Joint Force Cyberspace Component Command: Establishing Cyberspace Operations Unity of Effort for the Joint Force Commander

A Monograph

by

MAJ Matthew Giovanni

United States Army

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2015-01

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 23-05-2015	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From - To)* JUN 2014 – MAY 2015

4. TITLE AND SUBTITLE Joint Force Cyberspace Component Command: Establishing Cyberspace Operations Unity of Effort for the Joint Force Commander	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) MAJ Matthew Giovanni	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301	**8. PERFORMING ORG REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Advanced Operational Arts Studies Fellowship, Advanced Military Studies Program	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Whether purposefully or out of sheer coincidence, cyberspace operations have chartered a course strikingly similar to that of air operations in history, theory, and doctrine. Both grew out of scientific innovation, theorists were quick to apply both of the new technologies to the art of warfare, and the doctrine for application of the military power associated with both of the new technologies evolved with scientific developments. However, the two have diverged as the United States military begins development of Cyber Mission Forces. As these forces grow and become available to a Joint Force Commander, he must establish a structure to unify the various offensive, defensive, and security operations in his cyberspace.

During Operation Desert Storm, the Commander United States Central Command unified air operations efforts through a Joint Force Air Component Command. This concept grew out of the experiences of the United States Air Forces beginning with the First World War and evolved with each subsequent application of air power. Current Cyberspace Operations doctrine lacks the guidance for achieving a unity of effort. Cyberspace theorists and doctrine writers would do well to continue to follow air power's historical example and develop a Joint Force Cyberspace Component Command to achieve unity of effort for Cyberspace Operations.

15. SUBJECT TERMS

Cyber; Cyberwar; Cyberspace Operations; Cyber Power development; Air Power development; Unity of Effort; Joint Force Cyberspace Component Command; Revolutions in Military Affairs;

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** MAJ Matthew Giovanni
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*

Monograph Approval Page

Name of Candidate: MAJ Matthew Giovanni

Monograph Title: Joint Force Cyberspace Component Command: Establishing Cyberspace Operations Unity of Effort for the Joint Force Commander

Approved by:

____, Monograph Director
Dan G. Cox, PhD

____, Seminar Leader
Michael D. Rayburn, COL

____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL

Accepted this 23rd day of May 2015 by:

____, Director, Graduate Degree Program
Robert F. Baumann, PhD

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

Abstract

Joint Force Cyberspace Component Command: Establishing Cyberspace Operations Unity of Effort for the Joint Force Commander, by MAJ Matthew Giovanni, 59 pages.

Whether purposefully or out of sheer coincidence, cyberspace operations have chartered a course strikingly similar to that of air operations in history, theory, and doctrine. Both grew out of scientific innovation, theorists were quick to apply both of the new technologies to the art of warfare, and the doctrine for application of the military power associated with both of the new technologies evolved with scientific developments. However, the two have diverged as the United States military begins development of Cyber Mission Forces. As these forces grow and become available to a Joint Force Commander, he must establish a structure to unify the various offensive, defensive, and security operations in his cyberspace.

During Operation Desert Storm, the Commander United States Central Command unified air operations efforts through a Joint Force Air Component Command. This concept grew out of the experiences of the United States Air Forces beginning with the First World War and evolved with each subsequent application of air power. Current Cyberspace Operations doctrine lacks the guidance for achieving a unity of effort. Cyberspace theorists and doctrine writers would do well to continue to follow air power’s historical example and develop a Joint Force Cyberspace Component Command to achieve unity of effort for Cyberspace Operations.

Contents

Acknowledgements……...………………………………………………….……………………v

Acronyms…………………………………………………………….………………………..vi

Introduction……………………………………………………………….……………………1

Development of Air Operations...……………………………………………………………..15

Development of Cyberspace Operations………………………………………………………45

Conclusion……………………………………………………………………………………..57

Bibliography…………………………………………………………………………….......60

Acknowledgements

To begin, I am deeply indebted to my family. Their love and support both energize and enable me to strive for excellence. I thank Colonel Michael Rayburn and my fellow Seminar 3 Majors who listened to my nonsensical ramblings and helped me arrange them into coherent thoughts. I hope to serve alongside of you again. Finally, I thank Dr. Dan Cox, “he’s kind of a big deal.” His patience and understanding empowered me to turn a random idea into a detailed analysis and ultimately this monograph. This process has truly been a lesson in learning and humility. I could not have accomplished it without everyone’s help. Thank you.

Acronyms

ACP	Army Campaign Plan
ADCON	Administrative Control
AOD	Air Operations Directive
APGM	Army Programming Guidance Memorandum
AR	Army Regulation
ARCIC	Army Capabilities Integration Center
ARPANET	Advanced Research Projects Agency Network
ATO	Air Tasking Order
CENTAF	United States Central Command Air Forces
CENTCOM	Unites States Central Command
CIO	Chief Information Officer
CMF	Cyber Mission Force
CMT	Combat Mission Team
COMAIRSOLS	Commander, Air Command Solomons
CPT	Cyber Protection Team
CSE	Cyber Support Element
CST	Combat Support Team
DHS	Department of Homeland Security
DoD	Department of Defense
DoDD	Department of Defense Directive
DODIN	Department of Defense Information Network
DOTMILPF-P	Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, Facilities, and Policy
GCC	Geographic Combatant Command
GHQ	General Headquarters

IT	Information Technology
JAOC	Joint Air Operations Center
JCC	Joint Cyber Center
JCIDS	Joint Capabilities Integration and Development System
JFACC	Joint Forces Air Component Command
JFC	Joint Force Commander
JFCCC	Joint Force Cyberspace Component Command
JFCC-NW	Joint Functional Component Command – Network Warfare
JP	Joint Publication
JTF-GNO	Joint Task Force-Global Network Operations
MAG	Marine Air Group
NATO	North Atlantic Treaty Organization
NMS	National Military Strategy
NMT	National Mission Team
NST	National Support Team
OPCON	Operational Control
QDR	Quadrennial Defense Review
RMA	Revolutions in Military Affairs
TAP	The Army Plan
TRADOC	Training and Doctrine Command
URL	Uniform Resource Locator
USCYBERCOM	United States Cyber Command
USSTRATCOM	United States Strategic Command

Introduction

Whether purposefully or out of sheer coincidence, cyberspace operations have chartered a course strikingly similar to that of air operations in history, theory, and doctrine. Both grew out of scientific innovation, theorists were quick to apply both of the new technologies to the art of warfare, and the doctrine for application of the military power associated with both of the new technologies evolved with scientific developments. However, the two have diverged as the United States military begins development of Cyber Mission Forces. As these forces grow and become available to a Joint Force Commander, he must establish a structure to unify the various offensive, defensive, and security operations in his cyberspace.

During Operation Desert Storm, the Commander United States Central Command unified air operations efforts through a Joint Force Air Component Command. This concept grew out of the experiences of United States Air Forces beginning with World War I and evolved with each subsequent application of air power. Current Cyberspace Operations doctrine lacks the guidance for achieving a unity of effort. Cyberspace theorists and doctrine writers would do well to continue to follow air power's historical example and develop a Joint Force Cyberspace Component Command to achieve unity of effort for Cyberspace Operations.

Literature Review

Revolutions in Military Affairs

Technological innovations and revolutions have changed the nature of conflict and warfare throughout history. Commonly referred to as revolutions in military affairs (RMA), these changes impact doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMILPF-P). Most scholars trace the origins of RMA to Soviet military theorists who, in the 1970s, identified fundamental changes in twentieth-century warfare. The Soviet concept on the matter however, was more limited than a RMA, as it was called a military-technical revolution; showing that the primary focus of Soviet theorists was on revolutions in military technology.[1] In their book *The Dynamics of Military Revolution, 1300-2050*, MacGregor Knox and Williamson Murray trace the origin to British historian Michael Roberts's 1955 lecture on military revolution and to the writings of Soviet military theorists from the 1960s onward.[2]

Scholars have identified ten revolutions in military affairs beginning in fourteenth-century England and occurring at sea, in the air, space, and most recently in the information environment today. Revolutions in military affairs occur when a group or nation combines technological innovation, with new organizational, doctrinal, and tactical concepts to attain a position of relative advantage over a competing organization. The lesser organization must then adapt similarly if they wish to remain a strategic peer. According to Steven Metz and James Kievit, "a revolution in military affairs dramatically increases combat effectiveness by four types of simultaneous and mutually supportive change: technological change; systems development; operational innovation; and, organizational adaptation."[3]

Revolutions in military affairs can be thought of similarly to Thomas Kuhn's paradigm shift. Scientific theories develop by accumulation until anomalies (in this case technological innovation) drive the development of new theories. Scientists test the old and new theories until forced to reject the old theory as no longer valid and accept the new.[4] Much like Kuhn's paradigm shift, Jeffrey Cooper's RMA process has five steps.

[1] Theodor W. Galdi, "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues," *Congressional Research Service Report for Congress*, Doc. 95-1170F, 11 December 1995, 3, accessed 30 August 2014, http://www.au.af.mil/au/awc/awcgate/crs/95-1170.htm.

[2] MacGregor Knox and Williamson Murray eds., *The Dynamics of Military Revolution, 1300-2050* (Cambridge, UK: Cambridge University Press, 2001), 1-2.

[3] Steven Metz and James Kievit, *Strategy and the Revolution in Military Affairs: From Theory to Policy* (Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College, 27 June 1995) accessed 30 August 2014, http://www.au.af.mil/au/awc/awcgate/ssi/stratrma.pdf.

[4] Thomas S. Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: The University of Chicago Press, 1962), 52-53.

> First, conditions must be right for the revolution to occur. The second step requires recognition that a revolution is in the making. Acceptance or validation of the revolution constitutes the third step. Understanding the problem and implications make up the fourth step. The fifth step involves active exploitation of the revolution and understanding its consequences.[5]

Another challenge with RMAs, as with any paradigm shift, is most true RMAs are only recognized after they have taken place.

Following the first gulf war and the 1993 publication of John Arquilla's and David Ronfeldt's monograph *Cyberwar is Coming!*, great effort and numerous studies have suggested how the United States and the Department of Defense should respond to the recent Cyber/Information Revolution and related RMA. Each study's approach to the RMA discussion greatly impacts his or her recommendations.

Theodor Galdi sums up the various RMA approaches best in his report to congress in 1995:

> A difficulty arises in understanding the current debate over the RMA because some participants use the term as referring to the revolutionary **technology itself** that is driving change, while others use the term as referring to revolutionary **adaptations** by military organizations that may be necessary to deal with the changes in technology or the geopolitical environment, and still others use the term to refer to the revolutionary **impact** of geopolitical or technological change **on the outcome** of military conflicts [emphasis his].[6]

Arquilla and Ronfeldt approached RMAs by way of the information revolution and its implications on organizational hierarchies and information as an economic and strategic target. In 1993, they wrote, "Information is becoming a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labor have been in the industrial age."[7]

[5] Jeffrey R. Cooper, "Another View of the Revolution in Military Affairs," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica: RAND Corporation, 1997), 120-121.

[6] Galdi, 4-5.

[7] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla and David Ronfeldt (Santa Monica: RAND Corporation, 1997), 25.

The proliferation of alleged industrial espionage news reports and charges by the Department of Justice support this assumption.[8]

In this same monograph, Arquilla and Ronfeldt presented two aspects of the nature of conflict involving information, or information warfare: Netwar and Cyberwar. "Netwar refers to information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around It … Netwars [can be] distinguished by their targeting of information and communications."[9] Netwar relates to both the global response to technical and information revolutions, and how people define and organize themselves in a constructivist sense.

"Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems."[10] Cyberwar may involve jamming radio transmissions, gaining access to and modifying global positioning systems, or gaining access to data systems to extract information or to disrupt information sharing on enemy networks. This presents significant implications to how nations conduct warfare resulting in a revolution in military affairs.

Since the beginning of the Global War on Terror, many have argued for the "death" of the RMA. In a 2010 article for Military Review, LTC (R) Scott Stephenson wrote of how the Pentagon in the middle 1990s and into the twenty-first century used the RMA as a rallying cry for

[8] Associated Press, "U.S. Files Economic Espionage Charges against Chinese Military Hackers," CBS News, 19 May 2014, accessed 29 December 2014, http://www.cbsnews.com/news/u-s-government-files-economic-espionage-charges-against-chinese-hackers-sources-say/. According to the article, "the hackers targeted big-name makers of nuclear and solar technology, stealing confidential business information, sensitive trade secrets and internal communications for competitive advantage." The article adds, "a recent government report said that more than 40 Pentagon weapons programs and nearly 30 other defense technologies have been compromised by cyber intrusions from China."

[9] Arquilla and Ronfeldt, 28.

[10] Ibid., 30.

military spending on weapons systems and restructuring organizations. "Today," Stephenson writes, "the rallying cry is dead. One would have difficulty in pinpointing the exact time and place of RMA's demise. However, with the beginning of a full-blown insurgency in Iraq in late 2003, the use of 'RMA' as a Pentagon mantra came to an abrupt end. The exact location of the phrase's collapse is open to speculation, but one place to look for it might be along Route Irish, between the Green Zone and the Baghdad International Airport."[11]

Yet, the emergence of Cyberpower has re-energized the RMA discussion. Writing in 2013, strategists such as Colin S. Gray, Martin C. Libicki, Paulo Shakarian, and Kamal Jabbour all argue cyberpower is another RMA. "Today, it is believed and IT-enabled RMA either has occurred or plainly is occurring in real time."[12] A review of the current national strategic guidance and recent Department of Defense force modernization and development efforts across the DOTMILPF-P support this claim.

Force Modernization and Development

Army Regulation (AR) 5-22*, The Army Force Modernization Proponent System,* describes how the Army manages transformation commonly driven by RMA. The vertical process culminates with final decisions by the Secretary of the Army. US Army Training and Doctrine Command (TRADOC), through the Army Capabilities Integration Center (ARCIC) and designated modernizations proponents, determines and integrates force requirements synchronizing the development across the Army.[13] The process of force modernization and

[11] Scott Stephenson, "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea," *Military Review* XC, no. 3 (May 2010): 38, accessed 30 September 2014. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20100630_art001.pdf.

[12] Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 21.

[13] Department of the Army, Army Regulation (AR) 5-22, *The Army Force Modernization Proponent System* (Washington DC: Government Printing Office, March 2011), 1-3.

development has its roots in the Joint Capabilities Integration and Development System (JCIDS) process for developing operational concepts to meet the future needs of the Joint force. This process begins with national strategic guidance such as the National Security Strategy, National Defense Strategy, National Military Strategy, and the Quadrennial Defense Review.[14]

The Army then develops The Army Plan (TAP), to include Army strategic planning guidance and planning priorities, the Army Programming Guidance Memorandum (APGM), and the Army Campaign Plan (ACP) along with a family of operational concepts designed to accomplish the Army mission. TRADOC assesses the future concepts through a series of analyses, tests, experiments, and studies to gain insights for solutions across DOTMLPF-P domains for emerging functional needs. Through this analysis, key capability requirements are refined and documented.

National Strategic Guidance on Cyber Security and Cyberspace Operations

Early national strategic documents concentrated on cyber security, the growing cyber threat, and highlighted the United States' increasing vulnerabilities. The 2008 National Defense Strategy focuses primarily on the risk presented by cyberspace related vulnerabilities. Additionally, it discusses the threats posed by violent extremists and nation-states developing cyber warfare capabilities. However, it does not offer a strategy to deter these growing threats. The 2010 National Security Strategy also highlights the importance of cybersecurity. "The capabilities that power our daily lives and military operations are vulnerable to disruption and attack."[15] It mentions cyberspace-based threats ranging from individual criminal hackers to advanced nation states. It identifies the nation's digital infrastructure as a strategic asset and

[14] Department of the Army, *2013-2014 How the Army Runs: A Senior Leader Reference Handbook* (Carlisle, PA: U.S. Army War College Press, 2013), 2-5.

[15] Barack Obama, *National Security Strategy of the United States, May 2010,* 8, accessed 4 September 2014, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

protecting it as a national security priority. Finally, it guides the accomplishment of this through a whole of government and industry approach while strengthening partnerships with global allies. Yet it too did not identify a structure to unite the whole of government approach.

The 2011 National Military Strategy (NMS) discusses several aspects of cyberspace and cyberspace operations across the topics of the strategic environment, deterring and defeating aggression, strengthening international and regional security, and shaping the future force. First, it covers the nature or character of the "globally connected "cyberspace domain as "increasingly challenged by both state and non-state actors," adding that our continued reliance on the cyberspace domain increases our vulnerability to "malicious actions." It notes the interlinked domains permit the "high-speed, high-volume exchange of ideas, goods, information, and capital." The 2011 NMS provided strategic guidance that "we must deter these threats while possessing the capability to fight through a degraded environment. Simultaneously we must improve our ability to attribute and defeat cyberspace attacks."[16]

The NMS continues to explain how joint assured access to cyberspace remains an enduring mission. Adhering to laws and regulations, our ability to operate effectively in cyberspace is tied directly to defeating aggression. In other words, cyberspace operations enable effective global warfighting. Chronologically, the NMS is the first to discuss broad command and control for cyberspace operations. It states, "Strategic Command and Cyber Command will collaborate with U.S. government agencies, non-government entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills."[17]

In terms of strengthening international and regional security, the NMS discusses our

[16] Chairman, Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011*: *Redefining America's Military Leadership,* (Washington, DC: Department of Defense, 2011), 3-9.

[17] NMS, 9-10.

response to a cyber-related incident, stating, "We will focus on rapidly providing planning, command and control, consequence management and logistic support."[18] In Europe, NATO will remain our primary partner in regional cyberspace security. In Asia and the Pacific, "we remain concerned about the extent and strategic intent of China's … assertiveness in cyberspace [within the region]."[19]

Regarding shaping the future force, the NMS seeks to achieve an appropriate balance of personnel (uniformed, civilian, and contract) operating in and supporting the cyberspace domain. Additionally, "Joint Forces must train and exercise in degraded air, sea, cyber and space environments."[20] It charges the joint force with the responsibility to ensure access, freedom of maneuver, and the ability to project power. To accomplish this in cyberspace joint forces will, "secure the '.mil' domain and improve our cyberspace capabilities"[21] in order to achieve cyberspace based effects.

The 2011 Department of Defense (DoD) Strategy for Operating in Cyberspace discusses the US and DoD reliance on cyberspace and the vulnerabilities that reliance presents, cybersecurity threats, and the importance of partnerships to protect cyberspace while respecting civil liberties. Identified as national strengths, the United States and DoD knowledge of cyberspace combined with the United States technical prowess and spirit of entrepreneurship provide us with a strategic advantage.[22] The Strategy highlights the character range of cyberspace threats (from state to non-state associated, from organized to individual, from internal

[18] NMS, 10-11.

[19] Ibid., 14.

[20] Ibid., 18.

[21] Ibid., 19.

[22] Department of Defense (DoD), *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: Government Printing Office, July 2011), 2.

to external, from economic to military) posed every day. The Strategy reflects the Department of Defense's concern for theft of or exploitation of data, disruption to or denial of services, and destruction or degradation of networks and systems. [23]

The 2011 Strategy lays out 5 strategic initiatives as a roadmap for cyberspace operations.

> 1: *Treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential.* "This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space to support national security interests." [24] Additionally, the first initiative briefly discusses DoD measures establishing mission command responsibilities regarding cyberspace and cyberspace operations. This paper will present those later in detail
>
> 2: *Employ new defense operating concepts to protect DoD networks and systems.* Recognizing the user as the first line of defense, the DoD plans to improve internal "cyber hygiene" practices. Additionally, the DoD will employ adaptive and dynamic network defense systems to improve externally focused defenses.[25]
>
> 3: *Partner with other U.S. government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.* Much of cyberspace and its associated physical domain fall outside the span of control and authority of the DoD. In order to effectively mitigate cyberspace risks the DoD will enhance its partnerships with the Department of Homeland Security, the Defense Industrial Base, along with other governmental agency and private sector entities.[26]
>
> 4: *Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.* Due to cyberspace's global nature, the DoD seeks to develop an international shared situational awareness to enable collective self-defense and increase deterrence.[27]
>
> 5: *Leverage the nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.* To capitalize on the United States' scientific, academic, and economic resources, the DoD will invest in recruiting, education, and training of the cyber workforce, and look to change the acquisition process to

[23] DoD *Strategy for Operating in Cyberspace*, 3.

[24] Ibid., 5.

[25] Ibid., 6-7.

[26] Ibid., 8-9.

[27] Ibid., 9-10.

keep pace with advancements in technology.[28]

Within the first initiative, the 2011 Strategy explains United States Strategic Command's (USSTRATCOM) role and responsibilities regarding cyberspace as well as the establishment of United States Cyber Command (USCYBERCOM) for synchronizing and coordinating Service components within each branch of the military.[29]

Published 7 December 2011, Joint Publication 3-12, *Cyberspace Operations,* provides joint guidance for the planning, execution, and assessment of cyberspace operations. It defines cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[30] It too highlights United States' reliance on cyberspace and the opportunities that reliance presents to adversaries. Uniquely, JP 3-12 discusses that "[p]ermanent global cyberspace superiority is likely not achievable. However, regional and local temporary cyberspace superiority may be attainable."[31] It advises commanders to use this temporary superiority to gain and retain the freedom of maneuver necessary to accomplish the commander's objectives. Additionally, JP 3-12 offers considerations commanders and staff must make in conducting cyberspace operations. These considerations include the need to synchronize and deconflict cyberspace operations with

[28] DoD *Strategy for Operating in Cyberspace*, 10-12.

[29] DoD *Strategy for Operating in Cyberspace*, 5. Specifically, the DoD Strategy for Operating in Cyberspace highlights USCYBERCOM's establishment as part of DoD's need to, manage cyberspace risk through efforts such as increased training, information assurance, greater situational awareness, and creating secure and resilient network environments; assure integrity and availability by engaging in smart partnerships, building collective self-defenses, and maintaining a common operating picture; and ensure the development of integrated capabilities by working closely with Combatant Commands, Services, Agencies, and the acquisition community to rapidly deliver and deploy innovative capabilities where they are needed the most.

[30] Department of Defense, Joint Publication (JP) 3-12, *Cyberspace Operations* (Washington DC: Government Printing Office, 7 December 2011), I-1.

[31] JP 3-12, I-2.

other theater operations, as well as deconfliction with other government entities and coalition partners.

JP 3-12 offers guidance on command and control of cyberspace operations suggesting adaptations in command and control structures to address the dual nature of cyberspace operations.[32] JP 3-12 identifies conditions when simultaneous cyberspace operations will be conducted under two separate but mutually supporting and supported chains of command. Noting that US Strategic Command, in conjunction with US Cyber Command, control global and trans-regional cyberspace operations, while cyberspace operations affecting only theater specific cyberspace falls under the control of that theater commander.[33] However, the aforementioned global nature of cyberspace limits the likelihood of these localized instances. When they do, the ability to prevent similar instances in other theaters raises the importance of sharing information globally and as immediately as possibly. This calls for a mechanism for the immediate sharing of information in order to maintain a common operational picture of cyberspace, as well as a structure for the command and control of any defensive cyberspace-based response action.

JP 3-12 identifies US Cyber Command as the authority to synchronize and direct trans-regional cyberspace operations. The Department of Defense (DoD) has three roles in cyberspace: defend the nation, national incident response (through support to civil authorities), and protect national critical infrastructure and key assets (in support of Department of Homeland Security (DHS) and other US Government departments and agencies).[34] Additionally, JP 3-12 lists the applicable Federal laws, legal and policy documents which authorize cyberspace operations.[35]

Plans and assessments related to cyberspace operations bear many similarities to the other

[32] JP 3-12, II-5.

[33] Ibid., II-5-6.

[34] Ibid., III-1-2.

[35] Ibid., III-2.

domains. However, planning for branches and sequels requires a full understanding of an adversary's cyberspace posture and capabilities. This includes not only the network infrastructure, but requires “profiles on system users and administrators, a clear understanding of what friendly forces or capabilities might be targeted and how, and an understanding of applicable domestic, foreign, and international laws and policy.”[36] While this should not change the fundamental planning process, it does highlight the need for planners with unique knowledge, skills and attributes and/or an assembled staff with the requisite knowledge, skills and attributes ready to plan such operations.

JP 3-12 highlights multiple times the importance of synchronization and deconfliction of cyberspace operations. Shared understanding or situational awareness forms the keystone to cyberspace operations planning. JP 3-12 charges planners to understand how operations in the physical domains impact cyberspace operations and vice versa. [37]

Department of Defense Directive (DoDD) 8500.01 *Cybersecurity*, dated 14 March 2014, gives the Department of Defense Chief Information Officer (DoD CIO) the lead for cybersecurity. Among other cybersecurity related responsibilities, the DoD CIO is authorized to: “monitor, evaluate, and provide advice to the Secretary of Defense regarding all DoD cybersecurity activities; and develop and establish DoD cybersecurity policy and guidance … in accordance with applicable federal law and regulations.”[38] Within DoDD 8500.01, the Director, Defense Information Systems Agency, is given the authority to develops, implement, and, in coordination with Commander, US Strategic Command (USSTRATCOM), manage cybersecurity for the Defense Information Systems Network.[39]

[36] JP 3-12, IV-2.

[37] Ibid., IV-9.

[38] Department of Defense, *Department of Defense Directive 8500.01, Cybersecurity* (Washington, DC: Department of Defense, 14 March 2014) 14.

Under the Unified Command Plan, USSTRATCOM is charged to coordinate and direct DoD information network operations and defense.[40] Since its establishment as a sub-unified command that is subordinate to USSTRATCOM, USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.[41]

The 2014 Quadrennial Defense Review (QDR) discusses the evolution of modern warfare and the increasingly contested nature of cyberspace. It highlights that US dependence on cyberspace presents an attractive target to adversaries, and the diverse range of those adversaries. In response to the growing cyber threats, the QDR continues to place a priority on cyber defense and capabilities. Of the national strategic documents guiding cyber strategy, it is the first to present response actions the Department of Defense will take, "The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten US interests."[42]

Later, the QDR links the US ability to project power to gaining, extending, and exploiting advantages in cyberspace. To accomplish this, the QDR provides guidance in the development of the Cyber Mission Force, and the migration of multiple Defense information systems to a

[39] DODD 8500.01, 16.

[40] Andrew Feickert, *The Unified Command Plan and Combatant Commands: Background and Issues for Congress Specialist in Military Ground Forces* (Washington, DC: Congressional Research Service, 3 January, 2013), 22, accessed 1 November 2014, http://fas.org/sgp/crs/natsec/R42077.pdf.

[41] "Mission," United States Cyber Command, accessed 1 November 2014, https://www.cybercom.mil/default.aspx.

[42] Department of Defense, *Quadrennial Defense Review* (Washington, DC: Government Printing Office, 2014), 14.

common, Defense-wide network infrastructure. The chapter on the planned US force structure FY2019 breaks down the Cyber Mission Force as follows:

> 13 National Mission Teams (NMTs) with 8 National Support Teams (NSTs)
> 27 Combat Mission Teams (CMTs) with 17 Combat Support Teams (CSTs)
> 18 National Cyber Protection Teams (CPTs)
> 24 Service CPTs
> 26 Combatant Command and DOD Information Network CPTs[43]

The QDR does not, however, place these forces into their respective service components, identify or recommend a command and control structure. If the Department of Defense expects to have one-hundred thirty-three various teams operating within the cyberspace domain it is imperative Joint Force Commanders establish a command and control structure to unify the efforts.

[43] QDR, 41. According to the Department of Defense website for the Cyber Domain Security and Operations, by 2016 the Cyber Mission Force will consist of 133 teams and 6000 people. Accessed 30 December 2014, http://www.defense.gov/home/features/2013/0713_cyberdomain/.

Development of Air Operations

Although the concept of militarizing the skies began well before the Wright Brothers' 17 December 1903 flight, air power theory took its great leap forward with the first heavier-than-air flying machine.[44] Air Vice Marshal R. A. Mason wrote of military aviation theorists envisioning air power as a concept similar to "command of the sea," translating it to "command of the air."[45] The first to utter this concept, according to David MacIsaac, was British Royal Engineer Major J. D. Fullerton in 1893. MacIsaac traces Major Fullerton's comments to a conference of military experts at Chicago's World Columbian Exposition of 1893. According to him, Fullerton spoke of a "revolution in the art of war where the chief work will be done in the air, and the arrival of the aerial fleet over the enemy's capital will probably conclude the campaign."[46] Building upon this comment, future air power theorists would apply this new technology to Clausewitz's theory of war suggesting military aviation would be the force applied "to compel our enemy to do our will."[47]

For nearly forty years, beginning in 1907, the debate over United States military air power and the call for a separate military air service branch raged. The debate hinged on two issues: command and control of air operations, and the purpose for air operations – better defined

[44] Andrew G. B. Vallance, *The Air Weapon: Doctrines of Air Power Strategy and Operational Art* (New York: St. Martin's Press, 1996), 1-2. Vallance highlights the invention and use of the hot-air and later the hydrogen-filled balloons. He points to France in 1793 as the first state to form a balloon detachment in their army, and their use at the Battle of Fleurus in 1794 against the Austrians as the first use of military air power.

[45] R. A. Mason, "War in the Third Dimension: Continuity, Innovation and Convergence," in *War in the Third Dimension: Essays in Contemporary Air Power*, ed. R. A. Mason (London: Brassey's Defence Publishers, 1986), 2.

[46] David MacIsaac, "Voices from the Central Blue: The Air Power Theorists," in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 627.

[47] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1984), 75.

as air power theory. The earliest prevailing Army theory viewed military aviation as another means for communications and reconnaissance. The Army therefore organized its aviation section as part of the general service of information and thus established the Aviation section of the Signal Corps in August 1907.[48] Despite congressional efforts to make a separate Army Air Corps in 1913, the prevailing opinion regarding the use of military aviation, to include the opinion of Army aviator, remained rooted in information related operations.[49]

The experiences of World War One showed military aviators the possibilities of a different kind of air war.   As a result, they began to think in terms of air power. During World War One, as Air Service Commander, First Army, reporting directly to General Pershing, General William "Billy" Mitchell exercised centralized control over air operations. In this capacity, Mitchell apportioned and assigned the various air operations of tactical aviation (air support to ground operations), counter-air to achieve air supremacy, reconnaissance, and bombardment.[50] He employed allied air power to great success in the battles of St. Mihiel and the Meuse-Argonne.[51] Mitchell applied air power against enemy airdromes, rail stations, supply depots and

[48] Thomas H. Greer, *The Development of Air Doctrine in the Army Air Arm, 1917-1941* (Maxwell Air force Base: USAF Historical Division, Research Studies Institute, Air University, 1955), 1. Greer notes his study was based primarily on official Air Force records and interviews with officers of the air arm who have been especially associated with air doctrine. Because of his exhaustive use of primary sources, this paper uses his work as the leading source for the early development of air power.

[49] Ibid., 1-2. In February 1913, the Chairman of the House Committee on Military Affairs, Representative James Hay, proposed a bill to create a separate Army Air Corps not subordinate to the Chief of Signal. Greer mentions that legislative hearing and correspondence relating to the bill showed most military men, including flyers, were opposed to it at the time. Greer adds that future air power leaders such as Benny Foulois, Hap Arnold, and Billy Mitchell felt it was too early for a separate Air Corps, the Signal Corps was doing all it could for aviation, and the creation of a separate branch would retard air reconnaissance development.

[50] Ibid., 5.

[51] Ibid., 5-6. According to Greer, Mitchell's air forces in sum consisted of 1,500 various types of French, British, Italian, and American aircraft brought under his direction for observation, artillery, pursuit, day and night bombardment, and reconnaissance. The plan assigned only what was needed for specific operations and placed the remainder in a central mass

communications centers as well as enemy ground elements.[52]

From this experience, Mitchell developed his theory that, “available air units should be placed under the control of an Air Service commander.”[53] Foreshadowing today’s Joint Air Operations Plan and the Air Tasking Order, Mitchell advocated an air operations plan coordinated with the Army operations and intelligence staffs then submitted to the commanding general for approval. Once approved, the plan served as a guide to subordinate aviation units and put into effect through field orders.[54] Additionally, Mitchell extolled the flexibility of air power due to its unique characteristics of speed and depth. In order to exploit these characteristics he and other air power theorists began to advocate for centralized control of aviation by air officers.[55]

The post-World War One attitude toward war in general had a profound impact on the development of air power theory and the continued debate on command and control of air operations. Theorists such as Guilio Douhet and Mitchell published and debated theories on strategic bombing and the ability to win wars through air power alone.[56] However, the atrocities of civilian casualties that resulted from Allied and Central powers’ bombardment of population centers led to a social rejection of strategic bombing. This attitude prompted Secretary of War

assigned to counter-air action until air supremacy was obtained. In both the battles of St. Mihiel and the Meuse-Argonne, Mitchell concentrated the mass of air power on the main axis of ground advance.

[52] Greer, 6.

[53] Ibid.

[54] Ibid. Greer cites William Mitchell, *Tactical Application of Military Aeronautics*, 5 January 1919.

[55] Ibid., 7.

[56] Greer, 16-17; John Shy, “Jomini,” in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 182; David MacIsaac, “Voices from the Central Blue: The Air Power Theorists,” in *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, ed. Peter Paret (Princeton, NJ: Princeton University Press, 1986), 630-631.

Newton Baker to declare, "there was no place for strategic bombardment in modern war."[57] In light of this, Army Air Service leadership adopted a doctrine placing the Air Service in support of ground operations.[58]

The debate for a separate Air Force continued as congress commissioned and the Secretary of War directed studies for the creation of a separate air arm. In his 2013 monograph, Colonel Eric Denny highlights these in his recounting of the Air Force's road to a separate branch of service.[59] Denny highlights the Curry bill, Lampert Commission, and Crowell Mission where each recommended a unified independent aviation branch juxtaposed with the Menoher Board, the Dickman Board, and the Morrow Board that each countered the other studies' findings. Despite the Army Reorganization Act of 1920 that made the Air Service a regular combatant arm, the debate continued until the creation of the Army Air Corps in 1926.[60]

The debate over the purpose of air operations at this time reached an agreement due to a lack of technology to support the theorists' claims. Without long-range bombers, regardless of the social rejection of strategic bombing, military aviation remained in a supporting role. "The attack of enemy field forces was the chief object once air control had been attained."[61]

The years 1926 through 1935 witnessed significant advances in aircraft technology and command of air operations. The successful 1935 test of Boeing's XB-17 provided air power

[57] Greer, 15. Greer cites the *Annual Report of the Secretary of War to the President, 1919,* for Secretary of War Baker's comments.

[58] Ibid., 15-16. Greer highlights a tentative service manual prepared in 1919 that declared it was the mission of the Air Service and all other arms to aid the infantry, and the 1923 Training Regulation 10-5 that stated all air action was auxiliary to the ground battle.

[59] Eric J. Denny, "The Cyberspace Domain: Path to a New Service?" (Monograph, Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies, 2013), 85-88. In his Appendix D, Denny summarizes the story of the Air Force's toad to a separate branch of service.

[60] Denny, 88.

[61] Greer, 32. Greer cites his 1952 interview of General J. T. McNarney (Retired) and a letter from General George C. Kenney from the same year.

theorists and planners with the airplane of their dreams.[62] The dominant thought emanating from the Air Corps Tactical School at this same time regarded the offensive employment of air power in massed air attacks upon the enemy's vital centers.[63] This placed increasing emphasis on the bomber as the key element and principle arm of the air forces, and unified control of those forces to mass air power at the decisive point. The official 1934-1935 Air Corps Tactical School text stated that:

> In order to secure the advantages which accrue from the radius of action and flexibility of an air force, it should be assigned and employed by no lesser commander than he who has the ultimate outcome at stake. Insofar as the field forces are concerned no commander less than the General Headquarters commander has this responsibility.[64]

Additional reports released at this time supported the establishment of a General Headquarters (GHQ) air force to unify current efforts and prepare for greater freedom of action necessary as aircraft capabilities increased.[65]

The 1935 creation of the GHQ Air Force gave its commander operational control of tactical units.[66] However, Training Regulation 440-15 retained command for the employment of air forces with the "territorial or tactical command to which it was assigned."[67] This sounds

[62] Greer, 46-47. In August 1935, the Boeing XB-17 flew from Seattle to Dayton. It weighed 35,000 pounds, could carry 2,500 pounds, and range 2,260 miles, with a maximum capacity of 5,000 pounds at 1,700 miles.

[63] Ibid., 50. Greer cites William Mitchell, *Skyways* (Philadelphia, 1930).

[64] Ibid., 54. Greer cites ACTS, Air Force, 1934-1935, p. 6, in USAFHD 4775-30.

[65] Ibid., 73. The reports mentioned include the 1933 Drum report which favored the establishment of a standing GHQ air force as a best-practice for employment of the Air Corps, the 1934 Baker Board which recommended establishment of a GHQ air force made of all air combat units trained as a homogeneous force and capable of either close support or independent action, and the 1935 Howell Commission report which recommended a GHQ air force as a step in the right direction. This final report predicted that as aircraft capabilities increased, progressively greater freedom of action would have to be granted the air arm.

[66] Greer, 73; Herman S. Wolk, *Toward Independence: The Emergence of the U.S. Air Force 1945-1947* (Washington DC: Air Force History and Museums Program, 1996), 3.

roughly similar to today's concept of Joint Force Commander exercising centralized control over assigned and attached air forces through his air component commander. In 1939, to unite air forces efforts, the Chief of the Air Corps was given jurisdiction over both the GHQ Air Force and Office of Chief of the Air Corps.[68] Regardless of the new structure, the debate continued over the role of air power: strategic versus tactical.[69]

The ultimate decision on the role of air power came from President Roosevelt following the Munich Conference in 1938. According to Greer, Roosevelt saw air power as the most likely to influence Hitler's activities. Therefore, "Roosevelt called for an immediate move toward mass production."[70] In support of his decision, in January 1939, Roosevelt sent a special request to Congress to fund aircraft with increased range, speed, and capacity.[71]

Prior to entering World War Two, the 1940 publication of Army Field Manual 1-5, *Employment of Aviation of the Army,* sought to settle the debate over command and control of tactical aviation.[72] According to the manual, four kinds of forces would be drawn from GHQ Air Forces aviation for the conduct of offensive and defensive air operations: striking forces, defense

[67] Greer, 74; Wolk, 3. Greer cites Training Regulation 440-15, *Employment of the Air Forces of the Army*, 15 October 1935, p. 5, in 062.12 (8-27-30), in National Archives, Central Decimal File, AGO, 1916-1939. Wolk adds that with the creation of the GHQ Air Force, the air units that previously reported to the area Army Corps commander in which they were assigned now reported to the Commander, GHQ Air Force. The Air Corps Chief, still not an operational commander, remained responsible to man, train, and equip the Army Air Forces.

[68] Greer, 106.

[69] Ibid., 95. The GHQ Air Force picked up the debate with the Army General Staff. While the General Staff saw the Air Forces role as tactical support of ground troops, the GHQ Air Force continued to develop strategic capabilities.

[70] Ibid., 100. Greer states Roosevelt wanted to see a rate of output of 10,000 planes per year, with an all-out capacity for 20,000 and indicated a special need for long-range aircraft.

[71] Ibid., 101. Greer cites Message to Congress, 12 January 1939, in The Public Papers and Addresses of F. D. Roosevelt (New York, 1941), 1939 vol., pp. 71-72.

[72] Ibid., 113-115.

forces, support forces, and Special Forces. The manual commented that the groupings overlapped and mutually supported one another. Further, GHQ would develop functional forces to be attached to territorial or tactical commands for the accomplishment of specified missions. The senior air officer would command the air units who received mission assignments from the higher commander.[73]

The Navy largely stayed out of the internal Army aviation debate except to reject the call for an independent Air Force. Similar to early Army aviation, the Navy saw aviation as a means for reconnaissance and communication, and later as an offensive arm to protect the fleet and sea lines of communication.[74] With the evolution of technology and the advent of aerial bombardment in the conduct of warfare, the Navy created the US Naval Aviation Service in March 1911.[75] As the First World War raged, the US Naval Commander-in-Chief in Europe, Admiral William S. Sims requested naval aviation to support defeat of German U-boats.[76]

Following World War One, the new chief of Naval Aviation, Admiral William A. Moffett, began the push for aircraft carriers. Naval historian Wilbur Morrison quotes Admiral Moffett as saying, “We must put planes on battleships and get aircraft carriers quickly. The safety of ships in the next war will depend to a great measure on aviation.”[77] With differing view of employment

[73] Greer, 115.

[74] Greer, 24; Wilbur H. Morrison, *Wings Over the Seven Seas: The Story of Naval Aviation's Fight for Survival* (London: A. S. Barnes and Co., Inc., 1975), 16. Greer recalls a unsigned statement from Naval officers supporting the rejection of a separate air arm based on the premise that the nation had to be prepared to defend itself at sea and on land. Further, that the dependence of all operations upon sea control reinforced the importance of naval aviation as an essential aid to the forces afloat.

[75] Morrison, 20.

[76] Ibid., 33. Morison quotes Admiral Sim's demand to Washington for both ships and planes to cover the battlefields and oceans, “The sooner planes get overseas the sooner the U-boats will be defeated.”

[77] Ibid., 47-48.

of military air power, commanders would create ad hoc structures to unify efforts of Naval and Army Air forces when operating in the same air space in the coming Second World War.

As a result to technological developments in air power following World War I, the air domain became increasingly congested, not just in air-to-air combat but among our own air forces. Advances in technology enabled specialized aircraft. The air became populated with reconnaissance aircraft, bombers, fighters, and transporters.[78] The congestion increased as various nations and military service components continued to develop their own capabilities.[79]

The air campaigns of World War II, most specifically in the Pacific Theater, would involve aircraft from the United States Army Air Forces, Navy, and Marines, as well as air forces from Allied nations. In order to sort out this congestion and establish a unity of effort in the air domain, theater commanders needed to establish a command and control structure that previously did not exist. Failure to do so risked not only mission accomplishment, but lives in the air and on the ground. While the World War II commanders achieved success, sometimes by luck, a command and control structure focused on unity of effort was not achieved until Operation Desert Storm, almost fifty years later.

Based on the speed of developments in the cyberspace domain, the United States cannot afford fifty years for theater and geographic combatant commanders to establish a joint cyberspace command and control structure. The cyberspace operations community should look to the achievement of unity of effort in the air domain as a guide. A look at a few United States

[78] Robin Higham, *Air Power: A Concise History*, 3rd ed. (Manhattan, KS: Sunflower University Press, 1988) 42, 48. Highman highlights the advances in speed, altitude, range, and lift that enabled specialization in aircraft design and capabilities.

[79] Higham, 48-49; James A. Winnefeld and Dana J. Johnson, *Command and Control of Joint Air Operations: Some Lessons Learned from Four Case Studies of an Enduring Issue* (Santa Monica, CA: RAND Corporation, 1991) 5-9. Higham discusses a few of the nations that explored air power in the years following World War I and leading to World War II. Winnefeld and Johnson discuss the development of air power from the perspectives of the United States Air Force, Navy, and Marines.

air campaigns throughout history will serve as this guide.

In 1991, Retired Naval Officer James Winnefeld and Dana Johnson conducted case studies on the World War II campaigns of Midway and the Solomon Islands, Korea from 1950 to 1953, and Vietnam from 1965 to 1968.[80] They focused unity of effort as they defined it as, "the objective of any command and control system." Winnefeld and Johnson later state, "unity of effort is defined as an overarching principle that encompasses 'solidarity of purpose, effort and command. It directs all energies, assets, and activities, physical and mental, toward desired ends.'"[81]

The current Joint Publication 3-0 *Joint Operations,* identifies and defines "unity of effort" within the twelve principles of Joint Operations.[82] In addition to operating under a single commander, the principle Unity of Command includes the importance of operating towards a common purpose. JP 3-0 defines this as Unity of Effort.

> During multinational operations and interagency coordination, unity of command may not be possible, but the requirement for unity of effort becomes paramount. Unity of effort—the coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization—is the product of successful unified action.[83]

[80] Winnefeld and Johnson, iii-iv. In their report, Winnefeld and Johnson note that at Midway and the Solomons, control of the air was in doubt and a considerable portion of the total effort was on naval and air targets. The opponent had first class forces and employed them (for the most part) very skillfully. The air campaigns of the Korean and Vietnam case studies were characterized by opponents with much less than first class air power and negligible naval power, but with major land forces. Air power's principal function was the destruction of the opponent's ground forces and their support structure. The report neglects the World War II air campaigns of Europe and Africa due to a lack of joint air operations. Winnefeld and Johnson end their report in 1968 when they determined most tactical air command and control issues had been addressed. Based on the timing of their report (written December 1990), they state it was too soon to discuss Desert Shield and Desert Storm.

[81] Ibid., v.

[82] Department of Defense, Joint Publication (JP) 3-0, *Joint Operations* (Washington, DC: Government Printing Office, August 2011), 1-2. The twelve principles of joint operations are: Objective, Offensive, Mass, Maneuver, Economy of force, Unity of command, Security, Surprise, Simplicity, Restraint, Perseverance, and Legitimacy. Appendix A provides doctrinal explanations for each of the principles.

This paper will analyze historic joint air campaigns to understand if and how they achieved unity of effort through unity of command. Using those case studies as examples, it will recommend a course of action for achieving the same for cyberspace operations.

During the Midway campaign of 1942, although the two air operations functioned separately (land-based and carrier-based) and each with their own commander, the two operations achieved their own internal simultaneity. This should not be confused with unity of effort. Winnefeld and Johnson conclude unity of effort was achieved, "largely by accident or as a result of imminent threat to the survival of the forces engaged."[84]

As the westernmost American base in the Pacific[85] "Midway Island act[ed] as a sentry for Hawaii."[86] As Commander of the U.S. Pacific Fleet and Pacific Ocean Areas, Admiral Chester W. Nimitz commanded all United States military forces in the Midway Theater of operation except for those under the command of General Douglas MacArthur in the Southwest Pacific.[87] Based on intelligence and his own assessment, on 2 May 1942 Nimitz determined Japan would next attack Midway Island.[88] Nimitz and his staff therefore planned for an estimated attack on 28

[83] JP 3-0, A-2.

[84] Winnefeld and Johnson, 56.

[85] Samuel Eliot Morison, *History of United States Naval Operations in World War II, Volume IV: Coral Sea, Midway and Submarine Actions May 1942 – August 1942* (Boston, MA: Little, Brown and Company, 1949) 74.

[86] Ibid., 70. Here Morison quotes Japanese Vice Admiral Chuichi Nagumo's report on the battle of Midway.

[87] Gordon W. Prange, Donald M. Goldstein and Katherine V. Dillon, *Miracle at Midway* (New York, NY: McGraw-Hill, 1982) 434.

[88] Morison, 38. Morison explains how Commander Joseph Rocheford and the Combat Intelligence Office through cryptanalysis cracked the Japanese Navy's operational code, JN25 and determined Midway as Japan's target. Morison, 17-46.

May[89] later revised to 4 June.[90] Nimitz's plan called for his commanders to "inflict maximum damage on [the] enemy by employing strong attrition tactics," which, as Morison notes, translated to "air strikes on enemy ships."[91]

For the Midway naval campaign, Nimitz placed Rear Admiral Frank Jack Fletcher in command of the Carrier Striking Force, which consisted of Task Force Seventeen and Task Force Sixteen.[92] In their book, *Miracle at Midway*, Gordon Prange, Donald Goldstein and Katherine Dillon, explain Rear Admiral Frank Jack Fletcher commanded Task Force Seventeen while Rear Admiral Raymond A. Spruance commanded Task Force Sixteen. At a meeting with the two in Admiral Nimitz's Pearl Harbor office on 27 May 1942, Nimitz instructed Spruance to sail first, then when Flectcher rendezvoused with Spruance before the battle, Fletcher, as senior officer present afloat, would assume tactical command of the combined forces. The rendezvous occurred on 2 June 1942 north of Midway "beyond the protective range of Midway's land-based planes."[93] Despite the two task forces becoming one fighting force, they operated independently. This independence included the carrier air groups.

For the defense of Midway Island and the land-based air forces, Nimitz gave command to Commander Cyril T. Simard.[94] Nimitz's instructions to Simard regarding the land-based air

[89] Morison, 44.

[90] Ibid., 102. Morison notes Fleet Intelligence Officer, Captain Edwin T. Layton anticipated contact would be made at 0600 Midway time, 4 June, 325 degrees northwest at a distance of 175 miles. His estimation was five minutes, five degrees, and five miles off as contact was made at 320 degrees, 180 miles, at 0555.

[91] Ibid., 84.

[92] Prange, Goldstein, and Dillon, 99-100.

[93] Ibid., 150.

[94] Morison, 85; Prange, Goldstein, and Dillon, 38. Cyril T. Simard commanded the Naval Air Station at Midway.

operations were, “go all out for the carriers.”[95] Subordinate to Simard were Marine Air Group Twenty-two (MAG-22) under Lieutenant Colonel Ira E. Kimes, the Marine ground forces which included anti-aircraft artillery,[96] and a reconnaissance group, commanded by Commander Massie Hughes.[97] Nimitz’s air forces included Seventh Air Force, commanded by Major General Clarence L. Tinker.[98] Coordination of these forces fell to Commander Logan C. Ramsey, the air operations officer brought in by Nimitz’s Chief of Staff for that particular purpose.[99]

The Midway Island based reconnaissance aircraft reported to air operations on the island. The reports then went to both Nimitz's Fleet headquarters at Pearl Harbor and to Fletcher's Task Force headquarters aboard Yorktown.[100] Once reconnaissance reports identified Japanese naval force locations, the land-based bombing group attacked.[101] Ramsey used his land-based marine aircraft as a cover patrol following the initial bomber run then as the intercept force as part of Commander Simard's defense plan.[102] After the combined Marine land and air defense force fought off the Japanese air attack, Ramsey launched the joint Marine Corps dive-bombers and Army Air Force bombers toward the Japanese carriers.[103]

[95] Morison, 105.

[96] Prange, Goldstein, and Dillon, 64-65.

[97] Ibid., 174.

[98] Ibid., 59-60.

[99] Prange, Goldstein, and Dillon, 117. Interestingly, Nimitz’s Fleet Aviation officer, Commander Arthur C. Davis, was not mentioned as involved in the planning or execution of the Midway air campaign. Commander Davis is mentioned in name once only in *Miracle at Midway*, and does not receive any mention in Samuel Eliot Morison's *History of United States Naval Operations in World War II, Volume IV.*

[100] Ibid., 170.

[101] Ibid., 167.

[102] Morison, 104; Prange, Goldstein, and Dillon, 183.

[103] Morison, 110.

Fletcher's Task Force 17 and Spruance's Task Force 16 each launched their own carrier-based reconnaissance on their own timetables as deemed appropriate by the respective Task Force Commanders.[104] Fletcher then coordinated the naval attack forces, but treated the carrier-based air forces as separate efforts. On the morning of 4 June, Fletcher instructed Spruance to "Proceed southwesterly and attack enemy carriers when definitely located. I will follow as soon as planes recovered."[105] At 0702 Spruance launched an all-out attack Fletcher however, delayed launching until 0838.[106]

The carrier-based air attacks included torpedo bombers[107] and dive-bombers[108] with fighter coverage.[109] In the sinking of the Japanese carrier *Akagi*, Morison quotes its Captain, "We were unable to avoid the dive-bombers because we were so occupied in avoiding the torpedo attacks."[110] The campaign ended with the sinking of four Japanese carriers and a general retirement of the remaining fleet.[111] While the carrier-based attack achieved simultaneity with their own aircraft, the Midway campaign lacked the mass of a full-scale coordinated attack from the added land-based air force.

In their report, Winnefeld and Johnson explain a possible lack of coordination in the air attacks due to the radio silence required for setting up the ambush.[112] Thus, aside from Nimitz's

[104] Morison, 97; Prange, Goldstein, and Dillon 185.

[105] Morison, 113.

[106] Ibid., 114.

[107] Ibid., 116.

[108] Ibid., 121.

[109] Ibid., 122.

[110] Ibid., 124.

[111] Ibid., 139.

[112] Winnefeld and Johnson, 12.

guidance, the carrier-based and land-based air attacks lacked the simultaneity expected from a unity of effort enabled by a unity of command. This would not be the case in the coming Solomon Island campaign.

Beginning February 1942, the Commander in Chief of the U.S. Navy, Admiral Ernest J. King, pursued an offensive campaign in the South Pacific to establish "a series of strong points near enough for mutual air support from which a step-by-step general advance could be made" that would eventually threaten the main island of Japan.[113] The 1 April 1942 decision to divide the Pacific Theater of Operation into three areas placed the whole of New Guinea and all the Bismark and Solomon Islands in General Douglas MacArthur's area of responsibility. The New Hebrides island group, New Caledonia, and New Zealand in Admiral Nimitz's South Pacific area of responsibility would be commanded by Vice Admiral Robert L. Ghormley.[114]

On 17 April 1942, Ghormley received his initial guidance from King to plan for a

[113] Morison, 245-247. Morison presents a sequence of memoranda exchanges between Admiral King and General George Marshall from 18FEB42 to 2MAR42 discussing the establishment of American bases in the Solomon Islands. In a memorandum to President Roosevelt, following the surrender of Java, King argued for the defense of Australia and New Zealand. Strategically, Morison suggests, Japan had gained territory which would enable her to attain economic self-sufficiency in all strategic materials if given time to organize them. Morison notes that according to King's plan, "the approaches from Japan to Australia should be actively and continuously probed in order to hamper the enemy's southeasterly advance and prevent his consolidation of conquered areas."

[114] Morison, 249-250. Here Morison provides the division of the Pacific Theater of Operation as follows: General Douglas MacArthur's Southwest Pacific Area started at the China coast on latitude 20 degrees north, east to 135 degrees east, south along that meridian through the Philippine Sea to the Equator, east to longitude 165 east, south on that line to latitude 10 degrees south, southwesterly to latitude 17 degrees south – 160 degrees east, then south on that meridian to the Pole. Rear Admiral John F. Shafroth's Southeast Pacific Area covered everything east of a line from the Mexico-Guatemala boundary to a latitude 11 degrees north – longitude 110 degrees west, then south to the Pole. Admiral Chester W. Nimitz's Pacific Ocean Area was subdivided into three areas: the North Pacific Area (north of latitude 42 degrees north) included the Aleutians and Alaska, the Central Pacific Area (from latitude 42 degrees north to the Equator) included the Hawaiian, Gilbert, Marshall, Caroline, and Marianas Islands, and the South Pacific Area (from the Equator to the Pole) included the Ellice, Phoenix, Marquesas, Tuamotu, Samoa, Fiji and New Hebrides island groups and New Caldonia and New Zealand.

possible fall offensive in the South Pacific.[115] Ghormley assembled his staff and placed Rear Admiral John R. McCain as Commander Aircraft South Pacific Area.[116] McCain would exercise operational control of all Allied planes in the South Pacific.[117]

Originally, McCain was responsible for operational control, including training and indoctrination. While Army commanders were willing to place their air forces under theater command, they objected to entrusting Naval officers with training and indoctrination of Army Air Forces. "Such a move exceeded existing authority under the principle of unity of command."[118] Air planners recommended naval jurisdiction be confined to operational control and nothing more. Prior to the assault, Admiral Ghormley settled the argument by naming Admiral McCain responsible for operational control of all land-based and carrier-based aircraft. Additionally, he named Major General Millard F. Harmon, already the Commanding General of all U.S. Army Forces in the South Pacific Area, separately responsible for the training and indoctrination of Army Air Forces in the area.[119] This arrangement ensured operational unity of effort but showed the reliance on personalities to achieve such unity.

In his new capacity, McCain published doctrine for the employment of the air forces available to him.[120] Harmon, in his capacity, supervised the training of Army air units through the island commanders on which the air forces were stationed. These base commanders retained

[115] Morison, 251.

[116] Morison, 252; Wesley Frank Craven and James Lea Cate, *The Army Air Forces in World War II, Volume IV: The Pacific: Guadalcanal to Saipan August 1942 to July 1944* (Chicago, IL: The University of Chicago Press, 1950), 10.

[117] Morison, 252; Craven and Cate, 10. Since this pre-dates the Midway campaign, lessons-learned from Midway cannot be applied to Ghormley's decision to create a structure to unify command and control of all air forces in his command.

[118] Craven and Cate, 30.

[119] Ibid.

[120] Ibid.

responsibility for the routine employment of their units. Craven and Crate explain McCain's guidance:

> McCain prescribed a basic air organization encompassing all Allied air units in the area and calling for four commands: air patrol, bomber, fighter, and base. Control and coordination of these units was vested in the island defense commander, operating under the principle of unity of command, and he in turn exercised his command function through the air officer who controlled the local units. All combat aircraft were to be maintained in a mobile status, prepared to shift at short notice to any point which might become the focus of an enemy attack.[121]

The Army had air bases on the islands of Caldonia and Efate with an advanced air base on Espiritu Santo.[122] However, since these bases were too remote for the bombing of Guadalcanal, McCain's operations were thus limited to air reconnaissance until the landing force secured and completed construction on the Guadalcanal air field.[123]

On 10 July 1942, Admiral Ghromley received guidance for the seizure of Tulagi, Guadalcanal and Santa Cruz, including a list of available ground, air, and naval forces. Ghromley in return requested additional air support from General MacArthur stating that he (Ghormley) "had been given enough to do the job, provided General MacArthur could interdict interference by enemy planes based at Rabual and near-by fields."[124]

MacArthur's air forces were under the command of U.S. Army Air Forces Major General George C. Kenney.[125] These forces provided the initial aerial reconnaissance of the island.[126] Longitude 158 eastern divided the air reconnaissance missions. MacArthur's air support covered

[121] Craven and Cate, 31.

[122] Morison, 253-254.

[123] Ibid., 270.

[124] Ibid., 264.

[125] Craven and Cate, 26.

[126] Morison, 267.

Port Moresby, the Bismarcks, and the line of the Solomons to Guadalcanal.[127] The 21 July 1942 Japanese landing on Buna redirected MacArthur's attention to fighting both a defensive battle to protect Allied air bases in the Southwest Pacific while simultaneously providing the much needed reconnaissance for the invasion in the South Pacific.[128]

Morison notes, "Admiral Ghormley well said that a basic problem of the operations would be to protect ships from land-based air attack during the landing and the unloading."[129] This was accomplished through carrier-based air and naval anti-aircraft artillery.[130] At this level, the tactical commander controlled the air battle. The unity of effort lay in his hands. For the assault on Guadalcanal, Ghormley had Admiral Fletcher as officer in tactical command as well as the Expeditionary Force Commander, which he designated Task Force 61.[131]

Admiral Fletcher focused his efforts to provide air cover for the amphibious force landings through the Amphibious Force commander, Rear Admiral Richmond K. Turner.[132] Designated as Task Force 62, Turner was responsible for coordinating naval gunfire support and anti-aircraft protection to the landings, and commanded Fletcher's carrier-based air protection.[133] However, fearing a Japanese air counter-attack, Fletcher would not hold his carrier force within supporting distance for more than two days.[134] This decision left the Amphibious Force without local air support until construction on the Guadalcanal airfield was completed.

[127] Morison, 269.

[128] Morison, 269; Craven and Cate, 23-25.

[129] Morison, 292.

[130] Ibid., 295.

[131] Ibid., 268-270. Morison provides the complete task organization on pages 270-275.

[132] Ibid., 269.

[133] Ibid., 269, 278.

[134] Ibid., 281.

When Fletcher pulled his carrier force on 8 August 1942, he left Turner (in Turner's words) “bare-arsed.”[135] With no U.S. air forces to prevent them, Japanese air forces spotted Allied Naval forces for an ensuing battle and the sinking of four Allied cruisers.[136] Despite the losses, the naval transports remained operational along with the Marines occupying Guadalcanal.[137] The Marines managed to defend their foothold while simultaneously completing the airfield.[138]

The Guadalcanal airfield (named Henderson Field upon completion) received its first Marine Corps planes on 20 August 1942.[139] On 22 August 1942, the airfield welcomed a portion of the Army's 67th Fighter Squadron.[140] They would provide close air support to the Marines.[141] Naval dive-bombers from the carrier *Enterprise* soon joined the fighter squadron. Marine Major General Roy S. Geiger took command of Henderson Field air operations.[142]

In their analysis, Winnefeld and Johnson note the unique joint air operations commanded

[135] Samuel Eliot Morison, *History of United States Naval Operations in World War II, Volume V: The Struggle for Guadalcanal August 1942 – February 1943* (Boston, MA: Little, Brown and Company, 1950), 28.

[136] Morison vol. V, 35-64. In his chapter on the battle of Savo Island, Morison recounts Japanese aerial reconnaissance of Allied naval positions southwest of Salvo Island on the night of 8 August 1942. The reports led to the movement of a Japanese naval column of five heavy cruisers, two light cruisers and a destroyer into the Sound off Guadalcanal and Tulagi. Outside the range of land-based and carrier-based aircraft, the Japanese aerial reconnaissance operated unmolested. Additionally, the surprised Allied navy lacked the added dimension provided by their own aerial reconnaissance and aerial counter-attack capabilities. This resulted in the sinking of the cruisers *Canberra, Astoria, Quincy,* and *Vincennes.*

[137] Ibid., 63.

[138] Ibid., 68.

[139] Ibid., 68. Morison notes Henderson Field was named after a Marine hero of Midway.

[140] Ibid., 74.

[141] Ibid.

[142] Ibid., 75.

by General Geiger.

> The air operations that General Geiger directed had a broad sweep. There were no cross service quarrels as to which component did what. Marine and Navy aviators joined in attacking Japanese naval forces attempting to reinforce their ground forces. It was not unusual for a Navy carrier pilot landing on Guadalcanal for refueling to find himself diverted to attack Japanese shipping, launch on an air defense sortie, or be called upon to assist Marine ground forces with close air support.[143]

As the size and role of air forces in the Solomons grew, so too did the need for an organization to command this joint-multinational force.[144] Thus, on 16 February 1943, the Senior Naval Aviator who had been operational commander of all Guadalcanal aircraft, received the title "Air Command, Solomons" or COMAIRSOLS.[145] Although the Marine Aircraft Wing provided the initial support, the staff included representatives from all three services.[146]

In their assessment of the Solomons air campaign, Winnefeld and Johnson saw a "willingness to improvise, a subordination of service doctrine and mission biases to urgent operational demands, and the emergence of a truly joint air operations organization. As the lead service from the outset, the Navy established the institutional norms the operational commander and subordinates would follow. Thus when an Air Force officer did succeed to command, an existing and functioning system ensured Navy and Marine subordinates would accept the taskings.[147]

[143] Winnefeld and Johnson, 18.

[144] Craven and Cate, 88. By 1 February 1942, the fighter group on Guadalcanal included Army, Navy, Marine, and New Zealand fighter squadrons.

[145] Ibid., 88-89.

[146] Ibid., 89. In their notes, Craven and Cate provide the composition of COMAIRSOLS as follows: AAF – 69th Bomb. Squadron, detachments from 12th, 44th, 67th, 68th, 70th, and 339th Fighter Squadrons, 5th, 11th and 307th Bomb. Groups, 17th Photo Reconnaissance Squadron; Navy – Forward Echelon HQ, 2d Marine Aircraft Wing, Headquarter Squadron 14, Service Squadron 14, VMSB-131, 144, 324, VMF-123, VS4D-14, VCS Recon 3 (RNZAF), VF-72, Patron 12 and 51, VTB-11, 12, 16 (Marine Air Wing 2, War Diary, 17 February1943).

[147] Winnefeld and Johnson, 20.

The existential threats to U.S. and Allied forces during World War II increased the importance of a unified effort in the air campaigns. Additionally, as we saw, personalities matter. Contrary commanders focused on rigid rules, regulations and restrictions to service employment invite an added element of risk to the pursuit of common objectives. The air campaigns of Midway and the Solomon Islands showed how personalities can rise above service guidelines and operate in a group towards a common purpose. The air campaigns of Korea and Vietnam would see clashes of personalities, a breakdown in the unity of command and thus the lack of unified efforts.[148]

The Goldwater-Nichols act of 1986 instilled unified combatant commands with the authority to direct all aspect of military operations including prescribing the chain of command, organizing command and forces, and employing forces to carry out assigned missions.[149] During

[148] Winnefeld and Johnson, viii. In their summary of the Korean and Vietnam air campaigns, Winnefeld and Johnson highlight the clash between and Navy and the Air Force over roles, mission, and hardware following World War II. The Air Force attempted to gain operational control of all tactical air forces operating in and from Korea. The Navy fought to keep control of its air component. Built around the concept of coordination control, the compromise the theater commander used, the Air Force acted as lead in coordinating joint air efforts, but had no command authority for requirements, taskings, or the direction of operations. The establishment of a joint task force further compartments the control of theater air forces. In Vietnam, unity of command issues occurred at two levels. First, the commander of the U.S. Military Assistance Command (COMUSMACV) did not have responsibility for operations in North Vietnam and Laos. That authority was retained by Commander U.S. Pacific Command. Second, COMUSMACV 's air component commander had three problems: he did not control all tactical air assets based or operating in South Vietnam, he did not have control of the helicopter operations characteristic of the campaign, he was responsible to his component commander, Commander in Chief Pacific Air Forces and the theater commander, but not to COMUSMACV for Air Force operations in most of North Vietnam and Laos. This resulted in a continuing battle for authority to task and apportion efforts among air forces, inefficient application of air assets and often an unsatisfactory state of control of air assets in the battle area.

[149] US Congress, Senate and House of Representatives, Goldwater-Nichols Department of Defense Reorganization Act of 1986, Public Law 99-433, 99th Cong., (1 October 1986), §164, accessed 11 November 2014, http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf. Specifically, the Goldwater-Nichols Act states, “Command authority of combatant commanders. (1) Unless otherwise directed by the President or the Secretary of Defense, the authority, direction, and control of the commander of a combatant command with respect to the commands and forces assigned to that command include the command functions of (a) giving authoritative direction to subordinate commands and forces necessary to

Operation Desert Storm, we would see the exercise of this authority in the creation of a Joint Forces Air Component Command. This would unify the command and therefore the unity of effort in the air campaign.

Prior to Iraq's 2 August 1990 pre-dawn invasion of Kuwait,[150] the planned used of air power was "to support ground forces in accordance with the AirLand Battle philosophy."[151] The theater commander's understanding of the capability and value of air power in the area of operation would change its application. His decision to unify the air effort enabled comprehensive management of a variety of resources in a heavily congested domain. This unity of effort directly supported and ultimately led to the rapid ground war victory.

As commander of US Central Command (CENTCOM), General Norman Schwarzkopf had Lieutenant General Charles A. Horner as commander of the CENTCOM supporting Ninth Air Force and US Central Command Air Forces (CENTAF). Schwarzkopf's additional air forces came

carry out missions assigned to the command, including authoritative direction over all aspects of military operations, joint training, and logistics; (b) prescribing the chain of command to the commands and Forces within the command; (c) organizing commands and forces within that command as he considers necessary to carry out missions assigned to the command; (d) employing forces within that command as he considers necessary to carry out missions assigned to the command; (e) assigning command functions to subordinate commanders; (f) coordinating and approving those aspects of administration and support (including control of resources and equipment, internal organization, and training) and discipline necessary to carry out missions assigned to the command; and (g) exercising the authority with respect to selecting subordinate commanders, selecting combatant command staff, suspending subordinates, and convening courts-martial, as provided in subsections (e), *(f),* and (g) of this section and section 822(a) of this title, respectively.

[150] Thomas A. Keaney and Eliot A. Cohen, *Revolution in Warfare? Air Power in the Persian Gulf* (Annapolis, MD: Naval Institute Press, 1995) 1.

[151] John Andreas Olsen, *Strategic Air Power in Desert Storm* (London: Frank Cass Publishers, 2003) 48. On the preceding page, 47, Olsen discusses how the Army's war fighting philosophies dominated military thinking and doctrine leading up to Operation Desert Storm. The doctrine of AirLand Battle and the concept of battlefield air interdiction placed air power in a subordinate role. Additionally, in 1984, the Army and Air Force Chiefs of Staff laid out 31 (later expanded to 35) Initiatives designed to enhance the joint employment of air power in support of land power in battle. "The doctrine assumed that a future war would involve ground forces against enemy ground forces, and the key to success would be to out-manoeuvre the enemy on the battlefield." Air power would provide fire support to the ground forces.

from US Marine air forces, a US Navy carrier battle group, and coalition air forces as follows: combat units from Great Britain, France, Canada, and Italy; transport aircraft and crews from South Korea, New Zealand and Argentina; and Gulf state air forces from Saudi Arabia, Kuwait, Bahrain, Qatar, and the United Arab Emirates.[152] Schwarzkopf designated Horner as his Joint Forces Air Component Commander (JFACC) with the authority to control most Coalition air power.[153] Saudi Air Forces ultimately remained under command of Saudi Lieutenant General Prince Khalid Bin Sultan al-Saud and his air forces commander.[154]

At a National Security Council meeting at Camp David on 4 August 1990, two days after Iraq's invasion, Schwarzkopf and Horner presented air power options.[155] When objections were raised to the potential success of air power alone, Schwarzkopf responded, “I am not an advocate of air power alone. But this is a target-rich environment. There is no cover in the desert. Their army has never operated under attack, and we have sophisticated munitions.”[156] Following the meeting, Secretary of Defense Dick Cheney instructed Schwarzkopf to develop an offensive option for the President.[157]

While Horner, now named the Forward commander for USCENTCOM in theater, focused on deployments and mobilizations, Schwarzkopf reached out to the Air Force Staff requesting a “retaliatory air campaign.”[158] Colonel John Ashley Warden III led a team that

[152] Keaney and Cohen, 2-3, 152.

[153] Ibid., 124.

[154] Ibid., 134.

[155] Olsen, 89.

[156] Ibid., 90.

[157] Ibid. The offensive option would be considered if the Iraqis engaged in further aggression or “unacceptable behavior such as killing Kuwaiti citizens or foreign nationals in Kuwait or Iraq,” or used chemical weapons. President George Bush was not contemplating intervention at the time, but stated, “this will not stand, this aggression against Kuwait.”

developed a plan calling for focused and intense air attacks on Iraqi leadership and its associated command, control, and communications systems.[159] Named “Instant Thunder,” the plan envisioned “unrelenting pressure on the Iraqi state and Saddam Hussein's regime,” according to Warden's “Five Rings Model.”[160] Targeting the enemy’s core and reducing the decision makers to a negligible level could enable defeat without needing to fully destroy the fifth ring - the forces in the field.[161] Approved through Chairman of the Joint Chiefs of Staff, General Colin Powell and General Schwarzkopf, Horner received “Instant Thunder,” but thought it fell short of applicability at the operational level.[162] Thus, Horner established a special planning group led by Brigadier General Buster Glosson with planners from Warden’s Checkmate group to translate “Instant Thunder” into an Air Tasking Order for implementation.[163] Their final four phased plan combined Warden’s and Checkmate’s strategic air offensive with suppression of enemy air

[158] Olsen, 91-92.

[159] Ibid., 64.

[160] Ibid., 93. On pages 73-87, Olsen explains the origins of Warden’s five rings. As director for war-fighting concept development, he focused on Air Force strategies, doctrine, long-range planning and new air power concepts. His Force Assessment Division, referred to as “Checkmate” developed the air campaign for Operation Desert Storm. In his Five Rings Model, Warden viewed the enemy as a system with the state’s centers of gravity as five concentric circles. At the center of the circle is the state’s national leadership which gives the state its strategic direction. The state’s energy facilities, as the next ring, surrounded the core. Oil, gas, and electricity provide the organic essentials necessary for the core to survive. The third ring contains the state’s infrastructure, industry, and transportation. These keep the society connected and enable mobility and movement. The fourth ring contained the population. Olsen notes that Warden did not find it acceptable to target citizens directly with anything but psychological means. The fifth and final ring is the state’s fielded military forces meant to protect the internal rings from aggression. Olsen also notes Warden thought the four outer rings should be attacked only as far as necessary to expose the leadership ring. For further information, see John A. Olsen, *John Warden and the Renaissance of American Air Power* (Washington, DC: Potomac Books, 2007).

[161] Ibid., 85.

[162] Ibid., 111.

[163] Ibid., 111 and 128.

defenses and targeting Iraqi combat power simultaneously in Kuwait preparing the way for and providing support to a ground offensive.[164]

Advancements in technology led to a vast array of capabilities available to the theater commander. At Schwarzkopf's disposal, and for Horner to manage, were the following operations: strategic and tactical air reconnaissance, inter- and intra-theater airlift, air refueling, command and control, electronic warfare, air-to-air combat, air attack (predominately of ground based targets), and rotary wing (predominately in support of the ground war).[165] While the US and Coalition forces still had reservations about target selection and the apportionment of taskings, Keaney and Cohen note, "they accepted the need for a single authority to coordinate an air campaign and to provide safe separation of the two- to three-thousand aircraft sorties flown per day in the theater's limited airspace.[166] Horner utilized the daily air tasking order (ATO) as the means to direct almost all Coalition air forces.[167] The daily ATO provided details on nearly every coalition fixed-wing sortie scheduled. This included all air refueling operations as well. The services and allied partners appreciated and understood the importance of the ATO, "if only to avoid midair collisions with any of the more than two thousand sorties flown daily during the air campaign. [168] Critics of the daily ATO complained its hundreds of pages were too cumbersome, took too long to prepare, transmit, and receive.[169] Nevertheless, the ATO was the JFACC's tool of

[164] Olsen, 156-157; Jerome V. Martin, *Victory from Above: Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm* (Maxwell Air Force Base, AL: Air University Press, 1994), 56-57.

[165] Keaney and Cohen, 152-172. This entire chapter of Keaney and Cohen's book explains the instruments of air power available. Keaney and Cohen present the volume and type of aircraft, the quantity of sorties flown, and purpose for each.

[166] Ibid., 5.

[167] Ibid. Keaney and Cohen note helicopters flying at less than five hundred feet above the ground were exempted from direct JFACC control, as were naval aircraft on overwater flights.

[168] Ibid., 127.

choice to successfully manage and deconflict operations in a heavily congested battlespace.

The variety of targets, available aircraft, and changing priorities as the battlefield matured presented unique challenges and opportunities to the JFACC staff. The air war began 17 January 1991 with coordinated strikes against strategic military, leadership, and infrastructure targets in Iraq.[170] The primary concern of air superiority in these first days was accomplished by specialized aircraft with most air combat losses occurring in the first week of the war.[171] The JFACC staff carefully matched the appropriate munitions to the desired effect while simultaneously striving to avoid excessive collateral damage in a process known as weaponeering. To reduce the risk of daylight flights over Baghdad, the JFACC coordinated the employment of naval Tomahawk land-attack missiles, "to keep the pressure on during daylight."[172] Laser-guided bombs, surface-to-surface, and air-to-surface missiles were directed against industrial, government, and communications facilities, and used in direct attacks against Iraqi armored forces.[173] A variety of anti-armor and anti-personnel cluster munitions were employed to reduce Iraqi ground force combat power by fifty percent before the ground war began.[174]

[169] Keaney and Cohen, 127-128. Keaney and Cohen highlight later on page 159, the intra-theater airlift aircraft physically delivered the daily ATO to locations that did not have the electronic equipment necessary for processing the information.

[170] Ibid., 10.

[171] Ibid., 12. The array of specialized aircraft included F-15 and F-14 fighters, E-3 and RC-135 airborne warning, control, and intelligence aircraft, EF-111 and EA-6 electronic jamming support aircraft, and high-speed anti-radiation missiles fired at Iraqi radars.

[172] Ibid.

[173] Ibid.

[174] Ibid., 13. Keaney and Cohen (on page 40) and Olsen (on page 145) note the fifty percent stemmed from General Schwarzkopf's CENTCOM Combat Analysis Group (CAG) when determining the necessary effective air power to avoid "heavy casualties." Although this attrition figure initially included all troops and major pieces of equipment, CENTCOM planners later revised it to theater-wide tanks, armored personnel carriers and artillery.

To achieve the desired attrition rate, the JFACC staff divided the labor against the Iraqi Republican Guard and the frontline Iraqi troops.

> F-16s, F/A-18s, F-15Es, F-111s, and A-6s flew against the more distant, better-equipped, and better dug-in Republican Guard. Closer to the front, AV-8Bs, A-10S, and many of the other Coalition aircraft tackled the entrenched Iraqi Infantry. B-52s attacked area targets (breaching sites, ammunition stockpiles, troop concentrations, and military field headquarters).[175]

Coalition helicopters brought additional mobility and firepower to the battlefield. "In several instances, because of low ceilings due to weather, blowing sand, or oil well fires, only helicopters could operate successfully."[176] In the later stages of the air campaign, the priority of effort shifted from the Republican Guard to more direct attacks on the frontline Iraqi troops.[177]

In preparation for the ground offensive, air and ground units rehearsed close air support procedures. Additionally, as the JFACC, General Horner established new rules of engagement to support the ground campaign. [178] As a result, the bulk of Coalition aircraft not scheduled for close air support were assigned to interdiction sorties to destroy supplies and prevent reinforcement of the front lines.[179] "The plan intended to put maximum pressure on the Iraqi forces with every

[175] Keaney and Cohen, 13. As a result of their success, B-52s became one of the most sought-after aircraft by ground commanders for close air support attacks against Iraqi ground forces.

[176] Ibid., 97-98.

[177] Ibid., 18. B-52 sorties increased to effect breaching operations, MC-130s dropped fifteen-thousand-pound bombs to clear mine field, and a greater concentration of A-10s attacked the Iraqi forces.

[178] Ibid., 19. Keaney and Cohen cite: Comments come from log of 24 February 1991. Headquarters CENTAF Office of History. *Daily Comments of Lt Gen Charles A. Horner, 17 January through 28 February 1991,* GWAPS, CHP 13B. Horner's guidance, as provided in the log, were "The weather considerations that were valid last week are no longer valid. There are people's lives depending on our ability to help them if help is required. So I want a push put on. I want people feeling compulsion to hit a target. I do not want fratricide. So if in doubt don't shoot."

[179] Ibid.

type of strike aircraft at the Coalition's disposal."[180] Thus, when the ground offensive began on 24 February 1991, more than three thousand sorties flew, the majority directed towards the heavy reserve and retreating columns as the Iraqi army fled Kuwait.[181]

The war ended with a Coalition-declared cease-fire at 0800 on 28 February 1991.[182] Schwarzkopf understood the value and capability of air power and through his JFACC he employed it to great success. His early action naming his CENTAF commander as the JFACC ensured a unity of effort in the air campaign that ultimately led to victory on the ground. As Lieutenant Colonel Jerome Martin captured, "The decisive effects of the coalition's air offensive highlighted the importance of centralized control for all air assets in a theater. The JFACC ensured that the implementation of the air campaign plan was tightly focused and that the large air armada from many countries operated smoothly in a highly complex combat operation."[183]

The current Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*, captures this development in the evolution of air power command and control. As specified in the introduction, this publication provides joint doctrine for the command and control for joint air operations and discusses the responsibilities of a joint force air component commander (JFACC) as established by the joint force commander (JFC).[184] The joint publication recommends the air

[180] Ibid., 21.

[181] Ibid. The destruction caused by these air interdiction sorties led to the media termed, "Highway of Death." On page 99, Keaney and Cohen explain how retreating traffic from southeast Kuwait combined with those fleeing Kuwait City along the major highway leading north to Iraq. Once air attacks halted the lead vehicles, the remaining vehicles became choked and thus destroyed in subsequent air attacks. A count of destroyed vehicles from photos on 1 March 1991 show more than fourteen hundred including fourteen tanks and fourteen other armored vehicles. For more information, Keaney and Cohen direct readers to: Steve Coll and William Branigan, "U.S. Scrambled to Shape View of 'Highway of Death,'" *The Washington Post*, 11 March 1991, 1.

[182] Keaney and Cohen, 21.

[183] Martin, 63.

[184] Department of Defense, Joint Publication (JP) 3-30, *Command and Control of Joint*

component be organized for unified action through the principle of unity of command. Doctrinally, the joint force commander has three options for organizing command and control of joint air operations: designate a joint force air component commander, designate a Service component commander, or retain and exercise command and control through his own joint force staff.[185] Joint forces normally conduct air operations through centralized control and decentralized execution, "to achieve effective control and foster initiative, responsiveness and flexibility."[186]

JP 3-30 states joint force commanders normally designate a JFACC to establish unit of command and unity of effort for joint air operations.[187] The JFACC, usually a dual-hatted Service component commander, exercises operational control over his own Service forces and tactical control over other Services' forces.[188] The JFACC is responsible for developing a joint air operations plan, recommending air apportionment priorities, allocating and tasking the joint air forces, providing oversight and guidance in the execution of joint air operations, assessing the effectiveness of joint air operations, and, if designated, perform the duties of the airspace control

Air Operations (Washington DC: Government Printing Office, 10 February 2014) I-1.

[185] JP 3-30, I-2.

[186] Ibid., I-3. JP 3-30 defines centralized control as giving one commander the responsibility and authority for planning, directing, and coordinating a military operation or group or category of operations and decentralized execution as the delegation of execution authority to subordinate commanders thus making it possible to generate the required tempo of operations and to cope with uncertainty, disorder, and fluidity of combat.

[187] Ibid., II-2.

[188] JP 3-30., II-2. JP 1-02 *Department of Defense Dictionary of Military and Associated Terms* defines operational control as, "The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission." That same publication defines tactical control as, "The authority over forces that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned."

authority, area air defense commander, and space coordinating authority.[189] The JFACC normally operates from a joint air operations center (JAOC) staffed and structured to operate as a fully integrated command center.[190] JP 3-30 recommends staff elements common to all JAOCs should be a strategy division, a combat plans division, an intelligence, surveillance, and reconnaissance division, an air mobility division, and a combat operations division with other divisions, cells or teams established as needed.[191]

According to JP 3-30, joint air forces are tasked by the JFACC, based on the JFC's approval of the air apportionment recommendation.[192] This is published in the air operations directive (AOD) and used throughout the planning stages of the joint air tasking cycle and the execution of the air tasking order (ATO).[193] The planning for joint air operations follows the joint operations planning process published in JP 5-0, *Joint Operations Planning*, with additional details in step seven, plan or order development that focuses on joint targeting and the joint air tasking cycle.[194] The six steps of the joint air tasking cycle provides "an iterative cyclic process for the planning, apportionment, allocation, coordination, and tasking of joint air missions,"[195] The JFACC continuously plans and evaluates the results of joint air operations, with all levels of the joint force performing assessments of the operation. [196]

[189] JP 3-30, II-2-3.

[190] Ibid., xi.

[191] Ibid., II-14. JP 3-30 Appendix E, "Joint Air Operations Center Divisions and Descriptions" provides detailed explanations of the roles and responsibilities of each of the recommended divisions.

[192] Ibid., II-16.

[193] Ibid., II-3.

[194] Ibid., III-15 – III-18.

[195] Ibid., xiii.

[196] Ibid., III-26.

Thus, twenty-three years following Operation Desert Storm, Command and Control of Joint Air Operations doctrine concisely guides the joint force and geographic combatant commanders through the establishment of a command and control structure to achieve unity of effort in a heavily congested domain. Similarly, Joint Publication 3-12 (R), *Cyberspace Operations,* states cyberspace operations "requires unity of effort to synchronize forces toward a common objective."[197] However, it does not recommend a command and control structure similar to a JFACC to achieve this unity of effort. Instead, it suggests adapting traditional command and control structures to conduct simultaneous global, theater, and joint operations area operations.[198]

[197] Department of Defense, Joint Publication (JP) 3-12 (R), *Cyberspace Operations* (Washington DC: Government Printing Office, 5 February 2013) II-6.

[198] JP 3-12 (R), II-6. The section on the joint functions of cyberspace operations highlights the dual nature of cyberspace operations and notes there may be times when cyberspace operations are conducted under two separate, but mutually supporting/supported chains of command.

Development of Cyberspace Operations

The last ten years has witnessed rapid developments in cyberspace especially with respect to command and control of cyberspace operations. The importance of unifying efforts in this new, contested, and heavily congested domain cannot be overstated. In an operational domain in contact with a variety of adversarial forces each and every day, the Department of Defense and Joint Forces does not have the luxury of forty years to determine the best command and control structure. History has provided a ready example of an effective structure for achieving unity of effort. With that in mind, a review of the cyberspace developments and an understanding of the nature of cyberspace itself will lead us to a command and control structure appropriate for this domain.

Most cyber power theorists trace the origin of cyberspace to the birth of the Advanced Research Projects Agency Network (ARPANET); the first ARPANET message was sent on 29 October 1969.[199] Two years later, the first virus-like program known as "The Creeper" spread across the ARPANET.[200] As the internet and the Department of Defense Information Network grew out of the ARPANET[201] and malicious programs became more sophisticated, great efforts

[199] Stuart H. Star, "Toward a Preliminary Theory of Cyberpower" in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington DC: National Defense University Press and Potomac Books, 2009), 82; Robert O'Harrow Jr. and Greg Linch, "Timeline: Key Events in Cyber History," *The Washington Post*, 3 June 2012, accessed 30 December 2014, http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/. Both sources provide a graphical timeline of important cyberspace related events. Star breaks his into five different portions: evolution of cyberspace, evolution of cyberpower: military perspective, evolution of cyberpower: economic perspective, evolution of cyber strategy: selected attacks and responses, timeline of key institutional events. O'Harrow and Linch provide a single timeline.

[200] "First Computer Virus, Creeper, Was No Bug," Discovery News, 16 March 2011, accessed 30 December 2014, http://news.discovery.com/tech/first-computer-virus-creeper-was-no-bug-110316.htm.

[201] Star, 84. Star cites 1983 as the date the military network (MILNET) split from ARPANET thus creating the internet while O'Harrow and Linch cite 1990 as when ARPANET became the internet.

went to both tame and weaponize this new domain.[202] The 2007 cyber attacks on Estonia, the 2008 cyber attacks on Georgia, and the 2010 "Stuxnet" attack on Iran offer just a hint of the open-source evidence of weaponized cyberspace.[203]

In 2012, then Secretary of Defense Leon Panetta warned of a "cyber Pearl Harbor" attack that could, "could dismantle the nation's power grid, transportation system, financial networks and government."[204] Sounding very much like the total war theorists of early air power, Secretary Panetta contradicted cyber power theorists like Martin Libicki and Colin Gray who view cyber power as a supporting capability to terrestrial operations. As Libicki states,

> Operational cyberwar cannot win an overall war on its own; it is a support function, and is likely to remain so indefinitely. It cannot occupy territory; put people's lives at risk; or, except in specialized cases, break things.[205]

The Department of Defense's recent efforts in doctrine and command and control of cyberspace operations support this theory. This includes establishing United States Cyber Command and

[202] O'Harrow and Linch cite a Gus W. Weiss article, "The Farewell Dossier," on the Central Intelligence Agency's website detailing a 1982 operation that sold United States made computer equipment with malicious code to the Soviet Union as the first nation-on-nation cyberattack. For further information see https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm. O'Harrow's and Linch's timeline continues to recount thirteen more "hacks" of various types, individual, military, nation-state, industrial, and academic.

[203] Deborah S. Karagosian, "The Megabyte Will Always Get Through," (Monograph, Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies, 2012), 1; David Hollis, "Cyberwar Case Study: Georgia 2008" *Small Wars Journals*, 6 January 2011. Accessed 29 July 2014 http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[204] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of cyberattack on U.S.," *New York Times,* 11 October 2012, accessed 5 February 2015, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

[205] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 140. Libicki refers to cyber power as cyberwar, and differentiates between strategic and operational cyberwar. On page 139, he defines the as follows: a campaign of cyberattacks launched by one entity against a state and its society, primarily but not exclusively for the purpose of affecting the target state's behavior, would be strategic cyberwar (emphasis his); while operational cyberwar consists of wartime cyberattacks against military targets and military-related civilian targets.

declaring Cyberspace as an operational domain. A January 2013 announcement to expand the Department of Defense cyberspace workforce indicated Joint Force Commanders will soon have trained and ready forces to conduct cyberspace operations in each Geographic Combatant Commander's area of operations.

The remarkable advancements in cyberspace operations places its development on par with air operations. Today's Commanders could potentially have control over simultaneous offensive, defensive, and stability operations in their assigned cyberspace much like the Joint Commanders had with air operations in World War II. Unfortunately, today's cyberspace operations doctrine does not offer guidance on how to unify efforts in cyberspace. Instead, Commanders must rely on personalities to coordinate and cooperate towards common cyberspace objectives, again much like air operations of World War II. The Joint Force Commander should look to history for a structure to unite his cyberspace efforts that support his larger objectives.

The 2010 Quadrennial Defense Review declared that, "[a]lthough it is a manmade domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space."[206] Over a year later, in July 2011, Deputy Defense Secretary William Lynn unveiled the *Department of Defense Strategy for Operating in Cyberspace,* designating cyberspace as an operational domain.[207] As mentioned in the strategy this designation, "is a critical organizing concept for DoD's national security missions. This allows DoD to organize, train, and equip for cyberspace as we do in air, land, maritime, and space

[206] Department of Defense, *Quadrennial Defense Review Report, February 2010* (Washington, DC: Department of Defense, February 2010), 37. The QDR notes the following regarding the nature of cyberspace: "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."

[207] David Alexander, "Pentagon to Treat Cyberspace as 'Operational Domain,'" *Reuters,* 14 July 2011, accessed 23 December 2014, http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

to support national security interests."[208] However, as mentioned in the 2011 version of Joint Publication 3-12 *Cyberspace Operations*, the unique nature of cyberspace requires a unique approach to command and control.[209]

A quick review of how joint doctrine defines the operational domains reveals this unique nature that ties cyberspace simultaneously to all other operational domains while maintaining an environment unique unto itself:

> The land domain is the land 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. The land domain shares the Earth's surface with the maritime domain.[210]
>
> The maritime domain consists of the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals.[211]
>
> The air domain is described as the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible.[212]
>
> Cyberspace is defined as the global domain within the information environment consisting of the interdependent network of information technology (IT) infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[213]
>
> Cyberspace consists of three different layers, "physical network, logical network, and

[208] DoD *Strategy for Operating in Cyberspace*, 11.

[209] JP 3-12, II-5. The joint publication specifically states, "the dual nature of cyberspace operations as simultaneously providing actions at the global level and at the theater or joint operational area level necessitates adaptations in command and control structures."

[210] Department of Defense, Joint Publication (JP) 3-31, *Command and Control for Joint Land Operations* (Washington DC: Government Printing Office, 24 February 2014) I-4.

[211] Department of Defense, Joint Publication (JP) 3-32 *Command and Control for Joint Maritime Operations* (Washington DC: Government Printing Office, 7 August 2013) I-1.

[212] Department of Defense, Joint Publication (JP) 3-30 *Command and Control of Joint Air Operations* (Washington DC: Government Printing Office, 10 February 2014) I-1.

[213] JP 3-12 (R), I-1.

cyber-persona."[214] Each layer presents a level, or plane, on which to conduct cyberspace operations. The telecommunications networks, computers, switches, routers, wires, frequencies along the electromagnetic spectrum, and the geographical area occupied by these objects comprise the physical network layer. As noted in JP 3-12 (R), "While geopolitical boundaries can easily be crossed in cyberspace at a rate approaching the speed of light, there are still sovereignty issues tied to the physical domains."[215]

The logical network layer consists of elements related to one another, but separated from the physical network layer. As an example, JP 3-12 (R) offers, "any web site that is hosted on servers in multiple physical locations where all content can be accessed through a single uniform resource locator (URL)."[216] The cyber-persona layer relates to the network users, but recognizes an individual user can have multiple cyber-personas and vice-versa. This creates challenges when targeting in cyberspace. [217] .

Additional characteristics of cyberspace include rapidly evolving technology and low barriers to entry. Often tied to Moore's law of semiconductor development,[218] the rapidly

[214] JP 3-12 (R), I-2.

[215] Ibid., I-3.

[216] Ibid., I-3. As a further example, the joint publication provides: Defense Knowledge Online exists on multiple servers in multiple locations in the physical domains, but is represented as a single URL on the World Wide Web. A more complex example of the logical layer is the DOD's Nonsecure Internet Protocol Router Network (NIPRNET).

[217] Ibid., I-4. JP 3-12 (R) specifically states, "Because cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form, significant intelligence collection and analysis capabilities are required for the joint forces to gain sufficient insight and situational awareness (SA) of a cyber-persona to enable effective targeting and creation of the JFC's desired effect."

[218] Michael Kanellos, "Moore's Law to Roll on for Another Decade," *CNET News*, 10 February 2003, accessed 24 December 2014, http://news.cnet.com/2100-1001-984051.html. Moore's Law states that the number of transistors on a given chip can be doubled every two years. Kanellos states this law has been the guiding principle of progress in electronics and computing since Moore first formulated the famous dictum in 1965.

evolving technology that makes up cyberspace enables cyberspace operations to "occur near the speed of light and in real time, and often can impact the entire spectrum of the cyberspace domain simultaneously without notice or intelligence indicators."[219] Commonly referred to as the, "low barrier to entry," this second characteristic, compares the cost of a large combat weapons system, like the F-22, to the cost of a computer, internet connection, and malware code. Enabled by the rapid advancements in technology, the inexpensive alternative of cyberspace "provides actors who could not otherwise effectively oppose the United States using traditional military forces with an asymmetric alternative."[220] Therefore, to achieve a unity of effort for operations in the cyberspace domain, the command and control structure must address the geography of cyberspace, the speed of cyberspace, and the global effect of operations, while maintaining awareness of cyberspace based threats.[221]

In the wake of a breach on the United States military's classified data network,[222] the Secretary of Defense initiated efforts to create such a command when he directed the Commander of United States Strategic Command (USSTRATCOM) to establish United States Cyber Command (USCYBERCOM).[223] In his autobiography, Robert Gates recalls how the Department

[219] David Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Forces Quarterly* 58, (3rd Quarter, July 2010): 50, accessed 24 December 2014, http://www.dtic.mil/doctrine/jfq/jfq-58.pdf.

[220] JP 3-12 (R), I-4.

[221] The geography of cyberspace refers to the geographical nature of the physical entities that make up the domain. The speed of cyberspace refers to the speed and ease at which the data passing through cyberspace violates any sovereignty tied to the geographical location of the objects that make up cyberspace. Cyberspace based threats are those that seek to deny United States and Allied forces the freedom of action in and through cyberspace.

[222] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010), accessed 26 December 2014 http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain. The article discusses "Operation Buckshot Yankee."

[223] United States Cyber Command, accessed 24 December 2014, https://www.cybercom.mil/default.aspx. Also found on the USCYBERCOM website is the

of Defense was "not well organized internally to deal with cyber issues."[224] He recognized that the unique characteristics and threats to national security presented by cyberspace required a command structure to unify the various Department of Defense cyberspace related efforts.

Prior to the 23 June 2009 memorandum that created USCYBERCOM, the defense and global operations of the Department of Defense networks was under the Joint Task Force-Global Network Operations (JTF-GNO) while offensive operations were under the Joint Functional Component Command – Net Warfare (JFCC-NW).[225] In a disjointed effort, both reported separately to USSTRATCOM. The USSTRATCOM website tells a short history of JTF-GNO and JFCC-NW:

> The U.S. military's reliance on computer networks grew exponentially in the 1980s and 1990s. National leaders took steps to protect defense networks in 1998, creating a Joint Task Force for Computer Network Defense and assigning it to USSPACECOM. In April 2001, the task force's mission expanded to include computer network attack, and it was renamed Joint Task Force—Computer Network Operations. The task force became part of USSTRATCOM in October 2002; it was renamed Joint Task Force—Global Network Operations (JTF-GNO) in 2004. The network attack mission transferred in 2003 to a new organization, which evolved into the Joint Functional Component Command—Network Warfare (JFCC-NW) in January 2005.
>
> A new attack led to further reorganization. A malicious code, which would allow an adversary to download critical defense information, spread across the DoD's classified and unclassified networks in 2008. As JTF-GNO synchronized efforts to disinfect and protect over 2.5 million computers in 3,500 DoD organizations spanning 99 countries, Defense Secretary Robert Gates endorsed the idea of a new sub-unified command under USSTRATCOM that would recombine offensive and defensive computer network operations.[226]

organization's mission statement: "United States Cyber Command (USCC) plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries."

[224] Robert M. Gates, *Duty: Memoirs of a Secretary at War* (New York, NY: Alfred A Knopf, 2014) 449.

[225] US Congress, House of Representatives, *U.S. Cyber Command: Organizing for Cyberspace Operations, Hearing before the Committee on Armed Services,* 111th Cong., 2nd sess., 23 September 2010, 6.

With these two organizations as its foundation, USCYBERCOM reached its initial operational capability on 21 May 2010.[227] According to the organization's website.

To support USCYBERCOM, the services (Army, Navy, Air Force, and Marines) each established their own cyber component. The timeline for the activation of those commands are as follows:

United States Air Forces Cyber Command, activated 18 August 2009.[228]
United States Marine Corps Forces Cyber Command, activated 21 January 2010.[229]
United States Fleet Cyber Command, activated 29 January 2010.[230]
United States Army Cyber Command, activated 1 October 2010.[231]

These service cyber components would later supply the manpower for the evolving cyberspace operations support to Combatant Commanders.

In order to provide cyberspace operations support to the Combatant Commanders, in June of 2012 Secretary of Defense Leon Panetta announced another new cyber related command and control structure, referred to as the "Joint Staff Transitional Cyberspace Operations Command

[226] "History" United States Strategic Command, August 2014, accessed 26 December 2014 http://www.stratcom.mil/history/.

[227] Department of Defense, *U.S. Cyber Command Fact Sheet* (Washington DC: Department of Defense Office of Public Affairs, 25 May 2010), accessed 26 December 2014 http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

[228] Department of the Air Force, 24th Air Force Office of History, *History of HQ Twenty-Fourth Air Force and 624th Operations Center* (Lackland, TX: 24th Air Force Public Affairs, 17 January 2014), accessed 26 December 2014, http://www.24af.af.mil/shared/media/document/AFD-140429-035.pdf.

[229] Alan J. McCombs, "Marines Launch into Cyberspace Mission with New Command" United States Army News Archives, last modified 29 January 2010, accessed 26 December 2014, http://www.army.mil/article/33744/Marines_launch_into_cyberspace_mission_with_new_command/.

[230] Fleet Cyber Command/10 Fleet Public Affairs, "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," last modified 29 January 2010, accessed 26 December 2014, http://www.navy.mil/submit/display.asp?story_id=50954.

[231] "Establishment of U.S. Army Cyber Command" United States Army Cyber Command, accessed 26 December 2014, http://www.arcyber.army.mil/history_arcyber.html.

and Control Concept of Operations."[232] According to the Defense News article, the concept places more authority for both offensive and defensive operations under the geographic combatant commanders (GCC) and creates Joint Cyber Centers (JCC) for the purpose of improved situational awareness, defense of the command's networks, and defense response and recovery support.[233] The concept also calls for USCYBERCOM staffed Cyber Support Elements (CSE) to locate with the GCC and work as part of a unified effort with the JCCs for planning and synchronizing cyberspace operations. The shortcomings of this structure includes a lack of trained personnel for the JCCs and the continued requirement for National Command Authority approval for offensive cyberspace operations. According to the article, the JCCs would be staffed by existing personnel from the GCC staff, thus leaving other staff sections short of personnel to fulfill this new requirement. With the exception of defensive cyberspace operations, Commanders still must seek approval from the President or Sectary of Defense for offensive cyberspace operations, and coordinate with other commands or agencies for Department of Defense Information Network (DODIN) operations.[234]

Despite these shortcomings, GCCs reported standing up JCCs as early as May of 2012.[235] In his 2014 Posture Statement to the House Armed Services Committee Statement, Commander, United States Pacific Command, Admiral Samuel J. Locklear, III reported on his command's

[232] Zachary Fryer-Briggs, "Panetta Green Lights First Cyber Operations Plan," *Defense News*, 6 June 2012, accessed 31 July 2014 http://www.defensenews.com/article/20120606/DEFREG02/306060010/Panetta-Green-Lights-First-Cyber-Operations-Plan.

[233] Fryer-Briggs, "Panetta Green Lights First Cyber Operations Plan."

[234] Department of the Army, Field Manual (FM) 3-38 *Cyber Electromagnetic Activities* (Washington DC: Government Printing Office, February 2014) 3-10.

[235] Thomas J. Doscher**, "**NORAD, USNORTHCOM Joint Cyber Center Stands Up," Peterson Air Force Base, CO: United States Northern Command Public Affairs, last modified 1 May 2012, accessed 27 December 2014, http://www.northcom.mil/Newsroom/tabid/3104/Article/3062/norad-usnorthcom-joint-cyber-center-stands-up.aspx.

progress with the JCC indicating it was not new and showing a commitment to a unity of effort.

> USPACOM continues as a global leader in intelligence and cyber systems. It has established and is maturing the Joint Cyber Center-Pacific (CYBERPAC), which plans, integrates, synchronizes and directs theater cyberspace operations. The aim is to set the theater for cyberspace operations, provide assured command and control and information sharing with joint and inter-organizational partners and forces, and direct regional cyber missions to meet USPACOM objectives. USPACOM continues to work with DoD counterparts to receive additional cyber forces and build appropriate mechanisms to command and control such forces across all operations.[236]

While showing a commitment to unifying cyberspace operations efforts, the report also revealed the lack of "appropriate mechanism to command and control such forces." While the JCC structure may do well to deconflict and coordinate defensive cyberspace operations, commanders should have a structure to directly command and control all cyberspace operations in their area of operations.

The additional Cyber Support Elements (CSE), announced by Secretary Panetta, grew from a USCYBERCOM effort to provide commanders with knowledgeable personnel to support cyberspace operations planning. USCYBERCOM and the service cyber components would internally support the CSE personnel requirements in order to prevent any growth in the military's workforce. In a Defense News article, then Commander of USCYBERCOM, General Keith Alexander said, "Our goal is to ensure that a commander with a mission to execute has a full suite of cyber-assisted options from which to choose, and that he can understand what effects they will produce for him."[237]

[236] Senate Armed Services Committee, *Statement of United States Pacific Command Posture*, Admiral Samuel J. Locklear, Commander, United States Pacific Command, 25 March 2014, 23, accessed 27 December 2014, http://www.pacom.mil/Media/SpeechesTestimony/tabid/6706/Article/8597/pacom-house-armed-services-committee-posture-statement.aspx.

[237] Zachary Fryer-Briggs, "CYBERCOM Arming U.S. Combatant Commands" *Defense News*, 21 March 2012, accessed 27 December 2014, http://www.defensenews.com/article/20120321/DEFREG02/303210007/CYBERCOM-Arming-U-S-Combatant-Commands.

Seven months after Secretary Panetta's announcement on the transitional command and control structure, Ellen Nakashima of the Washington Post wrote of the Pentagon's approval to expand the cyber workforce by approximately four-thousand soldiers and civilians. The Cyber Mission Forces plan, as published in the 2014 QDR calls for National Mission Forces to protect computer systems, Cyber Protection Forces to fortify the Department of Defense Information Network, and Combat Mission Forces to help commanders plan and execute offensive cyberspace operations. [238] In a March 2013 statement to the Senate Committee on Armed Services, General Alexander expanded on the scope and purpose of the new operational cyber forces, but did not reveal a structure to command the forces.[239]

These new operational cyber forces address USCYBERCOM's three ongoing and overlapping cyberspace operations: offensive cyberspace operations, defensive cyberspace operations, and Department of Defense Information Network Operations. Additionally, it provides Combatant Commands with trained teams to conduct cyberspace operations in direct

[238] Ellen Nakashima, "Pentagon to Boost Cybersecurity Force" *Washington Post,* 27 January 2013, accessed 27 December 2014, http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

[239] Senate Armed Services Committee, *Statement of General Keith B. Alexander Commander United States Cyber Command 12 March 2013*, 6, accessed 27 December 2014, http://www.armed-services.senate.gov/imo/media/doc/Alexander%2003-12-13.pdf. General Alexander's statement included the comments: "We are establishing cyber mission teams in line with the principles of task organizing for the joint force. The Services are building these teams to present to U.S. Cyber Command or to support Service and other Combatant Command missions. The teams are analogous to battalions in the Army and Marine Corps—or squadrons in the Navy and Air Force. In short, they will soon be capable of operating on their own, with a range of operational and intelligence skill sets, as well as a mix of military and civilian personnel. They will also have appropriate authorities under order from the Secretary of Defense and from my capacity as the Director of NSA. Teams are now being constructed to perform all three of the missions given to U.S. Cyber Command. We will have 1) a Cyber National Mission Force and teams to help defend the nation against national-level threats; 2) a Cyber Combat Mission Force with teams that will be assigned to the operational control of individual Combatant Commanders to support their objectives (pending resolution of the cyber command and control model by the Joint Staff); and 3) a Cyber Protection Force and teams to help operate and defend DoD information environment."

support, but the command and control remains disjointed. As discussed earlier, any operation in the cyberspace domain can have far-reaching global effects. However, if not synchronized and unified, a commander taking offensive action in his neck of the cyberspace woods could cause a fellow commander, unaware of the ongoing operations, to take significant defensive actions in another neck.

According to JP 3-12 (R), "To minimize overlap, the primary responsibility for cyberspace operations coordination between USCYBERCOM and the JFCs will reside with the cyberspace support element in coordination with the Combatant Command joint cyberspace centers."[240] While this sounds good on paper, it also harkens back to the reliance on personalities to deconflict and unify the operational effort. This structure leaves Joint Force Commanders with a cyberspace operations effort much like air operations post World War II and prior to Desert Storm. In order to achieve a level of success on par with Desert Storm air operations, the new Cyber Mission Force and Joint Force Commanders require a command and control structure that addresses the daily operations of maintaining and defending the DODIN, while simultaneously planning offensive and defensive operations necessary for the United States military to maintain freedom of maneuver in cyberspace.

[240] JP 3-12 (R), II-1.

Conclusion

In his guide to Joint Force Commanders on cyberspace operations, Major Brett Williams reminds his readers of the Joint Force Commander's two cyberspace objectives: freedom of maneuver and projecting power.[241] To accomplish both, the commander should command and control all forces operating within the domains in his area of operations. Assuming the Joint Force Commander owns the tactical cyberspace in which he operates, he needs a command structure to unify the operations in *his* cyberspace.[242] However, joint doctrine for forming a joint task force, Joint Publication 3-33, does not address unifying efforts for cyberspace operations.

Due to the military's reliance on cyberspace for day-to-day information sharing and command and control operations, the Joint Force Commander can safely assume all his forces will operate within the cyberspace domain. To protect these operations, he may choose to request a Cyber Protect Force from the cyber mission force. Additionally, based on the new structure of cyber mission force, he should expect to receive a Cyber Combat Mission Force. Therefore, to unite his own communications directorate staff with the various cyber mission forces into a singular effort, the Joint Force Commander should establish joint force cyberspace component command or a JFCCC.

Reviewing the history and development of air power and cyber power reveal striking

[241] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly* no. 73 (April 2014): 14, accessed 31 July 2014, http://ndupress.ndu.edu/JFQ/JointForceQuarterly73.aspx.

[242] This assumption is based on comments made by then Commander, Combined Arms Center, Lieutenant General David Perkins, at the Association of the United States Army panel on Building the Army's cyber Forces. "We have decided who owns cyber domain, and it's the same person that owns the land domain – the commander. What the commander has to do with the staff … is synchronize all of the efforts and actions in all of the domains with all of the other domains." General David G. Perkins, "Building the Army's cyber Forces: 2013 Association of the United States Army Panel Discussion" (video), AUSA Annual Meeting 2013, Washington DC, published 24 October 2013, accessed 29 December 2014, https://www.youtube.com/watch?v=fFQvcqIRdiI.

similarities to one another. The success of air operations united through a component commander either as a best practice or by doctrine should serve as a guide for the continued development of cyberspace operations. As the size and capability of the Cyber Mission Forces continues to grow along with the need for those forces to support Joint Force Command priorities, so does the need to unify efforts.

Based on the current doctrine, the most likely command and control structure for the Cyber Mission Force teams reporting to the Joint Force Commander would be operational control (OPCON) through a Joint Cyber Center within the Operations Directorate (J-3). The teams would still maintain their administrative control (ADCON) reporting structure with their parent command as well as USCYBERCOM for deconfliction and situational awareness. The addition of multinational partners would significantly increase the complexity of the already complex relationship, thus increasing the time in the commander's decision cycle. This would likely result in missed opportunities or a lost position of advantage in a domain where timeliness is critical.

Much like other component commands, a JFCCC would provide the Joint Force Commander with a subordinate command to plan, task, and control joint cyberspace operations. By designating a single, knowledgeable commander responsible to unify the cyberspace efforts, the Joint Force Commander enables his Director of Operations to focus on unifying all joint command efforts in support of unified action. The JFCCC would then unite the efforts of the attached cyber protection forces conducting the daily operation and defense of the JFC's assigned portion of the DODIN and the cyber combat mission forces planning and executing offensive cyberspace operations. The JFCCC would provide additional situational awareness to the joint staff, boards, bureaus, centers, cells, and working groups through their respective liaison officers. Drawing further examples from the structure of the JFACC, the JCCC would have the responsibility to develop a joint cyber operations plan (JCOP), act as the cyberspace control authority (CCA) and area cyberspace defense commander (ACDC), oversee the joint cyberspace targeting process and joint cyberspace tasking cycle, and publish the cyberspace tasking order. The joint cyberspace targeting process would directly support the greater joint targeting cycle in accordance with Joint Publication 3-60, *Joint Targeting.*

The continued development of forces specially trained to enable Joint Force Commanders with the ability to maneuver freely in and through cyberspace calls for a structure to unify those forces' efforts. The striking similarities between the developments of air power and cyber power offer an applicable example. Joint Force Commanders, cyberspace theorists and doctrine writers should continue to follow air power's historical examples and establish a joint force cyberspace component command as that structure.

Bibliography

Alexander, David. “Pentagon to Treat Cyberspace as ‘Operational Domain,” *Reuters.* 14 July 2011. Accessed 23 December 2014. http://www.reuters.com/article/2011/07/14/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714.

Arquilla, John and David Ronfeldt. “Cyberwar is Coming!” In *In Athena’s Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 23-60. Santa Monica: RAND Corporation, 1997.

Associated Press. “U.S. Files Economic Espionage Charges against Chinese Military Hackers,” CBS News. Last modified 19 May 2014. Accessed 29 December 2014. http://www.cbsnews.com/news/u-s-government-files-economic-espionage-charges-against-chinese-hackers-sources-say/.

Brown, Gary D. and Owen W. Tullos, “On the Spectrum of Cyberspace Operations.” *Small Wars Journal*, 11 December 2012. Accessed 31 July 2014. http://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.

Bumiller, Elisabeth and Thom Shanker. “Panetta Warns of Dire Threat of cyberattack on U.S.,” *New York Times.* 11 October 2012. Accessed 5 February 2015. http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Chen, Thomas M. “An Assessment of the Department of Defense Strategy for Operating in Cyberspace.” *The Letort Papers.* Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press. September 2013.

Chairman, Joint Chiefs of Staff. *The National Military Strategy of the United States of America, 2011*: *Redefining America's Military Leadership.* Washington, DC: Department of Defense, 2011.

Clausewitz, Carl von. *On War*. Translated and edited Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

Cooper, Jeffrey R. “Another View of the Revolution in Military Affairs.” In *In Athena’s Camp: Preparing for Conflict in the Information Age*, edited by John Arquilla and David Ronfeldt, 99-140. Santa Monica: RAND Corporation, 1997.

Craven, Wesley Frank and James Lea Cate. *The Army Air Forces in World War II, Volume IV: The Pacific: Guadalcanal to Saipan August 1942 to July 1944.* Chicago, IL: The University of Chicago Press, 1950.

Denny, Eric J. “The Cyberspace Domain: Path to a New Service?” Monograph, Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies, 2013.

Department of Defense. *Department of Defense Directive 8500.01, Cybersecurity.* Washington, DC: Department of Defense, 14 March 2014.

Department of Defense. *Department of Defense Strategy for Operating in Cyberspace.* Washington, DC: Government Printing Office, July 2011.

______. Joint Publication (JP) 3-0, *Joint Operations.* Washington DC: Government Printing Office, August 2011.

______. Joint Publication (JP) 3-12, *Cyberspace Operations*. Washington DC: Government Printing Office, 7 December 2011.

______. Joint Publication (JP) 3-12 (R), *Cyberspace Operations.* Washington DC: Government Printing Office, 5 February 2013.

______. Joint Publication (JP) 3-14 *Space Operations*. Washington DC: Government Printing Office, 29 May 2013.

______. Joint Publication (JP) 3-30, *Command and Control of Joint Air Operations*. Washington DC: Government Printing Office, February 2014.

______. Joint Publication (JP) 3-31, *Command and Control for Joint Land Operations*. Washington DC: Government Printing Office, 24 February 2014.

______. Joint Publication (JP) 3-32 *Command and Control for Joint Maritime Operations.* Washington DC: Government Printing Office, 7 August 2013.

______. Joint Publication (JP) 3-33, *Joint Task Force Headquarters*. Washington DC: Government Printing Office, 30 July 2012.

______. Joint Publication (JP) 3-59 *Meteorological and Oceanographic Operations*. Washington DC: Government Printing Office, 7 December 2012.

______. Joint Publication (JP) 5-0, *Joint Operation Planning.* Washington DC: Government Printing Office, 11 August 2011.

______. *Quadrennial Defense Review Report, February 2010*. Washington, DC: Department of Defense, February 2010.

______. *Quadrennial Defense Review.* Washington, DC: Government Printing Office, 2014.

______. *U.S. Cyber Command Fact Sheet*. Washington DC: Department of Defense Office of Public Affairs, 25 May 2010. Accessed 26 December 2014. http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

Department of the Air Force. 24th Air Force Office of History. *History of HQ Twenty-Fourth Air Force and 624th Operations Center*. Lackland, TX: 24th Air Force Public Affairs, 17 January 2014. Accessed 26 December 2014. http://www.24af.af.mil/shared/media/document/AFD-140429-035.pdf

Department of the Army. *2013-2014 How the Army Runs: A Senior Leader Reference Handbook.* Carlisle, PA: U.S. Army War College Press, 2013.

______. Army Doctrine Publication (ADP) 3-0, *Unified Land Operations*. Washington DC: Government Printing Office, October 2011.

______. Army Field Manual (FM) 3-38, *Cyber and Electromagnetic Activities.* Washington DC: Government Printing Office, February 2014.

______. Army Regulation (AR) 5-22, *The Army Force Modernization Proponent System.* Washington DC: Government Printing Office, March 2011.

Discovery News. "First Computer Virus, Creeper, Was No Bug," Discovery News Tech. Last modified 16 March 2011. Accessed 30 December 2014. http://news.discovery.com/tech/first-computer-virus-creeper-was-no-bug-110316.htm.

Doscher, Thomas J. "NORAD, USNORTHCOM Joint Cyber Center Stands Up." Peterson Air Force Base, CO: United States Northern Command Public Affairs. Last modified 1 May 2012. Accessed 27 December 2014. http://www.northcom.mil/Newsroom/tabid/3104/Article/3062/norad-usnorthcom-joint-cyber-center-stands-up.aspx

Feickert, Andrew. *The Unified Command Plan and Combatant Commands: Background and Issues for Congress Specialist in Military Ground Forces.* Washington, DC: Congressional Research Service, 3 January, 2013. Accessed 1 November 2014. http://fas.org/sgp/crs/natsec/R42077.pdf.

Fleet Cyber Command/10 Fleet Public Affairs. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet." Last modified 29 January 2010. Accessed 26 December 2014. http://www.navy.mil/submit/display.asp?story_id=50954.

Fryer-Briggs, Zachary. "Panetta Green Lights First Cyber Operations Plan," *Defense News.* 6 June 2012. Accessed 31 July 2014. http://www.defensenews.com/article/20120606/DEFREG02/306060010/Panetta-Green-Lights-First-Cyber-Operations-Plan.

______. "CYBERCOM Arming U.S. Combatant Commands" *Defense News*, 21 March 2012. Accessed 27 December 2014. http://www.defensenews.com/article/20120321/DEFREG02/303210007/CYBERCOM-Arming-U-S-Combatant-Commands.

Futrell, Robert F. *The United States Air Force in Korea, 1950-1953*. Washington, DC: Department of the Air Force, 1981.

Galdi, Theodor W. "Revolution in Military Affairs? Competing Concepts, Organizational Responses, Outstanding Issues." *Congressional Research Service Report for Congress*. Doc. 95-1170F. 11 December 1995. Accessed 30 August 2014. http://www.au.af.mil/au/awc/awcgate/crs/95-1170.htm.

Gates, Robert M. *Duty: Memoirs of a Secretary at War.* New York, NY: Alfred A Knopf, 2014.

Giles, Keir with Andrew Monaghan. “Legality in Cyberspace: An Adversary View.” *The Letort Papers*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press. March 2014.

Gjelten, Tom, “First Strike: US Cyber Warriors Seize the Offensive.” *World Affairs Journal,* January 2013. Accessed 31 July 2014. http://www.worldaffairsjournal.org/article/first-strike-us-cyber-warriors-seize-offensive.

Glines, Carroll V. *The Compact History of the United States Air Force.* New York, NY: Hawthorn Books, 1963.

Goldman, Emily O., and Thomas G. Mahnken, eds. 2004. *The Information Revolution in Military Affairs in Asia*, New York, NY: Palgrave MacMillan.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013.

Greer, Thomas H. *The Development of Air Doctrine in the Army Air Arm, 1917-1941.* Maxwell Air force Base: USAF Historical Division, Research Studies Institute, Air University, 1955.

Higham, Robin. *Air Power: A Concise History.* 3rd ed. Manhattan, KS: Sunflower University Press, 1988.

Hollis, David M. “Cyberwar Case Study: Georgia 2008” *Small Wars Journal*, 6 January 2011. Accessed 29 July 2014. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

______. “USCYBERCOM: The Need for a Combatant Command versus a Subunified Command,” *Joint Forces Quarterly* 58, (3rd Quarter, July 2010): 48-54. Accessed 24 December 2014, http://www.dtic.mil/doctrine/jfq/jfq-58.pdf.

Kanellos, Michael. “Moore's Law to Roll on for Another Decade.” *CNET News*, 10 February 2003. Accessed 24 December 2014. http://news.cnet.com/2100-1001-984051.html.

Karagosian, Deborah S., “The Megabyte Will Always Get Through.” Monograph, Fort Leavenworth, KS: U.S. Army School of Advanced Military Studies, 2012.

Keaney, Thomas A., and Eliot A. Cohen. *Revolution in Warfare? Air Power in the Persian Gulf.* Annapolis, MD: Naval Institute Press, 1995.

Knox, MacGregor and Williamson Murray, eds. *The Dynamics of Military Revolution*. Cambridge: Cambridge University Press, 2001.

Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz, eds. 2009. *Cyberpower and National Security.* Washington, DC: National Defense University Press and Potomac Books.

Kuhn, Thomas S. *The Structure of Scientific Revolutions.* Chicago, IL: The University of Chicago Press, 1962.

Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, CA: RAND Corporation, 2009.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy;* 2010, Vol. 4 Issue 1, p 63. Accessed 31 July 2014. http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf.

Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010). Accessed 26 December 2014. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

MacIsaac, David. "Voices from the Central Blue: The Air Power Theorists." In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 624-647. Princeton, NJ: Princeton University Press, 1986.

Mason, R. A. *War in the Third Dimension: Essays in Contemporary Air Power.* London: Brassey's Defence Publishers, 1986.

Martin, Jerome V. *Victory from Above: Air Power Theory and the Conduct of Operations Desert Shield and Desert Storm.* Maxwell Air Force Base, AL: Air University Press. 1994.

McCombs, Alan J. "Marines Launch into Cyberspace Mission with New Command" United States Army News Archives. Last modified 29 January 2010. Accessed 26 December 2014. http://www.army.mil/article/33744/Marines_launch_into_cyberspace_mission_with_new_command/.

Metz, Steven and James Kievit. *Strategy and the Revolution in Military Affairs: From Theory to Policy.* Carlisle Barracks, PA: Strategic Studies Institute and U.S. Army War College, 27 June 1995. Accessed 30 August 2014. http://www.au.af.mil/au/awc/awcgate/ssi/stratrma.pdf.

Morison, Samuel Eliot. *History of United States Naval Operations in World War II, Volume IV: Coral Sea, Midway and Submarine Actions May 1942 – August 1942*. Boston, MA: Little, Brown and Company, 1949.

______. *History of United States Naval Operations in World War II, Volume V: The Struggle for Guadalcanal August 1942 – February 1943*. Boston, MA: Little, Brown and Company, 1950.

Morrison, Wilbur H. *Wings Over the Seven Seas: The Story of Naval Aviation's Fight for Survival.* London: A. S. Barnes and Co., Inc., 1975.

Murphy, Matt. "War in the Fifth Domain. Are the Mouse and Keyboard the New Weapons of Conflict?" *The Economist,* (July 2010). Accessed July 19, 2014. http://www.economist.com/node/16478792.

Nakashima, Ellen. "Pentagon to Boost Cybersecurity Force" *Washington Post.* 27 January 2013. Accessed 27 December 2014. http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html.

Obama, Barack. *National Security Strategy of the United States*, *May 2010*. Accessed 4 September 2014. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

Office of the Secretary of Defense. *Memorandum for the Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations.* Washington DC: Government Printing Office, 23 June 2009.

O'Harrow, Robert Jr. and Greg Linch, "Timeline: Key Events in Cyber History." *The Washington Post* (3 June 2012). Accessed 30 December 2014. http://www.washingtonpost.com/wp-srv/special/investigative/zeroday/cyber-history-timeline/.

Olsen, John Andreas, *Strategic Air Power in Desert Storm.* London: Frank Cass Publishers. 2003.

Prange, Gordon W., Donald M. Goldstein and Katherine V. Dillon. *Miracle at Midway*. New York, NY: McGraw-Hill. 1982.

Scales, Robert H. Jr. *Certain Victory: The U.S. Army in the Gulf War.* Washington, DC: Brassey's Defence Publishers, 1997.

Shy, John. "Jomini." In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*, edited by Peter Paret, 143-185. Princeton, NJ: Princeton University Press, 1986.

Star, Stuart H. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, 43-88. Washington DC: National Defense University Press and Potomac Books, 2009.

Stephenson, Scott. "The Revolution in Military Affairs: 12 Observations on an Out-of-Fashion Idea," *Military Review.* XC, no. 3 (May 2010): 38-46. Accessed 30 September 2014. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20100630_art001.pdf.

Totty, Michael. "The First Virus...and Other Not-So-Great Moments in the History of Computer Mischief," *The Wall Street Journal*, (26 September 2011). Accessed July 19, 2014. http://online.wsj.com/news/articles/SB10001424053111904265504576568770117066628.

United States Army Cyber Command. "Establishment of U.S. Army Cyber Command." Accessed 26 December 2014, http://www.arcyber.army.mil/history_arcyber.html.

United States Congress. House of Representatives. *U.S. Cyber Command: Organizing for Cyberspace Operations, Hearing before the Committee on Armed Services,* 111th Cong., 2nd sess., 23 September 2010.

______. Senate. Committee on Armed Services. *Statement of General Keith B. Alexander Commander United States Cyber Command. 12 March 2013*. Accessed 27 December 2014. http://www.armed-services.senate.gov/imo/media/doc/Alexander%2003-12-13.pdf.

United States Congress. Senate. Committee on Armed Services. *Statement of United States Pacific Command Posture. Admiral Samuel J. Locklear, Commander, United States Pacific Command. 25 March 2014.* Accessed 27 December 2014. http://www.pacom.mil/Media/SpeechesTestimony/tabid/6706/Article/8597/pacom-house-armed-services-committee-posture-statement.aspx.

______. Senate and House of Representatives. Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433, 99th Cong. 1 October 1986. Accessed 11 November 2014. http://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf.

United States Cyber Command. "Mission." Accessed 1 November 2014. https://www.cybercom.mil/default.aspx

United States Strategic Command. "History." Last modified August 2014. Accessed 26 December 2014. http://www.stratcom.mil/history.

Vallance, Andrew G. B. *The Air Weapon: Doctrines of Air Power Strategy and Operational Art.* New York: St. Martin's Press, 1996.

Van Evera, Stephen. *Guide to Methods for Students of Political Science.* Ithaca, NY: Cornell University Press, 1997.

Williams, Brett T. "The Joint Force Commander's Guide to Cyberspace Operations." *Joint Force Quarterly* no. 73 (April 2014): 12-19, accessed 31 July 2014, http://ndupress.ndu.edu/JFQ/JointForceQuarterly73.aspx.

Winnefeld, James A., and Dana J. Johnson. *Command and Control of Joint Air Operations: Some Lessons Learned from Four Case Studies of an Enduring Issue*. Santa Monica, CA: RAND Corporation. 1991.

Wolk, Herman S. *Toward Independence: The Emergence of the U.S. Air Force 1945-1947.* Washington DC: Air Force History and Museums Program, 1996.

Zager, Robert and John Zager. "Combat Identification in Cyberspace." *Small Wars Journal,* (25 August 2013). Accessed 31 July 2014. http://smallwarsjournal.com/jrnl/art/combat-identification-in-cyberspace.