversaries will also have the capability to deploy blockers and grapplers to impede the free operation of commercial and military satellites, and they will use ASAT weapons launched at space assets from the ground as well as from other satellites. Ultimately, this may generate space debris leading to a runaway chain reaction which destroys other satellites and threatens the integrity of many important orbits.

141 Ibid., p. 34.

142 Ibid., p. 35. The context of conflict in cyberspace includes:

A growing number of states will have extensive offensive cyber forces at their disposal to disrupt the smooth and efficient functioning of cyber-connected systems. In the future, state military and security organizations will increasingly use cross-border network and web-site

disruptions to cause social unrest. Attacks will work to undermine the trust and data integrity that are central to advanced societies, particularly financial, legal, and technical infrastructure. This competition may also feature strategic surveillance as well as industrial and scientific espionage.

143 Ibid., p. 36.

144 Ibid., pp. 40-50.

145 For additional reports on future security environments, see National Intelligence Council, *Global Trends 2030: Alternative Worlds*, Report NIC 2012-001, Washington, DC: Office of the Director of National Intelligence, available from *https://www.dni.gov/files/documents/GlobalTrends_2030.pdf*, accessed November 18, 2016. For additional views on the need for space and cyberspace capabilities to address increasing anti-access/area denial (A2/AD) challenges, see Jason D. Ellis, *Seizing the Initiative: Competitive Strategies and Modern U.S. Defense Policy*, Report LLNL-TR-680128, Livermore CA: Center for Global Security Research, Lawrence Livermore National Laboratory, January 2016, available from *https://cgsr.llnl.gov/content/assets/docs/J_Ellis_Seizing_the_Initiative_1_16.pdf*, accessed November 18, 2016. To explore challenges presented by China's increased military forces, see Peter Dombrowski, *America's Third Offset Strategy: New Military Technologies and Implications for the Asia Pacific*, Policy Report, Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, June 2015, available from *https://www.rsis.edu.sg/wp-content/uploads/2015/06/PR150608_Americas-Third-Offset-Strategy.pdf*, accessed November 18, 2016.

146 Mathew J. Burrrows, *Global Risks 2035: The Search for a New Normal*, Washington, DC: Atlantic Council, September 2016, available from *http://www.atlanticcouncil.org/publications/reports/global-risks-2035*, accessed October 6, 2016. The report is organized into nine chapters that address changing demographics, international governance, and technology advancement: Ch. 1. Individual Empowerment with More Unintended Consequences; Ch. 2. Growing Demographic Crunch for Everybody Except Sub-Saharan Africa; Ch. 3. A Malthusian World of Scarcities Increasingly Likely for the Poorest; Ch. 4. Technology with Downsides; Ch. 5. Conflict Risk Increasing; Ch. 6. Middles East: High Risk of Continuing Conflict; Ch. 7. China's linchpin in the Global Order;

Ch. 8. The Difficult Transition to a Post-Western Order; and, Ch. 9. The Big Picture.

147 Ibid., p. 40. Regarding a future contested space environment, the report projects that:

> The space powers will continue to develop quantitative and qualitative space-based missile attack early warning systems, intelligence, navigation, communications and broadcasting, and military command-and-control systems.
>
> The likelihood of space incidents (such as the collision of Russian and US satellites in 2009) might increase. Such incidents also include the possibility that authoritarian and irresponsible regimes will attempt to disrupt the operation of space systems, with unpredictable socioeconomic and military consequences.
>
> The only way to prevent an arms race in space would be to improve the legal basis for activity in outer space, particularly by expanding restrictions and bans on weapons deployment in orbit and development of land-, air-, and sea-based means of destroying objects in space.

148 Ibid., p. ii.

149 Ibid., p. 8. The original source of this information was cited as Atlantic Council, Frederick S. Pardee Center for International Futures, and Zurich, *Risk Nexus: Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures*, Washington, DC: Atlantic Council, September 2015, available from *http://publications.atlanticcouncil.org/cyberrisks//risk-nexus-september-2015-overcome-by-cyber-risks.pdf*, accessed November 4, 2016. The original reports consider this cost-benefit inflection to be an ongoing global phenomena:

> A future where the annual costs of being connected outweigh the benefits is not only possible, it is happening now. According to our project models, annual cybersecurity costs in high-income economies like the U.S. have already begun to outweigh the annual economic benefits arising from global connectivity.

> For all economies, the inversion of costs and benefits is expected to occur within the next five years. In Latin America, it is expected before the year 2030, as the region bridges the digital divide. In the Asia-Pacific region, the inversion is expected sometime after that. (p. 2)

150 Burrrows, p. 29.

151 Army Cyber Proponent, *The U.S. Army LandCyber White Paper 2018-2030*, Fort George G. Meade, MD: U.S. Army Cyber Command/2nd U.S. Army, September 9, 2013, p. 9, available from *http://dtic.mil/dtic/tr/fulltext/u2/a592724.pdf*, accessed November 6, 2013.

152 Ibid., p. viii. The foundation of the LandCyber concept includes:

Eight Aspects of Convergence:
1. Time and space
2. Threat and technology
3. Land and cyber domains
4. Cyberspace and electromagnetic spectrum [EMS]
5. Defensive and offensive cyber operations
6. Information environment and cyberspace domain
7. Information management and knowledge management
8. Operational and institutional

Nine Guiding Principles:
1. Unified cyberspace operations [CO]
2. Integration
3. Localized cyberspace effects to the tactical edge
4. Enhanced understanding
5. All networks are operational warfighting platforms and functions
6. Combined arms approach
7. Achieve cyberspace domain superiority
8. Ensure mission command
9. Empowered LandCyber units and Soldiers

153 Ibid., p. 4-6. Per the white paper, the following are the Army's roles and responsibilities in cyberspace as an operating force:

> (1) Support prevent, shape, and win roles with cyberspace capabilities. This requires supporting intelligence operations and conducting cyberspace operational preparation of the environment (OPE) [sic] to plan and prepare for military operations. Building, operating and defending all Army

networks as an end-to-end enterprise ensures its availability to the Army.

(2) Provide critical infrastructure protection for the Army and U.S. Northern Command national systems, and provide Army-wide indications and warning against threats and attacks.

(3) Integrate cyberspace operations [CO] capabilities into joint and Army planning and exercises, facilitate security cooperation to create defense in depth (under the direction of COCOMs [combatant command-command authority] and subject to the limitations of National Foreign Disclosure Policy), develop shared indications and warning, and leverage combined cyberspace operations [CO] strengths. Plan and integrate world-class cyber opposing forces (WCCO) in concert with USCYBERCOM and provide representative adversary command, control, and networked systems into training, testing, experiments, and exercises. This integration develops Army forces that can detect and respond to adversary cyber attacks and operate in a degraded cyberspace environment.

(4) Integrate cyberspace operations [CO] into combatant command [CCMD] planning and targeting processes to broaden the range of options. Deliver offensive and defensive cyber effects, if approved and directed, planned and integrated through cyber electromagnetic activities (CEMA). Conduct information operations (IO) in or through the cyberspace domain for the Army and support inform and influence activities (IIA) in or through the cyberspace domain.

154 Ibid., pp. 13-14.

155 Ibid., pp. 17-22.

156 The new version of FM 3-12 was released 5 months after the research for this monograph was concluded. See Headquarters, Department of the Army, FM 3-12.

157 Malcom Martin, "Cyber Support to Corps and Below – Concepts and Doctrine," briefing at the TechNet Augusta 2016 conference sponsored by the Armed Forces Communications

and Electronics Association, Fort Gordon, GA: U.S. Army Cyber Center of Excellence, August 2, 2016.

158 Joint Staff Joint Force Development (J7), p. 4.

159 The excerpts in Table 8 are verbatim from Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, pp. 8-12.

160 Ibid., p. 14. The CCJO addresses the practical realities of force development:

> The pursuit of advanced technology may prove unaffordable. This concept envisions Joint Forces enabled by advanced technologies in global communications, networked operations, space, cyberspace, robotics, platforms and lift. Such technologies, especially in a time of restricted budgets, may prove prohibitively expensive to develop and deploy.

161 See R. J. Vince, "Cross-Domain Deterrence Seminar Summary Notes," report LLNL-ABS-670206, Livermore CA: Center for Global Security Research, Lawrence Livermore National Laboratory, May 1, 2015, p. 2, available from *https://cgsr.llnl.gov/content/assets/docs/SummaryNotes.pdf*, accessed November 18, 2016. This report defines cross-domain deterrence as:

> The act of deterring an action in one domain with a threat in another domain, where the domains are defined as land, under the land, at sea, under the sea, in the air, in space, and in cyberspace, and may use economic sanctions and other diplomatic and political tools.

162 See John L. Rafferty, Jr., *LandCyber Operations: A Double Edged Sword or a Dream Team?* Strategy Research Project, Carlisle Barracks, PA: U.S. Army War College, March 2013, abstract, this Strategy Research Project explores the questions: "Will LandCyber enable micro-managing leaders to be the 'wet blanket' of mission command? Or will it open new doors for more effective maneuver and influence operations?"

163 Joint Chiefs of Staff, *JOE 2035*, pp. 17-20, 26-27. Regarding potential adversary use of autonomous systems, the JOE notes:

> The development of small, smart, cheap, autonomous, long-range, and highly-capable systems operating in the air, land,

> sea, and undersea environments may further complicate the homeland defense mission by providing relatively cheap strategic attack options to both state and non-state actors. (pp. 26-27)

164 See Jeffrey L. Caton, *Autonomous Weapon Systems: A Brief Survey of Development, Operational, Legal, and Ethical Issues*, Carlisle, PA: Strategic Studies Institute, U.S. Army War College, December 2015.

165 Joint Staff Joint Force Development (J7), pp. 46, 52. For details of the space and cyberspace references to EMS, see Tables 3 and 4 of this monograph.

166 Joint Chiefs of Staff, JP 3-12 (R), p. IV-9. An example of a potentially confusing interaction between cyberspace, space, EMS, and EA [electronic attack]:

> Planners should maintain awareness of the EMS and its impact on mobile devices and wireless networks, including cellular, wireless local area network, Global Positioning System, and other commercial and military uses of the EMS. CO and EA, to include offensive space control, must be deconflicted. Uncoordinated EA may significantly impact OCO utilizing the EMS. Depending upon power levels, the terrain in which they are used, and the nature of the system being targeted, unintended effects of EA can also occur outside of a local commander's AOR just as second order effects of CO may occur outside the AOR.

167 Sydney J. Freedberg, Jr., "DoD CIO Says Spectrum May Become Warfighting Domain," Breaking Defense, December 9, 2015, available from *https://breakingdefense.com/2015/12/dod-cio-says-spectrum-may-become-warfighting-domain/*, accessed October 28, 2016. The article includes the text of a statement by DoD Chief Information Officer (CIO) Terry Halvorsen:

> The Department understands that EMS Superiority is a crucial enabler to achieving superiority in all other domains and must be considered a prerequisite to all successful operations. In response to the pressing need to implement both the DoD EMS Strategy and JCEMSO [Joint Concept for Electromagnetic Spectrum Operations], the Department has taken steps that strive to establish policy and assign

> responsibilities to achieve EMS Superiority through efficient and effective Electromagnetic Spectrum Operations (EMSO), which will enable the optimization of EMS access and use/ maneuver throughout the full range of military operations, and defines EMSO as all spectrum dependent (SD) activities occurring within the EMS.
>
> As part of this guidance, the Department will investigate all requirements and ramifications of its enactment, to include the potential recognition of the EMS as a domain. As the EMS transcends all domains the Department must systematically evolve its capabilities to ensure effective EMS operations. As the Primary Staff Assistant (PSA) to the Secretary of Defense for spectrum, the Office of the DoD Chief Information Officer (CIO) will be the Departmental lead for these efforts in close cooperation and coordination with the all appropriate DoD Components.

Also, see Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, No. 2, Fall 2012, pp. 325-340, available from *https://www.rand.org/pubs/external_publications/EP51077.html*, accessed October 28, 2016. Libicki states that the argument for cyberspace as a domain should also apply to EMS. (p. 366)

168 DoD, JOAC, p. 7. The JOAC inaccurately asserts that "Advances in airpower and long-range weapons have mitigated the degrading effects of distance to some extent but have not eliminated them, while cyber capabilities are unaffected by distance."

169 For details on the concept of ultra-tactical operations, see Jeffrey L. Caton, "Complexity and Emergence in Ultra-Tactical Cyberspace Operations," in Karlis Podins, Jan Stinissen, and Markus Maybaum, eds., *Proceeding of 5th International Conference in Cyber Conflict*, Tallinn, Estonia: North Atlantic Treaty Organization Cooperative Cyber Defence Center of Excellence Publications, June 2013, pp. 299-312.

170 DoD, JOAC, p. 1.

171 Joint Chiefs of Staff, *JOE 2035*, p. 43. With regard to cyber resiliency, *JOE 2035* includes:

The future security environment will continue to feature a range of adversaries attempting to shape political behavior by conducting damaging or disruptive cyber-attacks. The Joint Force must minimize the consequences of threatened or successful cyberattacks against the United States, its allies, and partners by conducting Military Support to Cyber Resiliency. Furthermore, the Joint Force should develop the capacity to work with a range of nontraditional partners such as private companies or cyber activists to offset adversary operations in cyberspace, for example, by identifying and interdicting adversary cyber operatives.

ACRONYMS

A2/AD	anti-access/area denial
ADCON	administrative control
ADP	Army Doctrine Publication
AFCY	Air Forces Cyber Command
AOR	area of responsibility
ARCY	Army Cyber Command
ASAT	anti-satellite weapons
C2	command and control
CBRN	chemical, biological, radiological, and nuclear
CCDR	combatant commander
CCJO	Capstone Concept for Joint Operations
CCMD	combatant command
CCP	Concept Capability Plan
CDRUSSTRATCOM	Commander, U.S. Strategic Command
CEMA	cyber electromagnetic activities
CF	Conventional Forces
CIKR	critical infrastructure and key resources
CIO	chief information officer
CO	cyberspace operations
COCOM	combatant command-command authority
C-OPE	cyberspace operational preparation of the environment
CSE	cyberspace support element
CyEM	cyber enterprise management
DAL	defended asset list
DCO	defensive cyberspace operations or defensive CO
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNC	DISA network center

DoD	Department of Defense
DODIN	DoD Information Network
EA	electronic attack
EMP	electromagnetic pulse
EMS	electromagnetic spectrum
EMSO	electromagnetic spectrum operations
EW	electronic warfare
FLTCY	Fleet Cyber Command
FM	Field Manual
GAO	Government Accountability Office
GCC	geographic combatant commander
GIG	global information grid
GPS	global positioning system
GSO	geostationary orbit
HPRF	high-powered radio frequency
IADS	integrated air defense systems
IIA	inform and influence activities
IO	information operations
ISR	intelligence, surveillance, and reconnaissance
ITU	International Telecommunication Union
JCC	Joint Cyberspace Center
JCEMSO	Joint Concept for Electromagnetic Spectrum Operations
JCEO	Joint Concept for Entry Operations
JFC	joint force commander
JFCC SPACE	Joint Functional Component Commander for Space
JFLCC	joint force land component commander
JNCC	joint network operations control center
JOAC	Joint Operational Access Concept
JOE	Joint Operating Environment
JOPP	joint operation planning process

JP	Joint Publication
MAR4CY	Marine Corps Forces Cyberspace Command
MILDEC	military deception
MISO	military information support operations
NATO	North Atlantic Treaty Organization
NAVWAR	navigation warfare
NETOPS	network operations
NGA	National Geospatial-Intelligence Agency
NOSC	network operations and security center
NSA	National Security Agency
OCO	offensive CO
OE	operational environment
OPCON	operational control
OPE	operational preparation of the environment
PED	processing, exploitation, and dissemination
PNT	position-navigation-timing
PSA	primary staff assistant
SAM	surface-to-air missiles
SATCOM	satellite communications
SCA	space coordinating authority
SD	spectrum dependent
SOF	Special Operations Forces
SSE	space support element
STO	special technical operations
TACON	tactical control
TNC	theater network center
TNCC	theater network coordination center
TRADOC	Training and Doctrine Command
UCP	Unified Command Plan
UN	United Nations

USCYBERCOM	U.S. Cyber Command
USSPACECOM	U.S. Space Command
USSTRATCOM	U.S. Strategic Command
WCCO	world-class cyber opposing forces
WMD	weapons of mass destruction

APPENDIX I: SUMMARY OF SPACE- AND CYBERSPACE-RELATED EXCERPTS FROM JOINT PUBLICATION (JP) 3-31

JP 3-31 excerpts related to the space domain.
2. Joint Land Operations f. It is important to understand that in today's complex operational environment [OE], adversary actions can be delivered on, from, within, and outside of the operational area, all with potentially global impacts and influence. To negate those threats, commanders at all levels should consider how space, cyberspace, and EMS [electromagnetic spectrum] capabilities enhance the effectiveness and execution of joint land operations. Furthermore, joint staffs should seek out experts who and capabilities that can enhance the effectiveness of land operations.[1]
2. Roles and Responsibility u. Performing the duties of the space coordinating authority (SCA), if designated. The individual designated to be the JFLCC [joint force land component commander] may also be designated to be the SCA within a joint force to coordinate joint space operations and integrate space capabilities. The SCA has primary responsibility for joint space operations planning, to include ascertaining space requirements within the joint force. The SCA gathers operational requirements that may be satisfied by space capabilities and facilitates the use of established processes by joint force staffs to plan and conduct space operations.[2]
8. Command and Control [C2] f. **Space Capabilities for C2** (1) Space systems may be employed to monitor land areas before friendly forces are established. If the individual designated to be the JFLCC is also designated to be the SCA, he will normally designate a senior space officer who facilitates coordination, integration, and staffing activities for space operations on a daily basis. (2) Space systems provide **ISR [intelligence, surveillance, and reconnaissance]; missile tracking; launch detection; environmental monitoring; satellite communications [SATCOM]; position, navigation, and timing; and navigation warfare [NAVWAR]**. Considering the difficulties in communications in and around land areas, space systems offers the JFLCC the ability to exchange information inside the operational area, between elements of the joint force, and also facilitates intertheater and intratheater communications. Space systems may form a critical link in the C2 architecture that rapidly passes data and information. This can enable taskings and warnings to forces, as well as critical situational awareness and location information. Space systems face simultaneous demands from many users and require prioritization.

(3) The space-based **Global Positioning System (GPS)** provides a critical capability during joint land operations. GPS can provide position, location, and velocity for weapon accuracy, ingress and egress, location, silent rendezvous coordination, and improved personnel situational awareness. The ability of space systems to provide real time terrain information that, enhanced by imagery data, can be used by all components of the joint force is especially crucial to the success of ground forces.[3]

11. Movement and Manuever

c. The JFLCC makes recommendations to the JFC [joint force commander] on the following:

(9) Space support to the land force.[4]

Figure A-4. Notional Joint Force Land Component Operations Staff Directorate.[5]

JP 3-31 excerpts related to the cyberspace domain.

2. Joint Land Operations

a. In the 20th century, joint and multinational operations have encompassed the full diversity of air, land, maritime, and space forces operating throughout the operational area. Advances in capabilities among all forces and the ability to communicate over great distances have made the application of military power in the 21st century more dependent on the ability of commanders to synchronize and integrate **joint land operations** with other components' operations. Many of these advances have been realized through the use of cyberspace and the electromagnetic spectrum (EMS), which has enabled the US military and allies to communicate and reach across geographic and geopolitical boundaries. However, these advances have also led to increased vulnerabilities and a critical dependence on cyberspace and the EMS for the US and its allies.[6]

f. [see excerpt in space domain section above in this table.]

2. Roles and Responsibility

p. Integrating cyberspace operations (CO) into plans. Offensive cyberspace operations [OCO] will typically be conducted in direct support of the JFC. The JFLCC conducts defensive cyberspace operations (DCO) and DODIN [DoD Information Network] operations throughout all phases of the operation.[7]

Figure II-5. Joint Force Land Component Commander [JFLCC] Interface with Other Joint Force Command and Control [C2] Mechanisms [This figure includes the following information about CO].[8]

C2 Mechanism	Role/Function	JFLCC Interface
JFC's Joint Cyberspace Center [JCC]	Combines input from United States Cyber Command and combatant commands [CCMD] to provide a regional/functional cyberspace situation awareness/ common operational picture. Facilitates the coordination and deconfliction of combatant commander [CCDR] directed cyberspace operations [CO].	JFLCC's representative participates to provide/request cyberspace operations [CO] products.

11. Cross-Functional Staff Organizations

c. **Operations**

(4) The IO [information operations] cell and cyberspace support element [CSE] works with the JFLCC and key components of the JFLCC's staff to determine the cyberspace component of the JFLCC's defended asset list (DAL). Once the DAL has been determined, the IO cell and cyberspace support element [CSE] focuses available capabilities to safeguard DAL assets.[9]

14. Communications Support Systems

The CCDR, through the JFC and functional/service components, ensures effective, reliable, and secure communications system and cyberspace defense services are consistent with the overall joint campaign plan. As driven by the mission, the foundation of the communications system is laid by the C2 organization of forces assigned to the JFC.[10]

Figure III-1. Joint Force Land Component Commander [JFLCC] Joint Planning Group Representation.[11]

8. Command and Control [C2]

e. **Communications.**

(2) **Joint network operations (NETOPS) are the means by which communications are established and maintained throughout the DODIN. Commander, United States Strategic Command (CDRUSSTRATCOM)** is the supported commander for global CO to secure, operate, and defend DODIN. CDRUSSTRATCOM cyberspace efforts are coordinated by US Cyber Command who in turn coordinates with the GCC [geographic combatant commander] at the GCC's joint cyberspace center [JCC]. As the JFLCC's single control agency for the management and operational direction of the joint communications network, the joint network operations control center **(JNCC) must be knowledgeable concerning the requirements of communications in the land environment, especially in the specific operational area.** The JNCC should be aware of the capabilities present in the urban area, their potential use, and any problems associated with that use. Vital to communications management is the need to support planning and execution to include information exchange requirements, radio frequency spectrum allocation, communications equipment dispersion, and assessment of communications effectiveness.[12]

12. Protection

h. **DODIN Operations and DCO.** DODIN operations are operations to design, build, configure, secure, operate, maintain, and sustain DOD [Department of Defense] networks to create and preserve information assurance on the DODIN, and DCO are passive and active CO intended to preserve the ability to utilize friendly cyberspace capabilities and protect DOD data, networks, and capabilities and other designated systems.[13]

15. Cyberspace Operations [CO]

CO are conducted across the range of military operations and CO capabilities should be considered during JOPP [joint operation planning process], integrated into plans, and synchronized with other operations during execution. Commanders conduct CO to retain freedom of maneuver in cyberspace, accomplish objectives, deny freedom of action to adversaries, and enable other operational activities. The importance of CO support in all military operations has grown as the joint force increasingly relies on cyberspace for C2 and other critical operations and logistics functions.[14]

Figure A-4. Notional Joint Force Land Component Operations Staff Directorate.[15]

8. Communications Systems Staff Section

The J-6 staff coordinates voice, video, data, and message connectivity, cyberspace defense, and DODIN operations supporting JFLCC operations, and gives needed guidance to ensure synchronization between all components and/or subordinate commands. A notional J-6 staff organization is depicted in Figure A-7. The following actions are the responsibility of the J-6:

aa. Conducts information assurance and NETOPS as part of cyberspace defense support of JFLCC networks.

ee. Develops a list of critical cyberspace assets so that they can be properly protected to support JFLCC operations.[16]

5. Command and Control [C2]

b. Communications Systems (annex K). Communications and cyberspace defense procedures and priorities such as location of key nodes, spectrum management, communications-electronics operating instructions, codes, and interface with joint or multinational forces.[17]

ENDNOTES – APPENDIX I

1. Joint Chiefs of Staff, Joint Publication (JP) 3-31, *Command and Control for Joint Land Operations*, Washington, DC: Joint Chiefs of Staff, February 24, 2014, p. I-4, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_31.pdf.*

2. Ibid., p. II-3.

3. Ibid., pp. IV-10–IV-11.

4. Ibid., pp. IV-18–IV-19.

5. Ibid., p. A-5. The figure includes a Space Operations section aligned under J-33 Current Operations.

6. Ibid., pp. I-3–I-4.

7. Ibid., p. II-3.

8. Ibid., p. II-20.

9. Ibid., pp. II-17–II-21.

10. Ibid., p. II-25.

11. Ibid., p. III-6. The figure includes a Cyberspace representative for the Cyberspace Cell included in the J-5 planning group. It also includes an electromagnetic spectrum (EMS) representative for the EMS Cell as well as the J-39/ information operations (IO) Officer for the IO Cell.

12. Ibid., pp. IV-8–IV-10.

13. Ibid., pp. IV-20–IV-23.

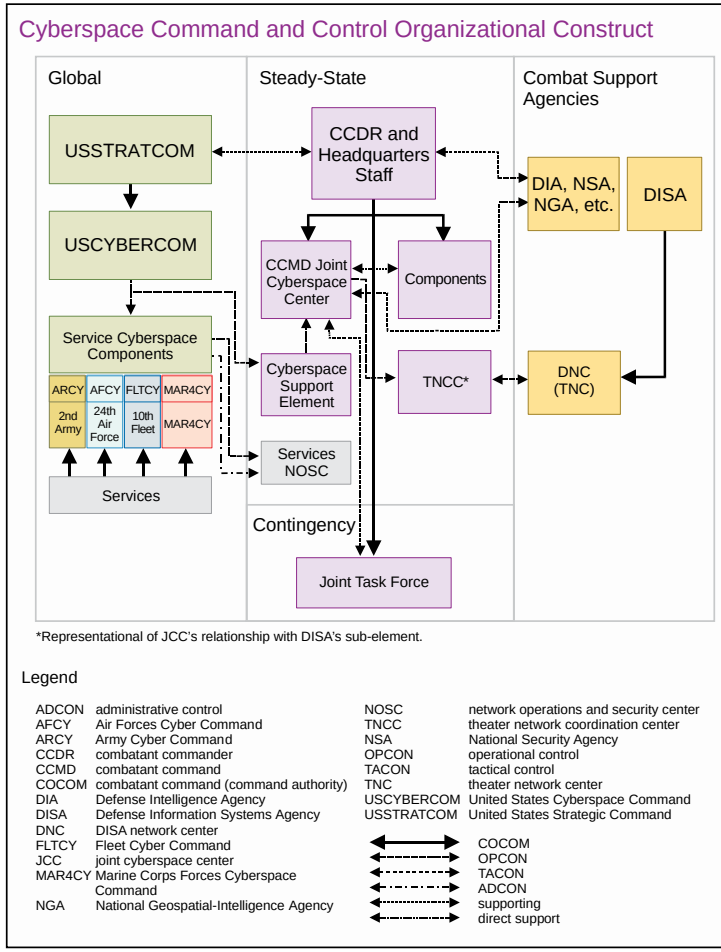
14. Ibid., p. IV-28.

15. The figure includes a Cyberspace Operations (CO) section that is aligned under J-33 Current Operations; Ibid., p. A-5.

16. Ibid., pp. A-9–A-11.

17. Ibid., pp. C-6–C-7.

APPENDIX II: CYBERSPACE COMMAND AND CONTROL ORGANIZATIONAL CONSTRUCT PER JOINT PUBLICATION 3-12 (R)[1]

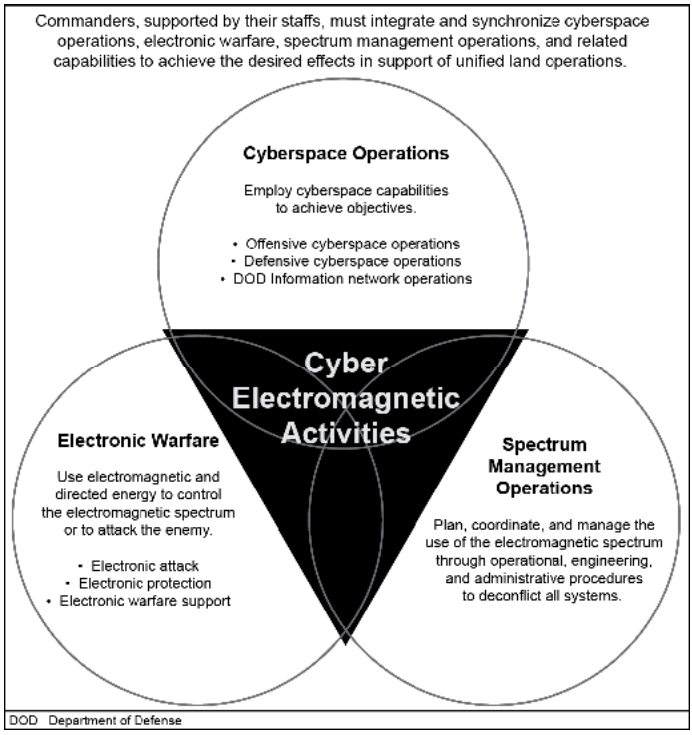


ENDNOTES – APPENDIX II

1. Image modified from "Figure IV-1. Cyberspace Command and Control Organization Construct," in Joint Chiefs of Staff, Joint Publication (JP) 3-12 (R), *Cyberspace Operations*, Washington, DC:

Joint Chiefs of Staff, original release February 5, 2013, updated (unclassified) October 21, 2014, p. IV-8, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf*, accessed February 14, 2018.

APPENDIX III: CYBER ELECTROMAGNETIC ACTIVITIES CONSTRUCT PER FIELD MANUAL 3-38[1]



ENDNOTES – APPENDIX III

1. Image from "Figure 1-1. Cyber electromagnetic activities," in Department of Army, Field Manual (FM) 3-38, *Cyber Electromagnetic Activities*, Washington, DC: Headquarters, Department of Army, February 2014, p. 1-2.

APPENDIX IV: SUMMARY OF SPACE- AND CYBERSPACE-RELATED FORCE DEVELOPMENT REQUIREMENTS FROM SELECTED JOINT CONCEPT DOCUMENTS

Excerpts from *Joint Operational Access Concept* (JOAC)[1]	
Command and Control [C2]	JOA-004. The ability to integrate cross-domain operations, to include at lower echelons, with the full integration of space and cyberspace operations [CO].
Intelligence	JOA-006. The ability of operational forces to detect and respond to hostile computer network attack in an opposed access situation.
Fires	JOA-011. The ability to conduct electronic attack [EA] and computer network attack against hostile antiaccess/area-denial [A2/AD] capabilities.
Movement and Maneuver	JOA-014. The ability to "maneuver" in cyberspace to gain entry into hostile digital networks.
Protection	JOA-022. The ability to protect friendly space forces while disrupting enemy space operations. JOA-023. The ability to conduct cyber defense in the context of opposed access.
Excerpts from *Joint Concept for Entry Operations* (JCEO)[2]	
Command and Control [C2]	Required Capability 3: The ability to command and control [C2] forces in austere or degraded environments, including communications, intelligence, cyberspace and space force enhancement degraded environments. b. Develop procedures for operating without some or all Space Force Enhancement capabilities (combat support operations and force multiplying capabilities delivered from space) or with degraded capabilities for extended periods. Space Force Enhancement capabilities may include ISR [intelligence, surveillance, and reconnaissance], launch detection, missile tracking, environmental monitoring, satellite communications (SATCOM), and position-navigation-timing capabilities (PNT).

	c. The ability to maintain operational access to key portions of the electro-magnetic spectrum during entry operations. d. Develop procedures for rapidly identifying, operating during, and recovering from significant cyberspace attacks. Effects of some attacks, such as denial of service, may be more obvious than others. f. The ability to provide operationally responsive space capabilities to augment or reconstitute existing space capabilities. Required Capability 4: The ability to execute effective and complementary Special Operations Forces (SOF) and Conventional Forces (CF) integration, where SOF or CF can be the supported force (depending on the nature of the entry operation). e. Consider expanding the integration and synchronization of space, cyberspace, and electronic warfare [EW] capabilities that CF and SOF units can leverage across the spectrum of operations.
Intelligence	Required Capability 7: The ability to provide Processing, Exploitation and Dissemination (PED) intelligence capabilities in degraded or austere environments during entry operations. a. Space-enhancement based and reachback PED capabilities must be able to support or be augmented in order to sufficiently meet entry operations' intelligence requirements en route, during initial entry, and even under degraded or austere conditions. b. When space-based and reachback support is interdicted, entry forces must be able to carry with themselves tailored PED capabilities sufficient to support intelligence requirements in such communications denied environments.

	c. Ensure all data dissemination methods and voice communications required by PED activities are sufficiently interoperable between services and allocated with sufficient redundancies to ensure continuation of data dissemination in contested environments, including loss of space-enhancement or reduced access to the electromagnetic spectrum [EMS].
Fires	Required Capability 10: The ability to continue to operate against A2/AD threats such as increasingly capable enemy subsurface and surface maritime threats, surface-to-air missiles (SAMs) and integrated air defense systems (IADS) capabilities, precision guided ballistic missiles, anti-ship cruise missiles, small boat swarms, landmines and maritime mines, complex obstacles, WMD [weapons of mass destruction] and related CBRN [chemical, biological, radiological, and nuclear] materials, and enemy aerial systems. c. The ability to deny an enemy's access to space. d. The ability to create denial effects within an enemy's networks. e. The ability to fully integrate offensive, reactive, and defensive cyberspace capabilities to protect and project force in support of entry operations. f. Ensure the joint force has the mechanism to employ appropriately delegated authority to use all non-kinetic fires assets, to include cyberspace capabilities.

ENDNOTES – APPENDIX IV

1. DoD, *Joint Operational Access Concept (JOAC)*, Version 1.0, Washington, DC: U.S. Department of Defense, January 17, 2012, pp. 33-35, available from *https://www.defense.gov/Portals/1/Documents/pubs/JOAC_Jan%202012_Signed.pdf*, accessed November 3, 2016.

2. Joint Chiefs of Staff, *Joint Concept for Entry Operations*, Washington, DC: Joint Chiefs of Staff, April 7, 2014, pp. 23-33, available from *http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jceo.pdf?ver=2017-12-28-162000-837*, accessed February 13, 2018.

U.S. ARMY WAR COLLEGE

Major General John S. Kem
Commandant

*****

STRATEGIC STUDIES INSTITUTE
AND
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Mr. Jeffrey L. Caton

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Denise J. Kersting

*****

Composition
Mrs. Jennifer E. Nevil

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
armywarcollege.edu

ISBN 1-58487-779-0

This Publication

SSI Website

USAWC Website