NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NETWORK ARCHITECTURE IN SUPPORT OF DATA STRATEGY FOR NAVAL SPECIAL WARFARE

by

Christopher R. Jennings

June 2021

Thesis Advisor:	Scot A. Miller
Co-Advisor:	Arkady A. Godin

THIS PAGE INTENTIONALLY LEFT BLANK

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 instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the 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 Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2021	**3. REPORT TYPE AND DATES COVERED** Master's thesis		
4. TITLE AND SUBTITLE NETWORK ARCHITECTURE IN SUPPORT OF DATA STRATEGY FOR NAVAL SPECIAL WARFARE				**5. FUNDING NUMBERS**
6. AUTHOR(S) Christopher R. Jennings				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000				**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A				**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.				**12b. DISTRIBUTION CODE** A
13. ABSTRACT (maximum 200 words)				
14. SUBJECT TERMS network architecture, data strategy, digital mission command, digital ecosystem, networks, data management, multi-dimensional arrays, naval special warfare command, NAVSPECWARCOM				**15. NUMBER OF PAGES** 117
				16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified		**20. LIMITATION OF ABSTRACT** UU

The United States Special Operations Command provides guidance on the development of a robust Digital Mission Command capability to meet future challenges in the uncertain operational environment. Research into innovative, state-of-the-art data management using multi-dimensional cubic storage promises to provide a single digital ecosystem to serve as the foundation for the employment of cutting-edge decision dominance, assured communications, and data-driven technological capabilities. This thesis examines the feasibility of implementing a modern data strategy in support of Naval Special Warfare operations at the tactical edge in a contested communications environment.

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

NETWORK ARCHITECTURE IN SUPPORT OF DATA STRATEGY FOR NAVAL SPECIAL WARFARE

Christopher R. Jennings
Lieutenant Commander, United States Navy
BS, Wayland Baptist University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
June 2021

Approved by: Scot A. Miller
Advisor

Arkady A. Godin
Co-Advisor

Alex Bordetsky
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Special Operations Command provides guidance on the development of a robust Digital Mission Command capability to meet future challenges in the uncertain operational environment. Research into innovative, state-of-the-art data management using multi-dimensional cubic storage promises to provide a single digital ecosystem to serve as the foundation for the employment of cutting-edge decision dominance, assured communications, and data-driven technological capabilities. This thesis examines the feasibility of implementing a modern data strategy in support of Naval Special Warfare operations at the tactical edge in a contested communications environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ADCON	Administrative Control
ADSI	Air Defense Systems Integrator
AI	Artificial Intelligence
AIDE	Automated Information Discovery Environment
AOR	Area of Responsibility
ATAK	Android Tactical Assault Kit
BLOS	Beyond Line of Sight
BMA	Battle Management Aid
BWC	Battle Watch Captain
C2	Command and Control
C2P	Command and Control Processor
C5ISR	Command, Control, Computers, Communications, Cyber, Intelligence, & Reconnaissance
CANES	Consolidated Afloat Networks and Enterprise Services
CAO	Civil Affairs Operations
CCIR	Commander's Critical Information Requirements
CIDNE	Combined Information Data Network Exchange
CJSOTF	Combined Joint Special Operations Task Force
COA	Course of Action
COIN	Counterinsurgency
COP	Common Operational Picture
CT	Counterterrorism
CWMD	Countering Weapons of Mass Destruction
DA	Direct Action
DARPA	Defense Advanced Research Projects Agency
DCGS	Distributed Common Ground System
DDIL	Denied, Degraded, Intermittent, Limited
DET	Detachment
DEVGRU	Naval Special Warfare Development Group
DOD	Department of Defense

DON	Department of the Navy
EEI	Essential Elements of Information
FHA	Foreign Humanitarian Assistance
FID	Foreign Internal Defense
FIR	Friendly Information Requirements
GCCS-J	Global Command and Control System – Joint
GCCS-M	Global Command and Control System – Maritime
GEOC	Global Enterprise Operations Center
HR	Hostage Rescue
IaaS	Infrastructure as a Service
JADOCS	Joint Automated Deep Operations Coordination System
JAIC	Joint Artificial Intelligence Center
JCS	Joint Chiefs of Staff
JEDI	Joint Enterprise Defense Infrastructure
JSOTF	Joint Special Operations Task Force
JTF	Joint Task Force
LDUUV	Large Displacement Unmanned Undersea Vehicle
LMMT	Link Monitoring and Management Tool
LOGSU	Logistic Support Unit
LOS	Line of Sight
MANET	Mobile Ad-Hoc Network
MCT	Mobile Communications Team
MDCOA	Most Dangerous Course of Action
MISO	Military Information Support Operations
ML	Machine Learning
MLCOA	Most Likely Course of Action
MSC	Mission Support Center
MT&E	Man, Train, and Equip
MTC2	Maritime Tactical Command and Control
NALCOMIS	Naval Aviation Logistics Command Management Information System
NAVSCIATTS	Naval Small Craft Instruction and Technical Training School

NAVSOF	Naval Special Operations Forces
NIST	National Institute of Science and Technology
NMCI	Navy Marine Corps Intranet
NSW	Naval Special Warfare
NSWC	Naval Special Warfare Command
NSWG	Naval Special Warfare Group
NSWTE	Naval Special Warfare Task Element
NSWTG	Naval Special Warfare Task Group
NSWTU	Naval Special Warfare Task Unit
NSWU	Naval Special Warfare Unit
NTCSS	Naval Tactical Command Support System
OLAP	Online Analytical Processing
OODA	Observe, Orient, Decide, Act
OPCON	Operational Control
OPT	Operational Planning Team
PaaS	Platform as a Service
PMESII-PT	Political, Military, Social, Information, Infrastructure, Physical Environment, and Time
POR	Program of Record
RFI	Request for Information
RoIP	Radio over Internet Protocol
SaaS	Software as a Service
SABRS	Standard Accounting, Budgeting, and Reporting System
SATCOM	Satellite Communications
SBT	Special Boat Team
SDN-H	SOF Deployable Node Heavy
SDN-L	SOF Deployable Node Light
SDN-M	SOF Deployable Node Medium
SDVT	SEAL Delivery Vehicle Team
SFA	Security Force Assistance
SIE	SOF Information Environment

SMARTS	Standard Accounting, Budgeting, and Reporting System (SABRS) Management Analysis Retrieval Tools System
SMEAC	Situation, Mission, Execution, Administration and Logistics, Command and Signal
SOCPAC	Special Operations Command, Pacific
SOF	Special Operations Forces
SOTF	Special Operations Task Force
SR	Special Reconnaissance
SRT	Special Reconnaissance Team
SUP C2	Supply Command and Control
SWCC	Special Warfare Combatant-Craft
TAC C2	Tactical Command and Control
TACLAN	Tactical Local Area Network
TACON	Tactical Control
TSOC	Theater Special Operations Command
USMC	United States Marine Corps
USSOCOM	United States Special Operations Command
UW	Unconventional Warfare
VOCO	Vocal Order

ACKNOWLEDGMENTS

First and foremost, I would like to express my love and deepest gratitude to my wife for her unwavering support and selfless understanding, which carried me through the many long hours, late evenings, and weekends. From the bottom of my heart, I am truly blessed to have such a wonderful, capable, and intelligent woman by my side. Liberty buddies for life.

Next, I would like to thank my thesis advisors, Scot Miller and Arkady Godin. Scot, your considerable encouragement and guidance was exactly what I needed to keep me on track and out of the weeds. Arkady, you are a delightful soul—your depth of knowledge and passion for learning are absolutely awe-inspiring. Thank you both very much for all that you have done for me, and all you continue to do to prepare the Fleet to meet the many challenges of the future.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Naval Special Warfare (NSW) fills a key role within the special operations community. As the maritime component of the United States Operations Command, NSW specializes in the execution of special operations within the maritime, littoral, and riverine environments. NSW relies on a relatively small group of highly intelligent, highly trained personnel who excel at operating in uncertain environments to perform a wide range of core and supporting activities including direct action, special reconnaissance, counter-terrorism, and unconventional warfare (Department of the Navy [DON], 2018). Often conducted in denied, hostile, and politically sensitive areas, NSW leverages the mission command framework of centralized planning and decentralized execution to achieve simplicity, security, repetition, surprise, speed, and purpose (McRaven, 1993) in the accomplishment of mission objectives.

Rapidly changing geopolitical, socio-economic, and technological conditions have presented new and evolving operational dilemmas for Joint Force Operations. With the return of Great Power Competition, the rise of non-state actors, the proliferation of advanced / disruptive technologies and a trend towards military problems below the level of traditional armed conflict, the Naval Special Warfare community will increasingly be called upon to employ their unique capabilities to provide a variety of understanding, influence, and precision actions that enable decisive operations by the Joint Force. This means that NSW must develop systems and processes that allow it to see itself, see the enemy, and quickly gain situational understanding of the operational environment to affect seamless horizontal and vertical integration in accordance with the tenants of mission command.

A. DIGITAL MISSION COMMAND

Digital Mission Command is derived from the United States Special Operations Command's vision for a global command and control capability that provides unparalleled situational awareness to meet future challenges in an uncertain operational environment. This vision calls for the innovative use of existing and cutting-edge technologies to create a highly responsive, all-domain C2 architecture that is networked physically, electronically, and virtually.

B. PROBLEM STATEMENT

A problem exists with the incorporation of Digital Mission Command into routine operations across various organizations and operational levels of command. It is difficult to distribute operationally relevant data and information required in a suitable format within tactically relevant timelines to realize true shared-situational understanding and unity of effort within a heterogeneous information environment. This is a problem because the preponderance of disparate and incompatible data processing, data storage, and communication systems results in the inability to achieve interoperability and graceful degradation among current command and control systems. A study that examines the feasibility of implementing a common foundational storage layer and supporting network architecture may lead to a deeper understanding of the capabilities and limitations of an integrated Digital Mission Command system in support of NSW operations.

C. PURPOSE STATEMENT

The purpose of this research is to increase understanding of the nature of Digital Mission Command as it relates to NSW operations and how to implement sharing of data, information, and knowledge at the enabling common data layer.

D. RESEARCH QUESTIONS

1. What is the nature of Digital Mission Command as it relates to NSW operations?
2. What are the limitations of current communications and data architectures with regard to the implementation of NSW Digital Mission Command?
3. What communications and data architectures would best support the implementation of NSW Digital Mission Command?
4. What additional research is required to further the NSW Digital Mission Command initiative?

E. THESIS DESIGN

This chapter lays out the context and background related to the problem of implementing Digital Mission Command. Chapter II of this thesis presents an in-depth overview of the principles of command and control, command and control systems, mission command and literature relevant to the problem and related context. Chapter III describes the methodology for the research and analysis of the problem. Chapter IV analyzes the problem. Finally, Chapter V summarizes the findings and conclusions of the analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. CHAPTER OVERVIEW

This thesis explores efforts to create digital mission command within the Naval Special Warfare community, such that it aligns to the broader Special Operations Command digital mission command initiatives. Prior to analysis, this chapter aims to establish a common understanding of the Naval Special Warfare mission, the principles of command and control in general, and how they relate to mission command. Additionally, it will provide an overview of the various command and control systems and describes essential information technology elements and data strategy connotations.

B. NAVAL SPECIAL WARFARE OVERVIEW

Naval Special Warfare (NSW), also known as Naval Special Operations Forces (NAVSOF) is the maritime component of the United States Special Operations Command (USSOCOM). NSW is responsible for the conduct of special operations within maritime, littoral and riverine environments to project power on, below, and from the sea (DON, 2018).

NSW is an agile force comprised of approximately 9,200 personnel. Members of this elite organization include SEALs, special warfare combatant-craft (SWCC) crewmen, combat support and combat service support personnel and civilians which account for less than 2 percent of the U.S. Navy and just over 10 percent total of U.S. Special Operations Forces (DON, 2018). According to the Naval Special Warfare Publication NWP 3-05, NSW's core operational approach is to

1. Maintain a readiness posture to respond to crises, contingencies, and war.
2. Win the trust and confidence of, and building the capacities and interoperability with, our coalition, regional, and host nation military counterparts.
3. Engage with interagency counterparts and country teams as part of an integrated effort.

NSW units rely on a maritime-focused, capabilities-based methodology characterized by stealth, dispersed, command and control (C2), and the precise application of force to accomplish mission objectives. Through carefully planned and executed actions, NSW effectively leverages its relatively small number of personnel and partner organizations in support of a broad spectrum of specialized tasks (DON, 2018).

1. Naval Special Warfare Command Core Activities

NSW Core Activities are separated into three distinct categories: Primary core activities, secondary core activities, and supporting core activities. Core activities are defined by the NWP 3-05 as derived from USSOCOM Directive 10–1 and are described in the following three subsections using the official definitions found within the DOD Dictionary of Military and Associated Terms (Joint Chiefs of Staff [JCS], 2021).

a. Primary Core Activities

A primary core activity is specific set of tasks that NSW is manned, trained and equipped to perform in a denied, hostile or politically sensitive environment which include (DON, 2018, pp. 17–18):

1. <u>Direct Action (DA)</u>. "Short-duration strikes and other small-scale offensive actions conducted as a special operation in hostile, denied, or diplomatically sensitive environments which employ specialized military capabilities to seize, destroy, capture, exploit, recover, or damage designated targets."

2. <u>Special Reconnaissance (SR)</u>. "Reconnaissance and surveillance actions conducted as a special operation in hostile, denied, or diplomatically and / or politically sensitive environments to collect or verify information of strategic or operational significance, employing military capabilities not normally found in conventional forces."

3. <u>Counterinsurgency (COIN)</u>. "Comprehensive civilian and military efforts designed to simultaneously defeat and contain insurgency and address its root causes."

4. Counterterrorism (CT). "Activities and operations taken to neutralize terrorist and their organizations and networks to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals."

5. Security Force Assistance (SFA). "The Department of Defense activities that support the deployment of the capacity and capability of foreign security forces and their supporting institutions."

6. Foreign Internal Defense (FID). "Participation by civilian agencies and military forces of a government or international organizations in any of the programs and activities undertaken by a host nation government to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security."

7. Countering Weapons of Mass Destruction (CWMD). "Efforts against actors of concern to curtail the conceptualization, development, possession, proliferation, use, and effects of weapons of mass destruction, related expertise, materials, technologies, and means of delivery."

b. Secondary Core Activities

A secondary core activity is a set of tasks that NSW has a limited degree of organization, manning, training, and equipment to perform in a denied, hostile, and politically sensitive environment which include (DON, 2018, pg. 18):

1. Foreign Humanitarian Assistance (FHA). "Department of Defense Activities conducted outside the United States and its territories to directly relieve or reduce human suffering, disease, hunger, or privation."

2. Hostage Rescue (HR). "A personnel recovery method used to recover isolated personnel who are specifically designated as hostages."

3. Unconventional Warfare (UW). "Activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a

government or occupying power by operating through or with an underground, auxiliary, and guerrilla force in a denied area."

c. Supporting Core Activities

A supporting core activity is a set of tasks that NSW can provide a limited supporting capability through the use of existing capabilities (DON, 2018, pg. 18):

1. Civil Affairs Operations (CAO). "Actions planned, coordinated, executed, and assessed to enhance awareness of, and manage the interactions with, the civil component of the operational environment; identify and mitigate underlying causes of instability within civil society, and/or involve the application of functional specialty skills normally the responsibility of civil government."

2. Military Information Support Operations (MISO). "Planned operations to convey selected information indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives."

2. Naval Special Warfare Administrative Organization

Naval Special Warfare is constituted by of the Naval Special Warfare Command (NSWC), six Naval Special Warfare Groups (NSWG) which are comprised of a mix of SEAL Teams, a SEAL Delivery Vehicle Team (SDVT), and Special Boat Teams (SBT) as well as the Naval Special Warfare Development Group and the Naval Special Warfare Training Center and a variety of supporting commands (DON, 2018).

The following sections provide a high-level overview of the various components. For a more detailed explanation, refer to the source material in NWP 3-05.

a. Naval Special Warfare Command

The Naval Special Warfare Command (NSWC) is located in Coronado, California and is assigned to the USSOCOM Combatant Command as the Echelon II Commander representing the Maritime Component. NSWC fulfills man, train, and equip (MT&E) functions to produce and deploy maritime SOF forces in support of USSOCOM tasking (DON, 2018). Figure 1 provides a general overview of NSW.

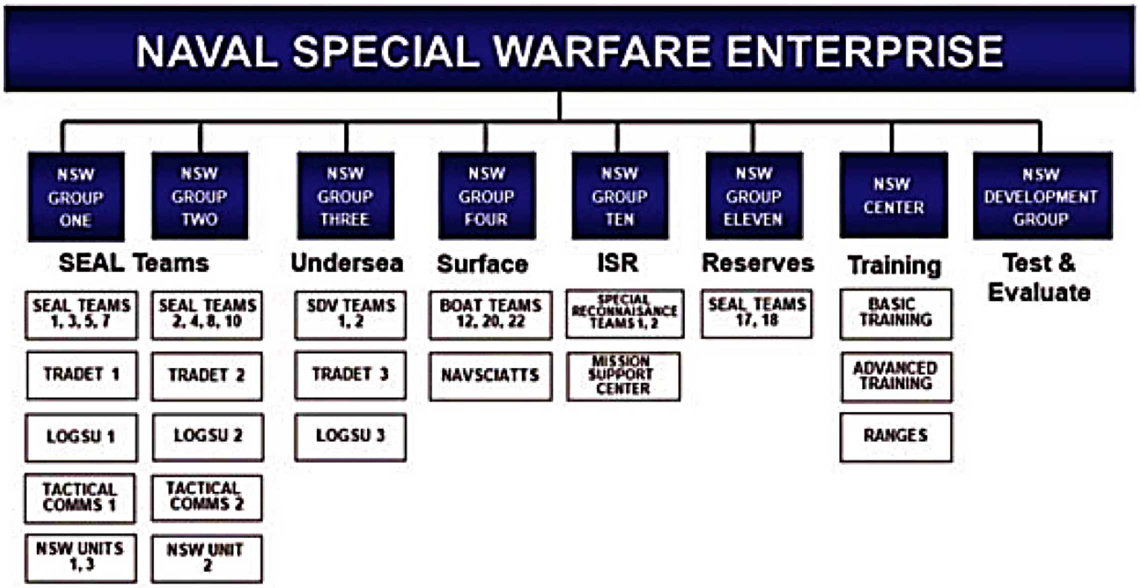


Figure 1. Naval Special Warfare Organization. Source: United States Special Operations Command (2021).

b. Naval Special Warfare Groups

A Naval Special Warfare Group is an Echelon III, O5-O6 Command comprised of various deployable forces such as SEAL Teams, SDVTs, SBTs and their supporting units. NSWG's exercise ADCON and OPCON and are responsible for the MT&E of assigned units. There are currently six NSWGs: NSWG ONE, NSWG TWO, NSWG THREE, NSWG FOUR, NSWG TEN and NSWG ELEVEN.

(1) Naval Special Warfare Group ONE - Coronado, CA

NSWG ONE serves as the regional coordinator for the provision of NSW support to the United States Central Command and the United States Indo-Pacific Command (INDOPACOM) Geographic Combatant Commander. Assigned forces include four SEAL

Teams, one training detachment, one logistics support unit, one mobile communications team, and two naval special warfare units. (DON, 2018)

(2) Naval Special Warfare Group TWO - Little Creek, VA

NSWG TWO is similar in function to NSWG ONE with the exception that it provides NSW support to the United States Africa Command (AFRICOM), the United States European Command (EUCOM), the United States Northern Command (NORTHCOM), and the United States Southern Command (SOUTHCOM). Assigned forces include four SEAL Teams, one training detachment, one logistics support unit, one mobile communications team, and three naval special warfare units.

(3) Naval Special Warfare Group THREE - Coronado, CA

NSWG THREE is responsible for the provision of undersea special operations in support of worldwide taskings by various entities. Assigned forces include SEAL Delivery Vehicle Team 1 stationed at Pearl Harbor, HI, one training detachment, one logistics unit and a secondary Group 3 detachment at Little Creek, VA to support East Coast operations.

(4) Naval Special Warfare Group FOUR - Little Creek, VA

NSWG FOUR provides rapid maritime surface mobility support for the NSW community in the form of various special operations craft capable of operating in open ocean, littoral, and riverine environments. Three Special Boat Teams, form the backbone of NSWG FOUR which are supported by the Naval Small Craft Instruction and Technical Training School and the Group 4 Detachment located at the Stennis Space Center in Mississippi.

(5) Naval Special Warfare Group TEN - Little Creek, VA

NSWG TEN is comprised of two Special Reconnaissance Teams (SRT) and the Mission Support Center (MSC). SRTs deploy to provide highly specialized intelligence capabilities to SOF and the Joint Force which combines intelligence gathering and operational analysis in support of various tasking. Analysts include diverse mix of personnel from the special operations, intelligence, METOC, and cryptological communities as well as electronics technicians and information systems technicians (DON, 2018).

(6) Naval Special Warfare Group ELEVEN - Coronado, CA

NSWG ELEVEN is the reserve component of NSW responsible for the MT&E and mobilization of two subordinate SEAL teams.

C. OBSERVE, ORIENT, DECIDE, ACT

The observe, orient, decide, act (OODA) loop, developed by Air Force Colonel John Boyd, is a decision-making approach that focuses on taking available information, placing it in context, deciding on a course of action, and then executing that course of action as part of a continuous loop. The idea originated from within the context of aerial combat where everything was immediate, in the now, and measured in seconds and milliseconds. It has since grown to encompass processes and concepts at the operational and strategic levels as well as the tactical, the only difference is the matter of time horizons.

Traditionally, the United States has been very good at observing and acting, but continues to develop its ability to orient and decide, especially in light of the deluge of data and information generated by modern command and control systems and sensor networks. The quicker first and second "O"s are, the more responsive decision-making and acting processes are. Theoretically, it is better to avoid tight coupling to support Modular Open Systems Architecture (MOSA) which decouples the first "O" from the second. MOSA ensures each temporal step or sub-step of the OODA loop is scalable due to its independence from adjacent temporal step or sub-step. A visualization of the OODA loop can be found in Figure 2.

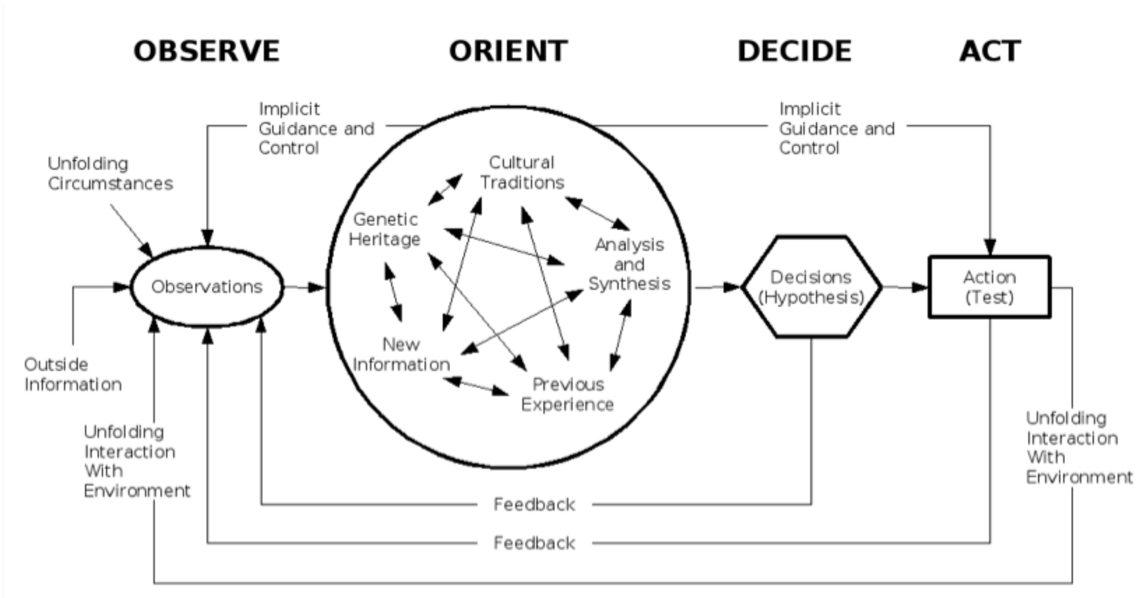


Figure 2. Boyd's OODA Loop. Source: Coram (2004).

D. COMMAND AND CONTROL

Command and control (C2) is defined as "the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of mission" (JCS, 2017, pg. 15). Commonly misattributed as a technological function, C2 is actually a combination of two very separate and distinct concepts. These concepts then enhanced through the use of technology and specific employment methodologies such as mission command (U.S. Marine Corps [USMC], 1996).

1. Command

Command can be seen as the "art" portion of command and control which consists of a combination of legal authorities and the way by which a commander exercises those authorities. It is important to understand the art of command to better understand the relative science of control. Simply put, command is the doctrinal assignment of authority over subordinates by virtue of position or rank. Authority, responsibility, decision making and leadership are the core elements of command (Department of the Army [DA], 2019).

a. Authority

Authority is “the right and power to judge, act, or command” (DA, 2019, pg. 36). A key feature of the concept of command is that authority is delegated by law to an individual, not a staff or organization. This is the cornerstone by which all other elements of command are derived. Authority come in two forms, legal and personal. As previously stated, legal authority is delegated to an individual by a superior as provided for by law or regulation. Personal authority is in large part based on interpersonal relationships, trust, and confidence in the actions of the commander. With due consideration for ability and competence, authority may be delegated to subordinates in the execution of duties assigned, however the commander remains accountable for any successes, failures, and decisions made in their name.

b. Responsibility

Responsibility, on the other hand can be viewed as the commander’s legal and ethical accountability for his/her action or inaction as well as those of his/her subordinates (DA, 2019). Unlike authority, responsibility and accountability cannot be delegated.

c. Decision Making

Decision Making is the application of the commander’s understanding of the art and science of war to determine a course of action for a given situation. Often faced with imperfect information, commanders must rely on their skill and experience to make the best decision for a given situation in a timely manner. “Striking the balance between acting now with imperfect information and acting later with better information is essential to the art of command” (DA, 2019, pg. 37). Key to decision making is the concept of understanding which is exemplified by the four levels of meaning for decision making as shown in Figure 3.

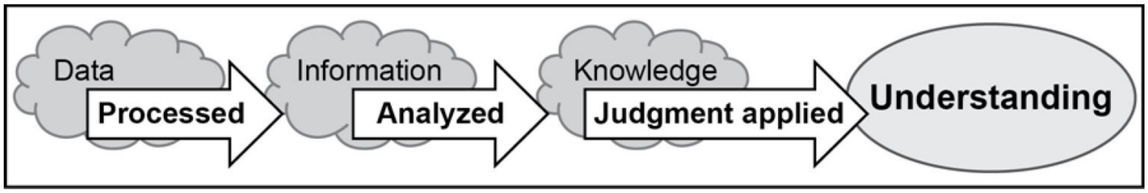


Figure 3. Four Levels of Meaning for Decision Making. Source: DA (2019).

Effective decision making relies on an understanding of the operational environment or situation. Situational understanding is "the product of applying analysis and judgment to relevant information to determine the relationships among the operational and mission variables" (DA, 2019, pg. 37). In the context of decision making, understanding is the end result of the data, information, knowledge chain.

(1) Data

Data is "unprocessed observations detected by a collector of any kind" (DA, 2019, pg. 98). Data can be generated by a number of sources including human intelligence, sensors, and simulations. Typically, data in its raw form has limited usefulness to a commander without further processing as it lacks context and meaning.

(2) Information

Information is "data that has been organized and processed in order to provide context for further analysis" (DA, 2019, pg. 99). For example, a group of sensors could be placed to collect similar data points across a geographic location. This data becomes information when it has been analyzed, labeled, categorized, displayed, or otherwise placed in the context of the operational environment.

Information quality is a key requirement for effective decision making and is described by the Joint Communications Publication JP 6-0 as having the following seven elements (Joint Chiefs of Staff [JCS], 2019):

1. Accuracy. Provides a true representation of a given event or situation that is correct and precise to level required.

2. Relevance. Possesses the quality or state of being appropriate and applicable to a given situation.

3. Timeliness. Information is available in time to affect the decision-making process.

4. Usability. Presented in a way that provides benefit to a user within a given context which facilitate understanding or further analysis using common formats.

5. Completeness. The state or condition of having all information relevant to making a decision.

6. Brevity. Information that has only the level of detail required, concise.

7. Security. Confidentiality, integrity, and availability.

Information can take a variety of forms including a single plot on a common operational picture (COP) system, an entry in a report representing the relative strength and composition of a specific or group of units, environmental conditions of a certain location and so on.

(3) Knowledge

Knowledge is “information that has been analyzed and evaluated for operational implications.” (DA, 2019, pg. 99). Knowledge can exist in two forms, tacit and explicit. Tacit knowledge resides within the mind, is largely based on personal experience, training, and skill and cannot be easily imparted on another individual or transferred to an electronic or written medium. Explicit knowledge on the other hand can be expressed in many forms including doctrine, visualization tools, databases, and so on. For the purposes of C2, knowledge can most easily be understood as information that imparts relevant meaning when placed in the context of a situation or operational environment.

(4) Understanding

The concept of understanding is “knowledge that has been synthesized and had judgment applied” (DA, 2019, pg. 100) to comprehend the relationships of an operational environment. Understanding is the culmination of data, information and knowledge that allows a commander to achieve situational awareness (SA) sufficient to make a decision based on relevant information within an operationally relevant timeline.

d. Leadership

Finally, leadership is the "activity of influencing people by providing purpose, direction, and motivation to accomplish the mission and improve the organization" (DA, 2019, pg. 44). While certainly not all-inclusive, leadership within the context of C2 can be summed up as the ability of a commander to achieve understanding of the operational environment, effectively make and convey decisions to subordinates based on the information available, and ensure unity of effort in the execution of those decisions.

2. Control

Control is the ability "to manage and direct forces and functions consistent with a commander's command authority" (JCS, 2017, pg. 58). Once a commander has determined a course of action, control is employed in order to meet commander's intent. Control is largely data driven and relies heavily on the objective analysis of the capabilities and limitations of both friendly and hostile forces in a dynamic environment to appropriately employ forces. The core elements of control can be defined as direction, feedback, information, and communication and are reciprocal in nature as shown in Figure 4 (DA, 2019).

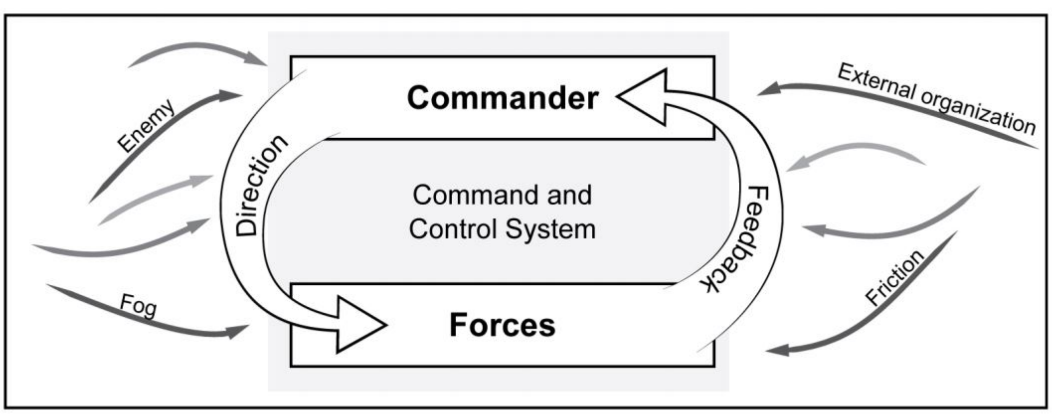


Figure 4. The Reciprocal Nature of Control. Source: DA (2019).

a. Direction

Direction means to "communicate information related to a decision that initiates and governs actions of subordinate and supporting units" (DA, 2019, pg. 62). This is typically accomplished through the use of plans and orders and can best be understood using the example of a five part situation, mission, execution, administration and logistics, command and signal (SMEAC) format as described in the Marine Corps Planning Process MCWP 5-10 (US Marine Corps [USMC], 2017):

1. Situation. Describes the commander's overall understanding of the operational environment to include the area of operations, adversarial forces, friendly forces, disposition of the population, assumptions, and legal considerations.

2. Mission. Purpose of the operation. Provides the who, what, where, when, why, and as much of how as necessary to ensure command, control, and coordination.

3. Execution. Provides commander's intent, concept of operations, explicit tasks, reserve forces, commander's critical information requirements (CCIR), and coordinating instructions.

4. Administration and Logistics. Sets requirements for personnel management, transportation, provisioning, and all related sustainment activities.

5. Command and Signal. Establishes command relationships, locations of command posts and headquarters, and provides a high-level overview of communications requirements.

b. Feedback

Feedback is essentially the reciprocal function of "direct" which includes the information that is fed back to the commander which enables him/her to track the progress of an operation and make any required adjustments as the understanding of a situation evolves. Feedback is critical for identifying possible issues and opportunities in a dynamic and ever-changing environment.

c. Operational Information

Operational information is quite literally the lifeblood that feeds all other elements of C2. Information can come from many different sources and can vary greatly in quality, relevance, and latency. As Carl von Clausewitz famously observed "Many intelligence reports in war are contradictory; even more are false; and most are uncertain…reports turn out to be lies, exaggerations, errors, and so on" (Clausewitz, 2006, pg. 64). For the purposes of C2, information can be divided into operational and mission variables.

Operational variables are those variables used to develop an understanding of the overall operational environment. ADP 6–0 describes operational variables in the form of the mnemonic "PMESII-PT" which stands for political, military, economic, social, information, infrastructure, physical environment, and time as shown in Table 1.

Table 1. Operational Variables. Source: DA (2019).

Variable	*Description*
Political	Describes the distribution of responsibility and power at all levels of governance—formally constituted authorities, as well as informal or covert political powers
Military	Explores the military and paramilitary capabilities of all relevant actors (enemy, friendly, and neutral) in a given operational environment
Economic	Encompasses individual and group behaviors related to producing, distributing, and consuming resources
Social	Describes the cultural, religious, and ethnic makeup within an operational environment and the beliefs, values, customs, and behaviors of society members
Information	Describes the nature, scope, characteristics, and effects of individuals, organizations, and systems that collect, process, disseminate, or act on information
Infrastructure	Is composed of the basic facilities, services, and installations needed for the functioning of a community or society
Physical environment	Includes the geography and manmade structures, as well as the climate and weather in the area of operations
Time	Describes the timing and duration of activities, events, or conditions within an operational environment, as well as how the timing and duration are perceived by various actors in the operational environment

Mission variables are more focused on a specific area of operations and often represent data at a more specific or granular level. A brief summary of some possible mission variables can be found in Table 2.

Table 2. Mission Variables. Source: DA (2019).

Variable	***Description***
Mission	Commanders and staffs view all of the mission variables in terms of their impact on mission accomplishment. The mission is the task, together with the purpose, that clearly indicates the action to be taken and the reason therefore. It is always the first variable commanders consider during decision making. A mission statement contains the "who, what, when, where, and why" of the operation.
Enemy	The second variable to consider is the enemy's dispositions (including organization, strength, location, and tactical mobility), doctrine, equipment, capabilities, vulnerabilities, and probable courses of action.
Terrain and weather	Terrain and weather analysis are inseparable and directly influence each other's impact on military operations. Terrain includes natural features (such as rivers and mountains) and manmade features (such as cities, airfields, and bridges). Commanders analyze terrain using the five military aspects of terrain expressed in the memory aid OAKOC: observation and fields of fire, avenues of approach, key and decisive terrain, obstacles, cover and concealment. The military aspects of weather include visibility, wind, precipitation, cloud cover, temperature, and humidity.
Troops and support available	This variable includes the number, type, capabilities, and condition of available friendly troops and support. These include supplies, services, and support available from joint, host nation, and unified action partners. They also include support from civilians and contractors employed by military organizations, such as the Defense Logistics Agency and the Army Materiel Command.
Time available	Commanders assess the time available for planning, preparing, and executing tasks and operations. This includes the time required to assemble, deploy, and maneuver units in relationship to the enemy and conditions.
Civil considerations	***Civil considerations* are the influence of manmade infrastructure, civilian institutions, and attitudes and activities of the civilian leaders, populations, and organizations within an area of operations on the conduct of military operations.** Civil considerations comprise six characteristics, expressed in the memory aid ASCOPE: areas, structures, capabilities, organizations, people, and events.

Given that operational variables tend to be used at the operational level while mission variables tend to have more relevance at the tactical level, it is important to note that these two are not mutually exclusive. In fact, a tactical unit that has a good understanding of the overall operational environment is arguably in a better position to meet commander's intent in the event opportunity or adversity presents itself. Likewise, there are times that an operational planner would benefit from more specific information provided by mission variables.

One should be aware that more information is not always better. Analysis paralysis is a common issue that can occur as the amount of available information exceeds the ability to effectively processes it. Further, the act of seeking information can lead to undesirable consequences. For example, excessive requests for information (RFI) or onerous reporting requirements can create inefficiencies within both superior and subordinate units. In this situation, processes may be duplicated or irrelevant information may be presented which negatively affects the commander's exercise of effective C2. A thorough understanding of the relationship among data, information, knowledge, and understanding as well as the ways these elements are obtained is essential to understanding the "information" portion of control.

(1) Commander's Critical Information Requirements

One way to overcome excessive reporting requirements is through the use of commander's critical information requirements (CCIR) which are defined as the "elements of friendly and enemy information the commander identifies as critical to timely decision making" (JCS, 2017, pg. 47). CCIRs accomplish two primary functions. First, CCIRs are used to provide the commander with understanding of the operational environment. Second, they assist the commander in the decision-making process by linking CCIRs with decision points (Joint Chiefs of Staff [JCS], 2020a). A general overview of the CCIR process is shown in Figure 5.

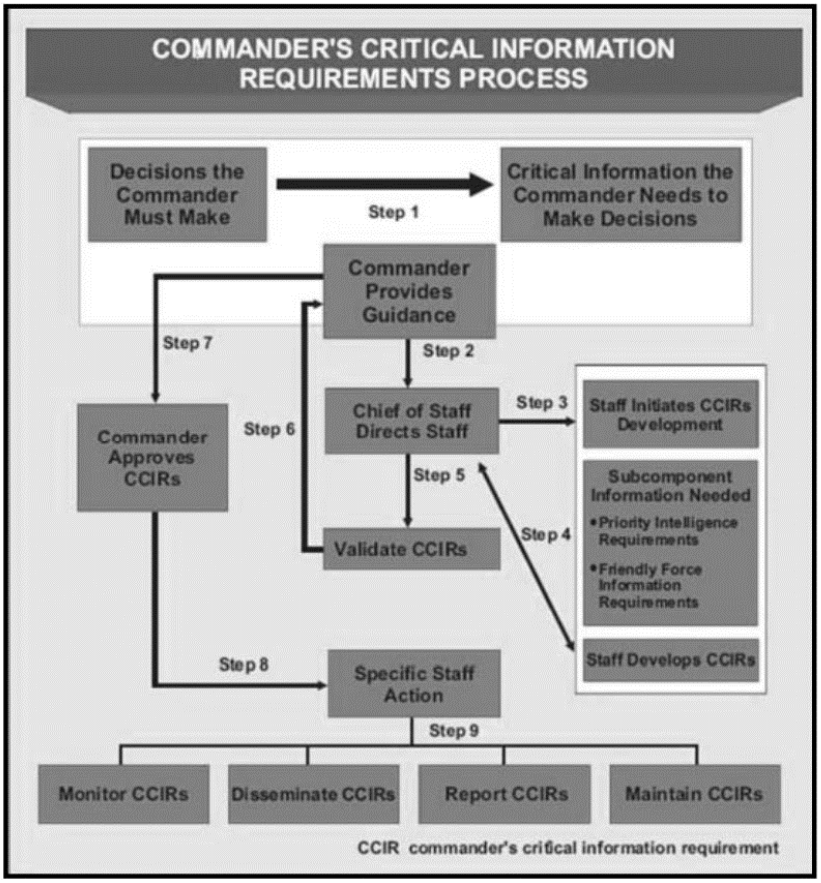


Figure 5. The Commander's Critical Information Requirements Process Source: JCS (2020a).

Properly defined CCIRs can help to optimize the allocation of collection resources, as well as limit the type and volume of information reported to that which has been deemed relevant to the commander. Any additional information required by the commander must generally be obtained through an RFI process.

For example, an operational commander might not find the movement of an individual hostile infantry unit relevant unless it presents a risk to the overall mission. Conversely, a tactical commander may find the same movement extremely relevant as it could directly impact an action for which he/she is responsible. In this situation, the tactical commander may determine individual unit movements are a CCIR and require subordinate reporting, whereas the operational commander may determine that individual unit movements only meet CCIR if it poses a certain level risk, e.g., an anti-aircraft battery moving into a position which presents a new threat to the ingress and egress of friendly forces.

Once approved by a commander, CCIRs are generally integrated into the staff's watch standing function which then ingests various reports and assesses their applicability to CCIR requirements. The entire process can be tedious and often requires a watch to spend an inordinate time and attention in an effort to sort through incoming information. This could further contribute to an overall increase in cognitive load which could lead to a loss of situational awareness as an individual is overwhelmed by the volume of incoming information (Clarke & Knudson, 2018). Recent data processing advances suggest that digitizing CCIRs might result in automated agents which could provide watch standers proactive CCIR alerts, decreasing their cognitive load.

(2) Priority and Friendly Force Information Requirements

CCIRs are further classified into priority information requirements (PIR) and friendly force information requirements (FFIR). A PIR is defined as "an intelligence requirement that the commander and staff need to understand the threat and other aspects of the operational environment" (Joint Chiefs of Staff [JCS], 2013, pg. 26) and are most commonly associated with information regarding enemy forces or other characteristics of the operational environment (DA, 2019). A subset of PIRs are essential elements of information (EEI) which are "the most critical information requirements regarding the adversary and the operational area needed by the commander to assist in reaching a decision" (JCS, 2013, pg. 26).

(3) Friendly Force Information Requirements

FFIRs, on the other hand, is "information a commander and staff need to understand the status of friendly force and supporting capabilities" (JCS, 2017, pg. 214). This can include items such as disposition, location, and strength of friendly forces relevant to the commander's decision-making process. Another crucial factor is the logistic status of various forces, especially fuel and weapons.

(4) Request for Information

Requests for information are “any specific time-sensitive ad-hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence [or operational] production” (JCS, 2013, pg. 141). RFI processes can be either formal or informal in nature and tend to vary greatly by command or location. A formal RFI is submitted to a supporting command for a number of reasons including a formal request for review of a certain plan or document, or to solicit the generation of a product. Formal RFIs typically utilize a system or process which documents the official issuance, receipt, and response to the request from one organization to another. As the name implies, an informal RFI is less structured and often takes place “behind-the-scenes” via email, telcons or other forms of personal communications. The RFI process can be a powerful tool for gathering information, but can also place undue burden on a staff if used too frequently which could result in undesirable outcomes such as inefficiency or a loss of initiative due to perceived micromanagement.

d. Communication

A core function of command and control is communication. Not to be confused with communication systems, communication within the context of C2 can be defined as the process of exchanging information via various methods to facilitate the collection, dissemination, collaboration, and sharing of information and ideas to develop a common understanding in support of planning and execution. Per the ADP 6–0, “Communication links information to decisions and decisions to action” (DA, 2019, pg. 66). Communication can take place in many forms including verbal, nonverbal, and written, which are further enabled through the use of technology, specifically communications and command and control systems.

E. MISSION COMMAND

Mission command is defined as the “conduct of military operations through decentralized execution based upon mission-type orders” (Joint Chiefs of Staff [JCS], 2018, pg. 11). As the definition implies, it is built on a philosophy of centralized command coupled with decentralized control and execution.

Perceived by some as a relatively new term, mission command has a deeply rooted tradition within the maritime domain. Historically, naval commanders were given great latitude to exercise discretion in the furtherance of operational objectives due to the great distances involved and relative inability to “reach back” to higher headquarters for guidance. Perhaps one of the best-known sentiments of mission command is the famous quote by Admiral Horatio Nelson in an address to his commanders on the eve of the Battle of Trafalgar where he said, “in case signals can neither be seen or perfectly understood, no Captain can do very wrong if he places his Ship alongside that of the enemy.” This declaration captures the essence of mission command by simplifying his operational intent into a single, concise statement.

Fast-forward to the present day, where despite advances in communications and C2 systems across the joint force, the proliferation of communications-denial capabilities threatens the ability to maintain robust, reliable C2 networks. Such a loss could result in the inability of a commander to maintain the same level of control previously enjoyed in a more permissive environment, necessitating the need for a mission command approach.

At its core, mission command seeks to exploit the “human element” which requires a thorough understanding of the commander’s intent coupled with the disciplined initiative of subordinate commanders to accomplish mission objectives (JCS, 2020). Of note, care must be taken to ensure decision making is maintained at the appropriate level and not simply delegated to the front-line commander. For this, mission command can be broken down into seven principles: Competence, mutual trust, shared understanding, mission orders, commander’s intent, disciplined initiative, and risk acceptance (Townsend et al., 2019).

1. Competence

Competence is foundational for the proper employment of mission command. Education, experience, and training play key roles in the professional development of a force capable operating at the highest levels of tactical and technical proficiency.

Competence can be expressed in many ways, but for the purposes of mission command, it comes down to ability of a servicemember to understand his/her taskings and to properly execute assigned tasks.

2. Mutual Trust

Mutual trust is "shared confidence between commanders, subordinates, and partners that they can be relied on and are competent in performing their assigned tasks" (DA, 2019, pg. 19). Trust is crucial to the chain of command in that a commander must have faith in the ability of his/her subordinates to execute in accordance with instructions. This enables them to then delegate accordingly, based on past performance and their perceived ability to execute in the future. Of course, trust is not, and should not be given by default. Discretion must be exercised, and trust given on the basis of demonstrated ability commensurate with the level of responsibility to be placed on the subordinate. For example, one may trust an E-5 to lead a platoon on a routine patrol, however the same E-5 may not be capable of overseeing a multi-platoon operation without further training and experience. Trust is developed over time through consistent performance and the demonstration of sound judgment. Similarly, a commander must also work to gain the trust of his/her subordinates. While commanders generally enjoy a baseline level of trust by virtue of their position, they too must develop trust over time. Trust among superiors and subordinates as well as between various organizations based on a common understanding of the operational environment and mission objectives greatly enhances the effectiveness of an organization.

3. Shared Understanding

Per the ADP 6–0, "A critical challenge for commanders, staffs, and unified action partners is creating shared understanding of an operational environment, an operation's purpose, problems, and approaches to solving problems" (DA, 2019, pg. 20). Shared understanding relies on common training, vocabulary, doctrine, and information to achieve a baseline level of knowledge to enable collaboration, planning and operations. A visual representation of shared understanding is shown in Figure 6.

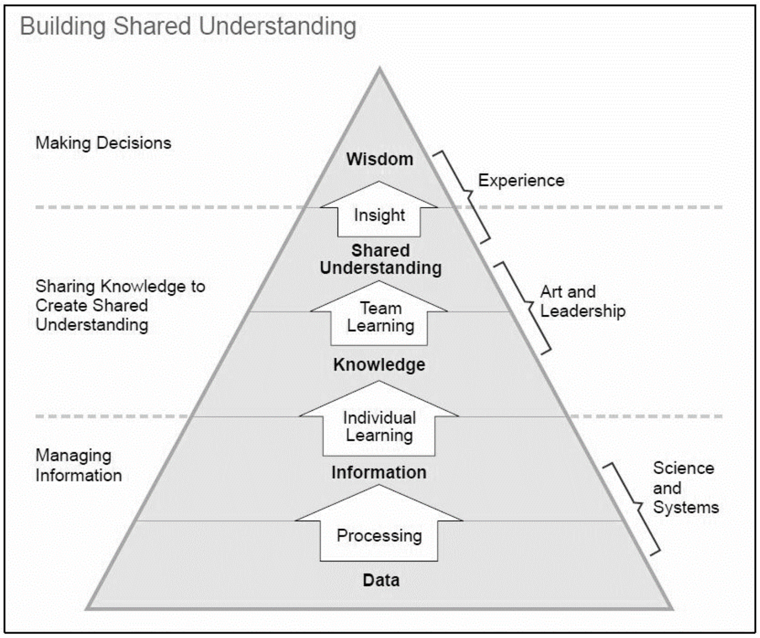


Figure 6. Building Shared Understanding. Source: JCS (2017).

Additionally, the concept of shared understanding can be further divided into situational awareness and situational understanding. Situational awareness is a perception of facts relevant to a given circumstance which provides the individual with a sense of "what" is happening (Hill & Niemi, 2017). Situational understanding answers the questions of "so what?" and "now what?" by applying judgment, in the form of insight, foresight, and critical analysis to achieve awareness of the context, consequences and implications of an event (Lovering, 2014). A more detailed visualization of the relationship between situational awareness and situational understanding is shown in Figure 7.

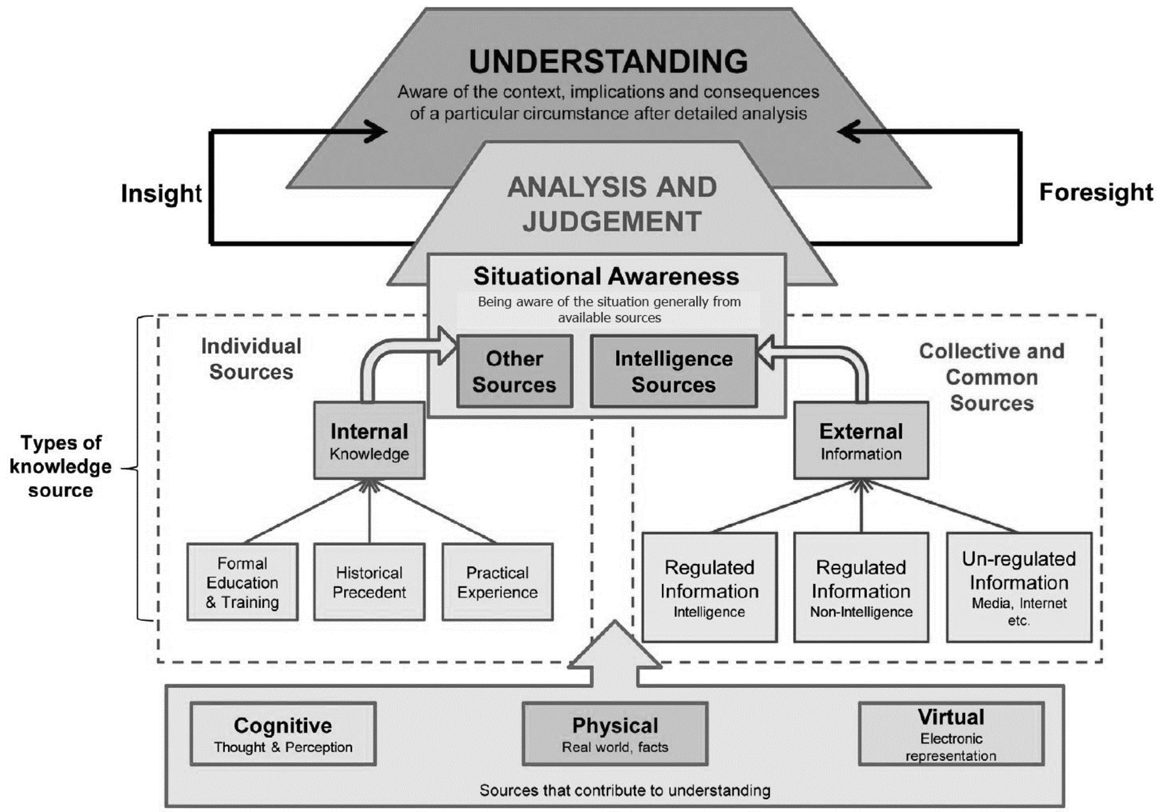


Figure 7. Situational Awareness to Situational Understanding.
Source: Lovering (2014)

Implicit in this model is that each level of awareness builds upon the next. Lack of quality, granularity, or depth will reduce the overall level of understanding one can achieve within a given context. While professional development, education, and competence can vary widely from person to person, technology continues to play an increasingly vital role in the creation, analysis, and distribution of knowledge in support of shared understanding.

4. Mission Orders

Mission orders are directives that provide clear guidance on a desired result or end-state, not specifics on how to attain or achieve those objectives. Mission orders support the core element of "direction" of the concept of control. Competence, shared understanding, and mutual trust play key roles in the development on mission orders. As previously discussed, the situation, mission, execution, administration and logistics, and command and signal (SMEAC) format provides a useful method for conveying mission-type orders to subordinate units, however units can also receive mission orders across a range of formal and informal mediums.

The key to effective mission orders is to provide enough detail to achieve a common understanding of the operational environment, mission objectives, constraints (must do), restraints (can't do), logistics, available, communications links, reporting requirements, organization, and command relationships, to enable subordinate activity and initiative but not so much detail that it unduly stifles a subordinate's ability to exercise his/her own command authority and freedom of action.

Due consideration must be given to various elements including the nature of the operation, associated strategic and political concerns, as well as the anticipated availability of communications, and the ability of a subordinates to make informed decisions based on their level of situational understanding (Hill & Niemi, 2017). For example, routine boarding operations in the Arabian Gulf may permit a commander to grant a higher level of autonomy to a subordinate than could be given to the leader of a direct-action mission within a hostile or otherwise politically sensitive area (e.g., Operation Neptune Spear) where the front-line commander may not have knowledge of all the pieces in play or the strategic implications of his or her decisions.

5. Commander's Intent

Commander's intent is a "clear and concise expression of what the force must do and the conditions the force must establish to accomplish mission" (JCS, 2017, pg. 211). While there is no agreed upon requirements for commander's intent, it generally includes statements of purpose, method, risk, and end-state. This allows staffs and subordinate commands to focus their efforts through insight into a commander's line of thinking to enable initiative and decision making without further orders in the event an operation does not progress as planned. And since no plan survives contact with the enemy intact, it is critical to understand what to do when the circumstances change.

6. Disciplined Initiative

Disciplined Initiative is "the duty individual subordinates have to exercise initiative within the constraints of the commander's intent to achieve the desired end state" (DA, 2019, pg. 24). Essentially, a subordinate is expected to execute in accordance with the plan, until evolving circumstances require a change or an opportunity presents itself to further mission objectives in accordance with commander's intent.

7. Risk Acceptance

Risk acceptance is the end result of the risk management process which seeks to "identify, assess, and control risks and make decisions that balance risk cost with mission benefits" (JCS, 2021, pg. 193). Due to the nature of military operations in a dynamic environment, risk is always present as a result of both anticipated and unanticipated actions by the enemy, friendly forces, or even third parties. In the context of mission command, a commander must be prepared to accept a certain level of risk and effectively convey this tolerance to subordinate commands. A prime example of the concept of risk acceptance is the letter of instruction by Fleet Admiral Nimitz issued concerning the defense of Midway:

> In carrying out the task assigned in Op Plan 29–42, you will be governed by the principle of calculated risk, which you will interpret to mean the avoidance of exposure of your force to attack by superior enemy forces without good prospect of inflicting, as a result of such exposure, greater damage to the enemy. (Rubel, 2015, pg. 2)

With this single statement, Nimitz demonstrated confidence in his operational commanders' ability to execute the plan while simultaneously empowering them to make calculated risks in accordance with his level of risk tolerance.

F. COMMAND AND CONTROL SYSTEMS

Command and control systems are a specific type of communications system used to collect, process, store, disseminate, and manage information and facilitates the direction, feedback, information, and communication functions for a designated commander over assigned and attached forces in the accomplishment of mission the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of mission.

The Joint Communications System (JP 6-0) outlines the following eight functions for communications systems (JCS, 2019, pg. 28):

1. Acquire: “The introduction of information into the communications system.”

2. Process: “A specified sequence of operations performed on well-defined inputs to produce a specified output.”

3. Store: “The retention, organization, and disposition of data, information, or knowledge to facilitate sharing and retrieval.”

4. Transport: “End-to-end information exchange and dissemination in a global environment.”

5. Control: “The function of directing, monitoring, and regulating communications system functions to fulfill operational requirements within specific performance parameters.”

6. Protect: “Information integrity, secure processing, and transmission with access only by authorized personnel.”

7. Disseminate: “Distribution of processed information to the appropriate users.”

8. Presentation: “Information provided to the user in the method that best facilitates understanding and use.”

Naval C2 systems are broadly defined by PEO C4I PMW 150 as maritime, tactical and support C2.

1. Maritime Command and Control

Maritime systems enable situational awareness and provide a common operational picture for planning and coordination of afloat forces. The Navy’s C2 program of record (POR) C2 system is the Global Command and Control System, Maritime (GCCS-M).

GCCS-M provides near real-time situational awareness and blue-force tracking of the maritime domain. GCCS-M is a legacy system that facilitates the exchange of data and information between more than 75 Navy and joint command, control, computers, communications, cyber, intelligence, surveillance, and reconnaissance (C5ISR) systems which is then processed to produce a common operational picture. First fielded in 1998, GCCS-M has demonstrated great success in providing commanders at all levels with a single, integrated, scalable C2 capability. However, GCCS-M has struggled to keep pace with recent technological advances. Limited by its specialized hardware and software architecture, GCCS has been unable to capitalize on opportunities presented by modern artificial intelligence (AI) and machine learning (ML) techniques, distributed storage methods, and processing power. Further, GCCS requires a significant amount of manual human intervention to maintain communications channels, manage databases, and correlate track data from various sources (Wilson et al., 2016).

The Maritime Tactical Command and Control (MTC2) is a relatively new C2 system which provides battle management aids (BMA) in an effort to "dynamically plan, assess, monitor and execute Distributed Maritime Operations" (Lo, 2021, pg. 9). The overall goal of MTC2 is to synchronize various planning process functions across the unit, strike group and fleet level. Initial decision aid capabilities focus on scheme of maneuver, schedule of events, representation of the operational environment, and force status reporting. Additional functionality is provided using a DevSecOps pipeline to rapidly develop, test, and field incremental capability-based improvements. The system is designed to be "hardware agnostic" and able to operate on standard Navy enterprise networks such as the Consolidated Afloat Networks and Enterprise Services (CANES) and the Navy-Marine Corps Intranet (NMCI) (Lo, 2021).

Additional C2 systems include the naval adaptations of the Army Joint Automated Deep Operations Coordination System (JADOCS) which supports time sensitive targeting, maritime dynamic targeting, and coordinates fires across all phases of the joint targeting cycle and the U.S. Air Force's Theater Battle Management Core System used to generate the joint air tasking order (Lo, 2021).

2. Tactical Command and Control

Tactical command and control (TAC C2) systems focus on achieving battlespace awareness through "the effective use of digital communications and data processing technologies, data links, and track data" (Rutledge, 2021, pg. 3).

As shown in Figure 8, data links are created among the various units using a combination of satellite, line-of-sight, and beyond line-of-sight transmission mediums. Individual platforms employ organic sensors to produce tracks which are then transmitted to other units in the link to extend the operational picture or for further correlation and consolidation by a Joint or Maritime C2 System.

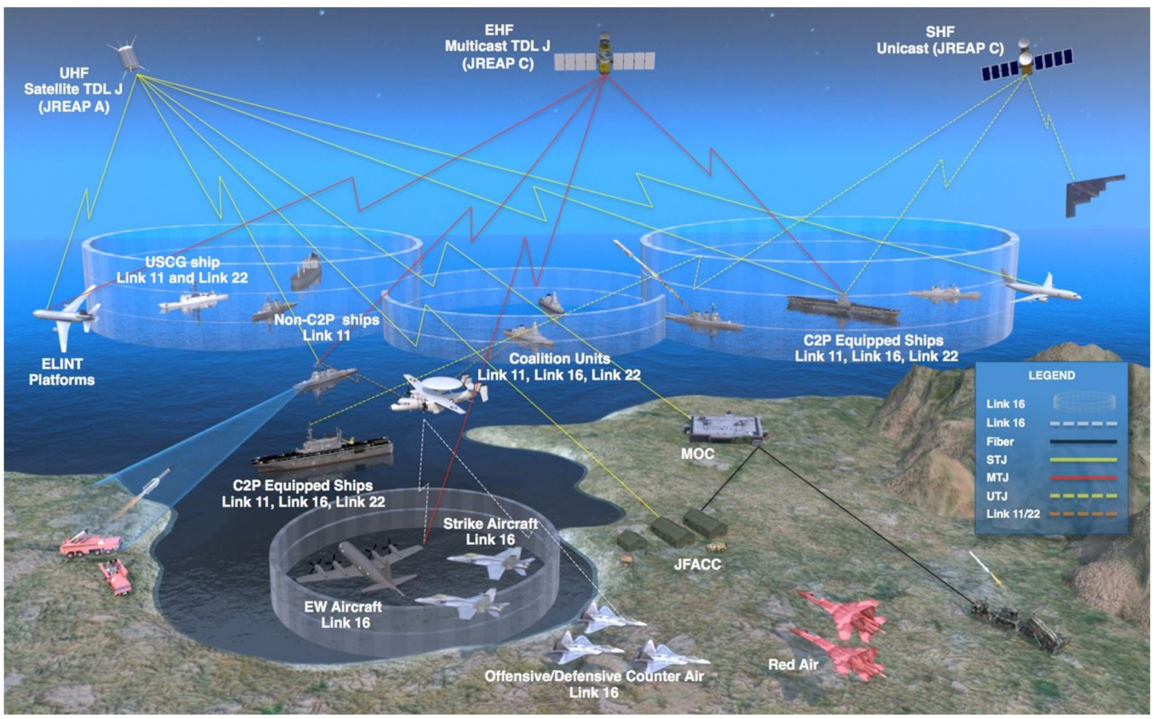


Figure 8. Tactical Data Links, OV1. Source: PMW 150 (2021).

Tactical C2 systems include tactical data links such as Link 11, Link 16, and Link 22 and the systems that manage them including the Link Management Monitoring Tool (LMMT) the Command and Control Processor (C2P), and the Air Defense Systems Integrator (ADSI).

3. Support Command and Control

Support command and control (SUP C2) is essentially a collection of business logistics systems which provide a range of supply, accounting, records management, and material readiness capabilities to the warfighter. Three example of SUP C2 systems are the Naval Tactical Command Support System (NTCSS), the Naval Aviation Logistics Command Information System (NALCOMIS) and the Standard Accounting, Budgeting, and Reporting System (SABRS) Management Analysis Retrieval Tools System (SMARTS).

4. Additional C2 Systems

C2 systems in support of Naval Special Warfare vary by geographic location based on the requirements of the respective theater special operations command (TSOC). Specific systems include the Global Command and Control System – Joint (GCCS-J), the Combined Information Data Network Exchange (CIDNE), the Deployable Common Ground System-SOF (DCGS-SOF), and the Automated Information Discovery Environment (AIDE).

GCCS-J is similar to GCCS-M except that it serves as the DOD's joint C2 system of record. GCCS-J is the primary C2 system used by geographic combatant commanders (GCC), joint task force commanders, TSOCs, and subordinate commands to in support of joint and coalition operations (Defense Information Systems Agency, 2018).

DCGS-SOF is an intelligence, surveillance, and reconnaissance (ISR) system used to provide planning, direction, collection, processing, exploitation, and dissemination functions in support of SOF operations at the operational and tactical level. The DCGS-SOF system is able to task, control, and collect data from multiple platforms including the RQ-4 Global Hawk, MQ-1 Predator, and organic capabilities. This data can then be fused with feeds from the intelligence community and other sources to provide timely, actionable, all-source intelligence products for SOF units and mission partners (United States Special Operations Command, 2014).

CIDNE is a C2 system which processes information about people, facilities, and organizations to track spheres of influence within region. Initially developed by the U.S. Army in conjunction with CENTCOM for managing contacts with high level personnel, but later found success in counter improvised explosive device (IED) operations (Vassiliou et al., 2011). CIDNE is currently used by the Special Operations Command, Pacific (SOCPAC) to receive and distribute mission reports which can be correlated with GCCS-J tracks to provide additional context and a more wholistic view to the common operating picture.

Finally, the AIDE is an all-domain command and control system used to process, exploit, integrate and disseminate information. AIDE applications provide red and blue force tracking, medical, visualization, and workflow services in a real-time environment. Special features are global storage with real-time distribution, cross-domain information sharing, AI/ML object detection and characterization, text translation and operations, intelligence, medical and logistics integration (Novetta, 2020).

5. Command and Control System Concerns

Despite tremendous advantages derived from current C2 systems, their continued reliance on specialized hardware, software, and data structures developed by multiple vendors and services, cause significant problems with interoperability, data silos, and cross-domain solutions. Interoperability is defined as the ability of a system or application to exchange and make use of information with another system or application. Differences in equipment, implementations of standards, or even operational procedures can result in a failure to communicate critical information over designated C2 channels.

A data silo occurs when information is isolated within a certain system due to process or technological barriers. For example, a modern radar system produces an enormous amount of data (position, altitude, bearing, speed, direction, signal quality, time, etc.) for all contacts which are processed and evaluated locally to identify contacts which meet specific criteria relevant to the context of the situation. Contacts that are considered relevant are turned into tracks and pushed out over the link to other units. Those that do not meet threshold criteria are usually discarded or stored locally. Data silos can also occur due to a process or reporting format, e.g., an intelligence report which provides detailed information on an event but is not machine readable precluding any opportunity to conduct advanced historical, operational, or pattern of life analysis techniques. Non-interoperability issues at the knowledge and understanding ladders of a pyramid are due to a lack of context and common understanding of a meaning of entities and events.

Security classification plays a key role in the ability to effectively share information. Typically, naval C2 is executed at the SECRET level which can prove problematic when attempting to coordinate with joint or multinational partners. To illustrate this point, during a recent presentation at the Naval Postgraduate School, the USSOCOM Commander remarked that he has four computers (unclassified, secret, top secret, and international) on his desk alone which he must constantly monitor in order to maintain situational awareness.

The current generation of cross-domain solutions and declassification processes are extremely tedious and limited in their ability to facilitate communications across classification levels regardless of the actual classification of the information. Further, information can sometimes be classified at a higher level than otherwise warranted due to the default classification level of the sensor or method of collection.

G. EMERGING TECHNOLOGIES

Several emerging technologies suggest that changes to how command and control will be conducted or supported may change in the near future. Four emerging technologies may force adaptions for the NSW approach to command and control.

1. Unmanned Systems

Sometimes called autonomous systems, unmanned systems are aerial, ground, and submersible platforms designed to perform tasks with little to no human intervention. Often used to perform jobs deemed dull, dirty, dangerous, or distant, unmanned systems have grown increasingly important in the NSW community as a force-multiplier to augment a traditionally small group of highly skilled professionals. Unmanned systems can support a number of Joint Capability Areas including Force Battlespace Awareness, Force Application, and Logistics (Joint Chiefs of Staff [JCS], 2018a).

a. Battlespace Awareness

Battlespace Awareness, as previously discussed, is the use of sensors and data links to develop situational awareness within a given domain. Future unmanned systems will continue to improve our ability to gain knowledge and understanding of the operational environment by producing increasingly detailed information at an exponential rate. Currently, the vast majority of the information produced by unmanned sensor networks is discarded or otherwise inaccessible for further analysis which misses a tremendous opportunity for the extraction, categorization, and exploitation in support of timely, relevant, comprehensive, and accurate decision-making processes. In addition to sensors, unmanned systems can be utilized to field rapid, ad-hoc communications capabilities to an operational area if existing capability is compromised or otherwise unavailable.

b. Force Application

Force application is supported through the use of an unmanned system to deliver a kinetic or non-kinetic effect. Kinetic effects include the employment of ordnance or munitions to disable or destroy a given target. Non-kinetic effects include various less-than-lethal capabilities such as radio-frequency jamming. Inherent in force application is the concept of the kill-chain, and how to exercise C2 throughout the joint targeting cycle to effectively match missions of shooters-to-targets.

c. Logistics

Sometimes overlooked is growing potential for unmanned systems in military logistics. Over the past ten years, the Department of Defense has invested heavily in unmanned transportation which provides a safer, more reliable, less human intensive alternative to traditional means of delivery. One successful program was the United States Marine Corps' K-MAX unmanned autonomous cargo helicopter which conducted approximately 1,730 resupply missions across Afghanistan to deliver over four million pounds of supplies (Haddick, 2016).

In the maritime domain, the U.S. Navy testing a high-endurance, multi-mission underwater submersible known as the Large Displacement Unmanned Underwater Vehicle

(LDUUV). The LDUUV can be deployed from a host submarine and features reconfigurable payloads which can provide a covert option for the automated delivery of supplies to rendezvous with SOF elements at a pre-determined location. Another intriguing method of delivery is the use of micro unmanned aerial vehicles to "deliver high-value items such as medical supplies, vaccines, cash…to deliver routine supply classes to combat outposts, patrols, and remote guerilla and SOF operator sites" (Haddick, 2016, pg. 28).

2. Artificial Intelligence and Machine Learning

With the exponential explosion in data, communications, and processing power since the turn of the century, artificial intelligence (AI) and machine learning (ML) have become nearly ubiquitous across a range of industries including healthcare, agriculture, retail, education, finance, research, logistics and is becoming increasingly prevalent in the defense sector. The 2018 Department of Defense Artificial Intelligence Strategy defines artificial intelligence as "the ability of machines to perform tasks that normally require human intelligence" (Department of Defense [DOD], 2018, pg. 5) such as perception, cognition, reasoning, and decision making. ML is a subset of AI which uses automated techniques that allow systems to learn from a given dataset, identify patterns, and make decisions with minimal human intervention.

a. Three Waves of Artificial Intelligence

The Department of Defense has been a strong supporter of AI/ML research and development, most notably through a number of research initiatives led by the Defense Advanced Research Projects Agency (DARPA) beginning in 1958. DARPA's leadership ushered in a "golden age" of AI research which led to the establishment of AI as a formal discipline. This laid the foundation for tech giants such as Amazon, Google, Facebook, and Microsoft to develop commercial products across a wide range of industries including healthcare, agriculture, retail, education, financial services, marketing, research, and logistics. DARPA has described AI as occurring in three separate waves: Handcrafted Knowledge, Statistical Learning, and Contextual Adaptation (Launchbury, 2017).

(1) Handcrafted Knowledge

Handcrafted knowledge is based on rulesets created by engineers which represent knowledge in well-defined domains (Launchbury, 2017). First wave AI systems excel in logical reasoning over narrowly-defined problem sets. The "Cyber Grand Challenge" is an example of leveraging first wave principles to identify vulnerabilities to be exploited or defended against using rule-based analysis in a cyber environment. Similar concepts could be used to support military operations in a number of capacities including operations, planning, and logistics. The principal drawback of a first wave system is that it cannot adapt or learn on its own and must be programmed by a human operator to achieve desired functionality.

(2) Statistical Learning

Statistical learning refers to the use of statistical models created for clearly defined problems and then trained using extremely large datasets. Also known as ML, second wave systems are currently the most popular form of AI in use and are characterized by their ability to make associations through the use of supervised, unsupervised, and reinforcement learning techniques. Second wave AI systems specialize in perceiving and classifying data, but suffer from a lack of context which limits their ability to reason and provide causal insight which can sometimes lead to erroneous errors that are expressed with a high degree of confidence. DARPA and other organizations are currently investing heavily in statistical learning systems that provide new capabilities to the warfighter such as the ability to observe and track global cyber-attacks in real time, manage spectrum usage in increasingly congested environments, and to train and operate autonomous vehicles (Launchbury, 2017).

(3) Contextual Adaptation

The third wave of AI is contextual adaptation which seeks to build explanatory models to describe and eventually predict real-world phenomena (Launchbury, 2017). Third wave systems are built using a contextual model which organizes data not only by specific datapoints, but also by additional attributes which govern how it relates and interacts with other data. These systems use a combination of first wave and second wave principles to learn about their environments over time and then apply that knowledge to further refine their base model to gain additional insight.

b. DOD Implementation of Artificial Intelligence

The DOD established the Joint Artificial Intelligence Center (JAIC) in response to the 2017 National Security Strategy which directed agencies to prioritize emerging technologies to modernize key capabilities. The JAIC quickly published the *Defense Artificial Intelligence Strategy* to formalize a set of initiatives which focus on rapidly incorporating AI in an iterative, responsible manner to enhance the decision-making process within key domains (DOD, 2019). The five initiatives are as follows:

1. Deliver AI-enabled capabilities that address key missions.
2. Scale AI's impact across DOD through a common foundation that enables decentralized development and experimentation.
3. Cultivate a leading AI workforce.
4. Engage with commercial, academic, and international allies and partners.
5. Lead in military ethics and AI safety.

Each initiative represents a monumental undertaking, however, none of this will be possible without first establishing the common foundation which includes establishing repositories of "shared data, reusable tools, frameworks and standards, and cloud and edge services" (DOD, 2019, pg. 7). In a 2020 article, the JAIC explained that much of the data required for the implementation of AI is either not collected, or not stored in a format or location for optimal use (Joint Artificial Intelligence Center [JAIC], 2020), which reemphasizes the previous discussion regarding data siloes.

Often, organizations seek outside assistance to build an AI application only to find out that they do not have the data required for success. The JAIC Joint Warfighting Operations mission lead recently observed "we are tasked with delivering AI capabilities. However, for my team to do that, the force has to meet us part of the way by getting themselves AI-Ready" (JAIC, 2020a, paragraph 2).

To assist, JAIC created a framework which guides service components on ways to prepare their organizations for the integration of AI. This can be achieved through taking steps such as saving data that was previously discarded, standardizing existing data and storing it with similar types, curating and normalizing databases, and cataloguing existing data repositories. Further, new opportunities for data collection should be explored (e.g., data from biometric monitoring devices) to build a historical dataset relevant to the organization. In addition, investments should be made in network, computer, and communications infrastructures that are capable of supporting AI applications (JAIC, 2020a). Additional items for NSW consideration are the use of open architectures, as well as understanding and documenting an organization's processes and workflows.

According to the JAIC, four key questions must be answered when considering data requirements (JAIC, 2020, paragraph 4):

1. What mission challenges are you trying to solve with the large datasets you are bringing into the Joint Common Foundation?
2. What are the intended and potential use cases?
3. What other data do you plan to use and why?
4. What will be the cost to prepare your data for use in AI/ML development?

USSOCOM has taken concrete steps to develop AI/ML and other cutting-edge data techniques with the commissioning of a data engineering lab in Tampa, Florida. Located at the SOFWERX facility, SOCOM is partnering with industry leaders and academic institutions such as Carnegie Mellon University to build a culture that is conducive to embracing state-of-the-art data technologies to address specific problem sets to generate options in support of Joint Force operations.

Ultimately, accurate, well-structured training data sets that are compatible with USSOCOM architectures are essential to further the development of NSW data-driven capabilities such as Digital Mission Command and SOF Connect. Acquiring data after-the-fact is difficult, which means NSW must begin to identify the data they currently have, the data they currently need, and data they may need in the future.

3. Cloud Technology

According to the National Institute of Science and Technology (NIST) cloud implementation is separated into the two broad categories of Deployment and Service Models.

a. Cloud Deployment Methods

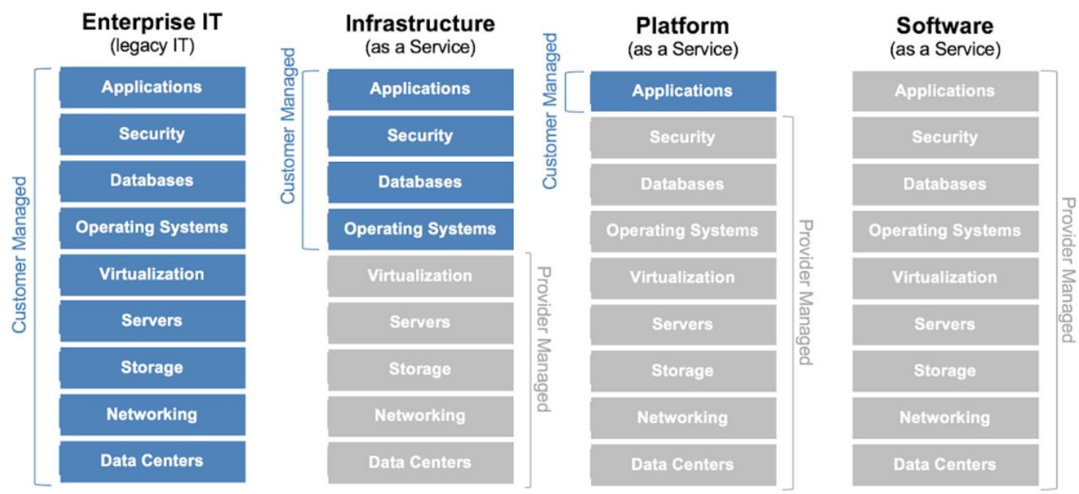
The first is the overall cloud deployment method which is characterized by a combination of the location of the cloud infrastructure relative to the intended user base. Cloud deployment methods can be public, private, or hybrid (Mell & Grance, 2011).

- Public cloud: Infrastructure provisioned for use by the general public and exists on the premises of the cloud provider.
- Private cloud: Infrastructure provisioned for exclusive use by a single organization which may be owned, managed, and operated by the organization or a third party. Private clouds may exist either on or off of the premises of the organization.
- Hybrid cloud: Cloud infrastructure comprised of a combination of public and private clouds. This is normally done to provide for cloud-bursting capability, or to satisfy legal or security requirements.

Another form of cloud deployment being developed is the concept of the Tactical Cloud. Essentially, this means extending cloud services out to the tactical edge (e.g., afloat and expeditionary forward operating units) where communications systems operate using relatively low data-rate, high-latency, unstable networks, typically over a satellite communications (SATCOM) link which inherently limits the richness of media that can be exchanged. Tactical clouds aim to provide the benefits of cloud services in an austere environment.

b. *Cloud Service Models*

The second broad category further refines cloud scope into three service levels known as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) (Mell & Grance, 2011) as illustrated in Figure 9.



Source: https://cic.gsa.gov/basics/cloud-security.

Figure 9. Cloud Service Levels.

In this figure, information systems management is broken up into nine separate categories. Starting from the left, legacy information systems are managed exclusively by the customer with management responsibilities gradually shifting to the cloud provider while progressing to the right through the service levels.

c. *Cloud Implementations*

Transition to a cloud-based infrastructure enables the efficient use resources via on-demand provisioning of shared storage, processing, memory, and network resources. Cloud computing also benefits from the ability to observe and implement industry standards and best practices to deliver a full range of services to a broad audience by leveraging commercial technology and distributed computing techniques over high capacity, low latency, stable, and robust networks. Cloud systems are a natural fit for AI/ML applications, big data warehousing, interoperability, and a common user experience.

Current cloud initiatives within the DOD include the Joint Enterprise Defense Infrastructure (JEDI) and the SOF Information Environment (SIE). JEDI is envisioned as the DOD's general, all-purpose enterprise cloud, which leverages commercial technology to deploy a single-source cloud infrastructure in support of operations from garrison to the tactical edge. JEDI will serve as the foundation for fast, flexible, and adaptive cloud services to users across all enclaves to enable efficient data sharing, cross domain solutions, advanced data analytics, and improved cybersecurity (Department of Defense, 2021).

USSOCOM continues to invest in the development of the SIE to provide services similar to JEDI which are tailored to the unique operational requirements of the SOF community. The SIE is managed by the Global Enterprise Operations Center (GEOC), co-located at USSOCOM Headquarters, and connects over 70,000 SOFNET users and 1,200 deployed nodes around the world (Thomas, 2017). Part of this development is the concept of the SOF Hybrid Cloud which according to the USSOCOM Chief Information Officer, Lisa Costa, "leverages hyperconverged infrastructure already on the network to host private cloud and take advantage of commercial cloud providers to host our [provider agnostic] containerized applications" (Stone, 2019, paragraph 5).

4. Advanced Data Strategies and Concepts

The final section of emerging technology focuses on advanced data strategies and concepts used to facilitate the collection, aggregation, storage and analysis throughout all levels of the data, information, knowledge continuum to enable "improved tactical action, faster and more accurate decision making, and adaptive, dynamic planning" (Godin, 2021, pg. 6). Current trends in operational data strategy center around building a robust, interoperable data layer, capable of ingesting and storing all data in a common format, processing and categorizing that data into information, then contextualizing and transforming that information into usable knowledge. As this data layer touches data, information, and knowledge, a more generalized description would be the data, information, and knowledge layer.

a. Relational Databases

Traditionally, data has been collected and stored in relational databases which organize data into a series of interrelated tables with pre-defined relationships. Relational databases work well for finite, two-dimensional, well-structured datasets, however struggle to process rich media (such as the ubiquitous sensor and imagery feeds NSW employs) and are extremely difficult to operate at scale in a cloud environment.

b. Big Data

Next-generation systems are designed to incorporate big data technology to overcome the limitations of traditional data-processing architectures. Big data refers to a process of storage, analysis, and systematic data extraction of information from extremely large datasets which is often described in terms of the "Five V's" which are volume, velocity, variety, veracity, and value. Essentially, the Five V's describe the amount a data a system can handle, how quickly it can process it, what formats it can accommodate, how accurate or true data is, and how useful it is.

Volume and velocity are largely the functions of infrastructure. As previously discussed, big data is closely associated with cloud computing, and is therefore constrained by available processing, networking, and storage resources. Variety on the other hand depends much more on the composition and organization of the data and falls into three main categories: structured, semi-structured, and unstructured.

- Structured. Strictly defined length and format, e.g., a phone-number, latitude / longitude, dates, etc.
- Semi-Structured. Follows a general format but does not conform to a strict format. Log files are an example of semi-structured data often include time-stamps, event numbers, free-form narratives, chat, and other data.
- Unstructured. Does not conform to a standard format or fit easily into a traditional relational database column / raw format. Video, audio, imagery, books, articles, and email communications are examples of unstructured data.

Veracity refers how complete, accurate, and trustworthy data is for a given application. Some applications may require an extremely precise dataset while others may need a less detailed input to achieve a desired result. For example, a C2 system such as GCCS may provide adequate resolution as long as tracks are updated every couple of minutes, whereas a ballistic missile defense system requires a real-time, target-quality input. Finally, value is determined by the relative usefulness of the available data.

c. *Multi-dimensional Databases*

Leading the way in next-generation data handling is multi-dimensional storage. Where relational databases are two-dimensional in nature, organized in a strict hierarchy of constraining pre-defined relationships, multi-dimensional storage integrates the various tables into a single entity comprised of multiple dimensions. This approach provides a data management foundation for information/knowledge exploitation needs, using advanced analytical processes called on-line analytical processing. An additional benefit of this storage method is that these multi-dimensional arrays are able to store and operate over sparse data such as audio, video, and imagery.

d. *Data Strategy in Support of Naval Operational Architecture*

In a recent study entitled *Data Strategy in Support of the Naval Operational Architecture*, Godin describes a revolutionary data strategy for the Navy based on the implementation of a common, scalable, core data management framework, using the multi-dimensional databases. This approach provides the foundation upon which the rest of the data strategy relies. Loading these data into this next-generation storage creates a basis for building a DIK pyramid as the foundation for the DIK layer (Godin, 2021).

A data lake is a cloud-based repository that holds large amounts of raw data in its native form that can then be leveraged by any number of secondary applications to achieve a desired function. Instead of data being stored in a hierarchical system that is organized by files and folders, data lakes use a flat architecture where all data is visible and assigned a unique identifier and labeled through the use of metadata, which is a set of data that describes and gives information about other data. Examples of metadata are data size, date of collection, quality, source, keywords, etc., which are standardized by the use of formally defined vocabularies and component relationships known as ontologies. The key benefit to the use of the data lake format is that it creates an authoritative source of data that is unaltered and considered to be true since no logic, processing, or conversions have been applied. Well-structured multi-dimensional array storage is a natural complement to the data lake as it provides the native ability to slice, dice, and subset incoming data.

Collecting, tagging, and categorizing all available data into properly catalogued data lakes, with embedded well-structured multi-dimensional arrays lays the foundation for advanced AI/ML enabled command and control systems. The use of first, second, and third wave AI principles in support of advanced data analysis will enable an end-state which Godin describes as operators and decision makers being "informed by actionable knowledge, organized around situations, which gives them insights and predictive future states to assist them to make the best possible tactical moves" (Godin, 2021, pg. 67).

H. SUMMARY

This chapter explored the definitions and concepts related to digital mission command. Mission command is a form of command and control. Leaders hypothesize that its use will be crucial to success with near peer competitors. Mission command depends on subordinate leaders understanding the commander's intent through iterative processes with their superiors, and a knowledge environment supported by emerging data technologies, which enable these smaller units to have increased amounts of valuable information at the right time on a right device.

Processes exist to organize that data. Such ideas as CCIRs, PIRs, and RFIs help organize collection and dissemination processes. Each phase of operations from planning to execution to post mission, have their own set of data challenges. These constructs, though, remain useful as organizing principles.

Emerging technologies, such as unmanned systems and new sensors, suggest there will be even more data available to support mission command. Other technologies, such as clouds, AI/ML, and multi-dimensional array storage, offer the promise that Navy Special Warfare will be able to leverage these data in remarkable new ways, ways that make mission command, now digitized, very effective and efficient.

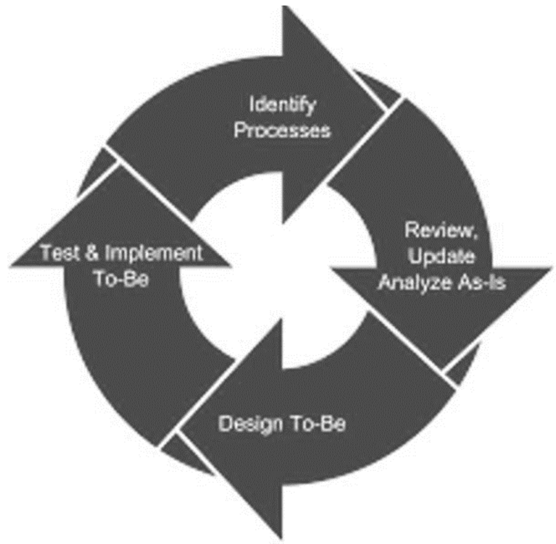
III. RESEARCH METHODOLOGY

A. INTRODUCTION

In Chapter I, this research explored the topic of interest, digital mission command, which laid out a vision of an integrated, assured, and resilient global command and control capability that leverages cutting-edge technology to achieve operational advantage in support of NSW operations in the maritime, littoral, and riverine environments. The research objective was to describe how NSW should proceed from their present state to a digital mission command posture. This is because NSW currently enjoys information dominance the majority of the time which allows for extensive collaboration and support from higher headquarters. With the resumption of great-power competition and rise of increasingly capable state and non-state actors, such assumptions of dominance can no longer be made. Therefore, a return to the tenants of mission command and mission-type orders, enhanced by modern communications and technology, must be relied upon to address this challenge. Chapter II explored a number of topics relevant to this research including the NSW operations, organizational structure, as well as the nature of command and control and mission command and the technologies that enable them. This chapter provides an explanation of the approach needed to move from the current NSW environment to an imagined new world where mission command, supported by the newest capabilities derived from digital readiness, are embraced.

B. APPROACH

Numerous approaches exist to determine how to incorporate emerging technologies into existing organizational processes in order to achieve a more efficient, capable end-state. When selecting an approach, one must consider how the transition is both informed and influenced by the organization's people, processes, and technologies. The Business Process Re-engineering (BPR) cycle addresses all three of these components and is illustrated in Figure 10.



Source: https://en.wikipedia.org/wiki/Business_process_re-engineering

Figure 10. The Business Process Reengineering Cycle

Using this as a starting point, this research effort employed a methodology which consists of identifying processes, analyzing the current environment, imagining the future environment and identifying areas for improvement.

1. Identify Processes

Processes are a set of procedures or steps taken to attain a certain end. Following are the sets of characteristics, functions, or opportunities that drive process.

a. Mission Command

Since this research addresses mission command, Table 3 lists the seven characteristics that apply to NSW operations which should be considered when mapping the current to the future state.

Table 3. Elements of Mission Command. Adapted from DA (2019) and JCS (2017).

Elements of Mission Command	
Competence	Ability to properly understand and execute assigned tasks.
Mutual Trust	Shared confidence among commanders, subordinates, and partners that they can be relied upon to perform as expected.
Shared Understanding	Common awareness of the context, implications, and consequences of a particular situation.
Mission Orders	Orders and directives that coordinate and focus subordinate efforts towards a desired result or end-state, not specifics on how to accomplish those objectives. SMEAC.
Commander's Intent	Clear and concise expression of what the force must do and the conditions the force must establish to accomplish mission.
Disciplined Initiative	Exercise of initiative within the constraints of the commander's intent to achieve the desired end state.
Risk Acceptance	End result of the risk management process where the commander conveys his/her tolerance to residual risk.

b. C2 / Communications Systems Characteristics

Second, since mission command is a form of command and control that is leveraged by the use of technology, ensure the current and future states are compared through the lens of C2 and communications systems characteristics. Regardless of age or sophistication, C2 systems serve eight core functions as described in Table 4.

Table 4. Eight Core Functions of C2 Systems. Source: JCS (2019).

Core Functions of C2 Systems	
Acquire	Introduction of information into the system.
Process	Sequence of operations performed on inputs to produce an output.
Store	Retention, organization, and disposition of data, information, or knowledge to facilitate sharing and retrieval.
Transport	End-to-end information exchange and dissemination.
Control	Directing, monitoring, and regulating of communications system functions to fulfill operational requirements.
Protect	Information integrity, secure processing, and transmission of with access only by authorized personnel.
Disseminate	Distribution of processed information to respective users.
Present	Information provided to the user in a method that best facilitates understanding.

c. Processes supported by Mission Command

There are three main processes associated with mission command: planning, execution, and post mission reporting and analysis.

d. Review of findings

Subject matter experts, faculty, and literature were used to validate assumptions and verify that the details of the previous factors are correct and appropriate to support research objectives.

2. Capture the Current Architecture

The current architecture represents a snapshot in time of a system that is constantly evolving and is different for every situation. This research will establish an understanding of current technologies and procedures using existing tactical publications and technical drawings. Further, it will leverage subject matter experts, faculty and relevant personnel to verify findings and gain additional insight. This architecture is based on information and data available at the unclassified for the purpose of exploring the feasibility of implementing a new data strategy in support of digital mission command NSW operations. It is not intended to represent the entirety of the SOF communications systems, capabilities, or processes.

3. Imagine the Future Architecture

Once the current architecture is understood, the next step is to imagine a new, more effective set of systems and procedures that are informed by emerging technologies and personal experience and expertise. Recognizing that the future environment is anticipated to experience increased disruptions and denials of communications and networking, the future state should account for those obstacles. Table 5 lists the key emerging technologies discussed in Chapter II that research indicates will significantly impact the drive towards a robust digital Mission command capability.

Table 5. Emerging Technologies

Emerging Technologies	
Unmanned Autonomous Systems	Unmanned aerial, ground and submersible platforms designed to perform tasks with little or no human intervention which be used to provide battlespace awareness, force application, and logistic support.
Artificial Intelligence	The use of machines to perform tasks that normally require human intelligence through the use of handcrafted knowledge, statistical learning, and contextual adaptation techniques.
Cloud Computing	Enables the efficient use of resources via on-demand provisioning of shared storage, processing, memory, and network resources.
Advanced Data Architecture/Strategies	Strategies and Architectures which facilitate the collection, aggregation, storage, analysis and dissemination across all levels of the Data, Information, and Knowledge continuum which will serve as the foundation for advanced AI/ML enabled systems.
Advanced Communications Architectures	Next-generation communications architectures or methodologies that enable the assured and resilient end-to-end information exchange and dissemination.

Imagining techniques were augmented by talking to faculty as well as multiple data and operational subject matter experts. Additionally, knowledge gained through numerous Network Operations and Technology curriculum courses served as inspiration for how to effectively integrate emerging technologies.

4. Chapter Summary

This chapter provided an explanation of the approach used in Chapter IV to evaluate the current as-is environment, to a proposed to-be environment that employs emerging technologies in support of the NSW Digital Mission Command initiative.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESEARCH ANALYSIS

A. INTRODUCTION

Chapter I discusses Naval Special Warfare's role within the Special Operations community and its primacy within the maritime, littoral, and riverine environments. Widely regarded as the gold-standard for special operations, the Navy SEAL embodies the spirit of the "silent professional," supported by a world class organization made up of highly trained, motivated, and well-resourced personnel, to project power on, under, and from the sea (DON, 2018). One of the reasons for NSW's continued success over the years is its uncanny ability to adapt, overcome, and thrive in an uncertain and rapidly changing environment. A tremendous accomplishment by itself, one must acknowledge that past performance in no way guarantees future success. Recent socio-economic, geopolitical, and technological trends have painted a dismal picture of the future operational environment where the United States will no longer enjoy the advantages as the world's sole remaining superpower. To this end, NSW must continue to evolve to meet the mounting challenges of future operations.

In Chapter II, emphasis was placed on differentiating between command and control, mission command, and command and control systems. While it is important to know what they are, it is equally as important to understand what they are not. Therefore, a thorough understanding of these three concepts is required to adequately describe their operational and technical relationships. Chapter II also discussed five areas of emerging technology which are projected to have a major impact on special operations. These technologies are broadly categorized as unmanned autonomous systems, artificial intelligence, cloud computing, advanced data architectures/strategies, and advanced communications architectures.

Chapter III provided an analytical framework for this chapter consisting of process identification, determination of NSW's current architecture, imagination of a future architecture which employs emerging technology and a comparison between the two. The results of this comparison will be used to inform current and future NSW efforts to create a robust digital mission command capability.

B. DIGITAL MISSION COMMAND ANALYSIS

1. Command and Control

As discussed in Chapter II, command and control is the "exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of mission" (JCS, 2017, pg. 15) and is a combination of two major functions.

Command and control is a fluid concept which varies by commander, organization, mission requirements, geographic location, and the operational environment. For example, SOF operations in the Pacific AOR requires an emphasis on the core activity of special reconnaissance in a maritime or littoral environment where NSW forces have primacy, whereas operations in the Middle East may focus more on land-based counter-insurgency and counter-terrorism activities in a supporting role as a member of a joint special operations task force (JSOTF).

The current generation of C2 systems primarily focus on the core control functions of feedback, information, and communications. This provides situational awareness to the commander in support of the command function of decision making. Decision making remains a largely manual process whereby an individual or staff will examine available information, apply context, and then make recommendations to the commander for consideration. The flow of data, converted to actionable information, is the lifeblood of decision making.

2. Mission Command

As mentioned before, mission command is a specific method for the employment of command and control, with deep roots within the maritime domain. Mission command employs centralized command and decentralized control and execution, exploiting the "human element" and requiring a thorough understanding of the commander's intent coupled with disciplined subordinate initiative (JCS, 2020).

Despite advances in communications and C2 systems across the joint force, the proliferation of communications-denial capabilities threatens the ability to maintain robust, reliable C2 networks. Such a loss results in the commander's inability to maintain the same level of control enjoyed in a more permissive environment, necessitating the need for a mission command approach.

With a few exceptions, current C2 systems only address the shared understanding aspect of mission command. Futures systems must incorporate additional functionality to enhance the remaining elements of competence, mutual trust, mission orders, commander's intent, disciplined initiative, and risk acceptance.

C. CURRENT ARCHITECTURE

To better visualize the current architecture, it is useful to provide a brief description of the C4I environment. The current environment is largely shaped by the past twenty years of operations which are characterized by the global war on terrorism, regional stability, and low intensity conflicts against a procession of technologically inferior, but highly mobile and adaptive opponents. To address these challenges, the joint force developed an extremely capable C4ISR system which provides unprecedented levels of connectivity, efficiency, and lethality. The current system is heavily dependent on the free flow of information where the satellite communications, overhead imagery, and all-domain superiority within the context of a permissive electromagnetic and cyber environment is, for the most part, assumed.

All of this has provided commanders with the ability to exercise C2 with a speed and fidelity that was previously unimaginable. As a result, many processes and decision-making authorities that were once delegated to lower echelons have been concentrated at higher levels where it is argued that well-manned, well-connected staffs are often in a better position to see the "bigger picture," make better decisions, and provide increased support to ongoing tactical missions.

1. Organizational Relationships

Due to the wide range of missions SOF is called upon to perform, there is no one "standard" operational chain of command. NSW forces normally deploy with three NSWTUs commanded by an O-4, and one NSWTG HQ, commanded by an O-5 (DON, 2018). NSWTEs represent the baseline platoon which is typically an eight-person, O-2 command. While NSW operations normally occur in conjunction with other forces, for the purposes of this research, the operational chain of command refers to the C2 relationships as they relate a notional NSWTG deployed in support of a geographic combatant commander (GCC). The NSWTG, NSWTU, and NSWTE construct was chosen to highlight differences in the size, capability, and function of deployed NSW forces. An example of an operational chain of command is shown in Figure 11.

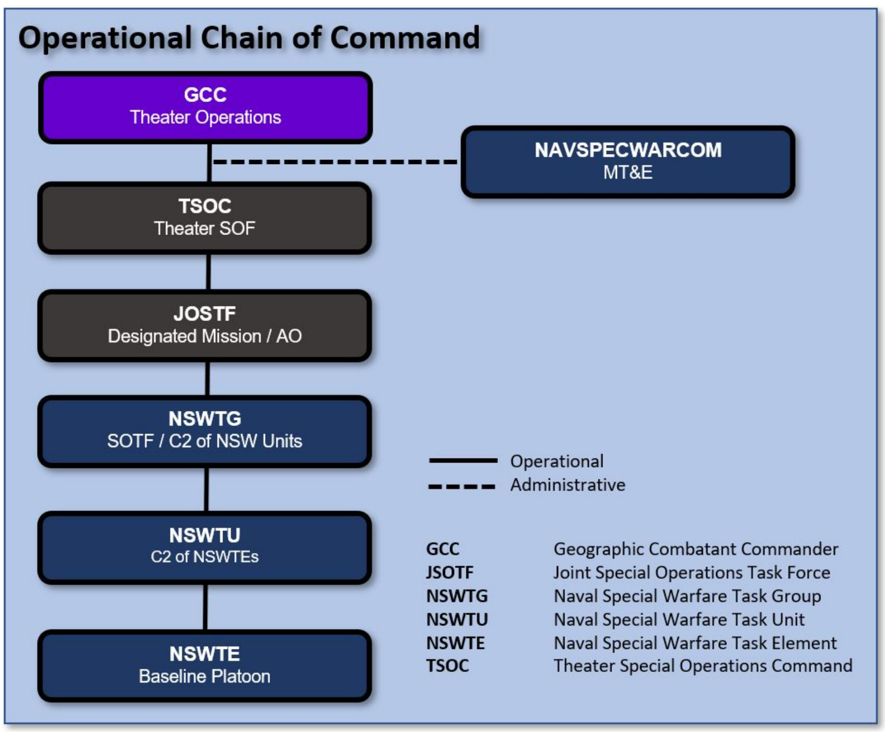


Figure 11. Notional Operational Chain of Command

(1) Strategic / Operational Level

A theater special operations command (TSOC) is a functional sub-unified command organized under USSOCOM. OPCON of deployed SOF units is delegated to the TSOC while USSOCOM retains COCOM. The Secretary of Defense then delegates OPCON of the TSOC to the respective GCC. In this scenario, the primary function of the TSOC is to plan and execute SOF operations on behalf of the GCC and delegates tactical control (TACON) to a JSOTF for execution.

(2) Tactical Level

A JSOTF is an O-6 command composed of SOF units from multiple services that executes SOF activities as directed by the TSOC in support of a specific mission or operational area. The JSOTF may designate additional SOTFs to conduct component-specific operations.

The NSWTG is the NSW equivalent of a SOTF which serves as the headquarters for NSW operations and is comprised of two or more NSTUs. Of note, the NSWTG N6 is responsible for the management and support of all subordinate NSW communications requirements including network operations, communications, computer network defense, and frequency management.

NSWTUs exercise C2 over three or more NSWTEs and are typically forward-deployed to different locations within the operating area to increase tactical reach. NSWTEs represent the tactical edge and may be broken into smaller maneuver elements which may or may not have reliable communications with the main body, even in the best of circumstances.

2. Communications Architecture

NSW is part of an integrated SOF communications architecture, primarily managed by USSOCOM. A high-level overview is provided in Figure 12.

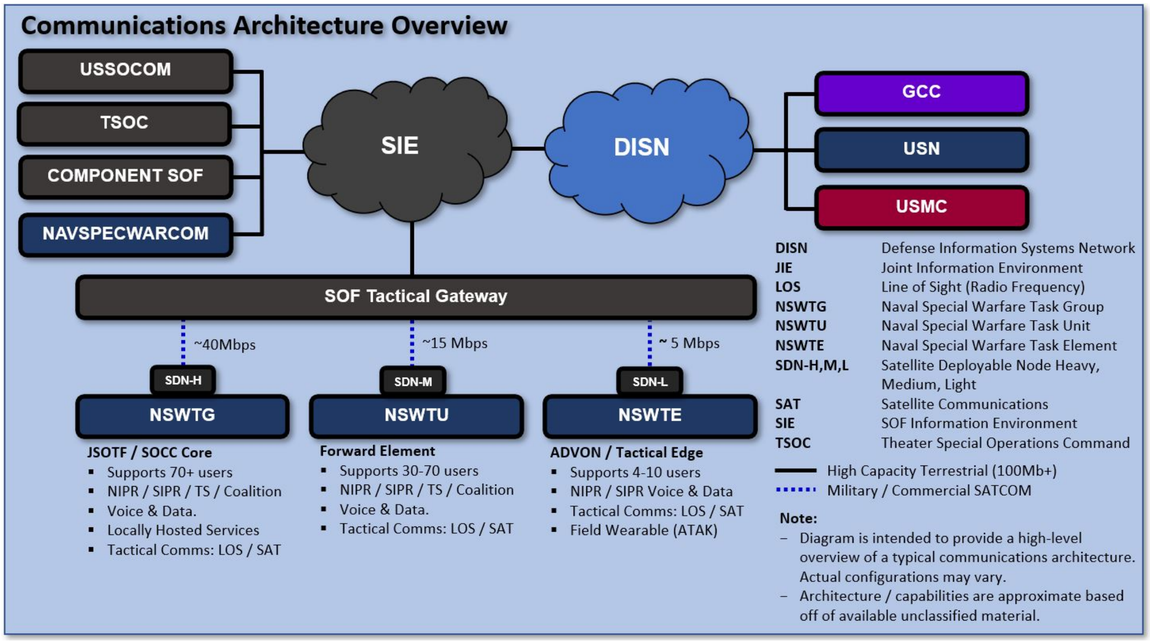


Figure 12. NSW Communications Architecture Overview.

a. SOF Information Environment

The SOF Information Environment (SIE) is the primary network used by the special operations community to process, store, disseminate and present data in support of vital C2 processes. The SIE is a cloud-enabled network that offers a full complement of secret, top-secret, and unclassified services, including SOFNET, to provide a common operating environment for SOF elements. SIE is connected to other DOD, component specific, and external networks via the Defense Information Systems Agency Information Network (DISN). Commands directly connected to the SIE include USSOCOM, NAVSPECWARCOM and the various TSOCs.

b. Satellite Deployable Nodes

Deployed NSW forces are able to access the SIE via a SOF Tactical Gateway. Units establish a satellite link over military or commercial SATCOM with a SOF Tactical Gateway via a Satellite Deployable Node (SDN). SDNs come in three different configurations, light, medium, and heavy, which provide varying levels of service based on the needs of the supported unit. As shown in Figure 12, typical aggregate data-rates range from approximately 40Mbps at the headquarters level down to 5 Mbps at the forward element and can be adjusted based on mission requirements. Decreases in data-rates will result in a corresponding decrease in available services.

SDNs also have the ability to use available tactical infrastructure or commercial internet services providers also known as "dirty" internet to establish virtual private network connection with the Tactical Gateway to establish SIE connectivity. Similar network functionality can be achieved through the use of other mobile communications platforms such as the Tactical Local Area Network (TACLAN) which can use various IP sources to provide scalable network solutions.

c. Communications

Tactical communications links over SATCOM, line of sight (LOS) and beyond line of sight (BLOS) circuits provide additional voice and data capability among the various levels of command, again predicated on C2 and mission requirements. Commonly used radios include the PRC-117G, PRC-160, PRC-163, and the PRC-167.

NSW employs a number of non-traditional tactical capabilities including Radio over IP (RoIP) and Mobile Ad-Hoc Networks (MANET) as shown in Figures 13 and 14 as well as field wearable equipment such as the Android Tactical Assault Kit (ATAK).

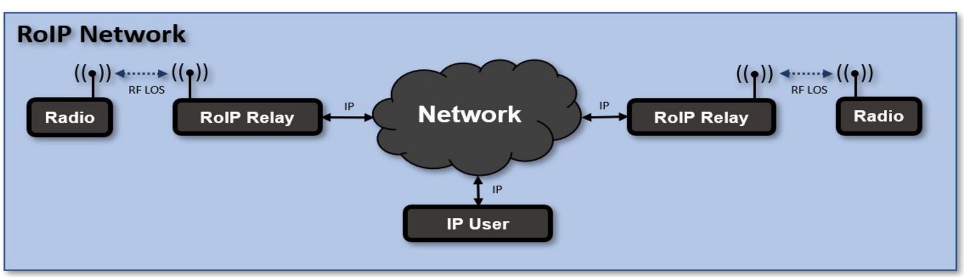


Figure 13. Example of Radio over IP.

RoIP essentially uses a specialized system to receive incoming radio frequency communications, convert and pass over an IP network, and then rebroadcast at another location to overcome line of sight limitations. An RoIP network can additionally be used to establish communications between an RF user and any user with IP connectivity.

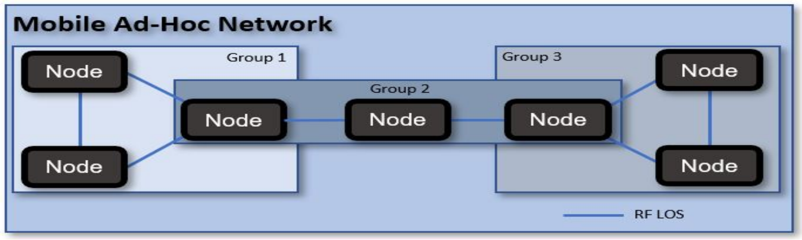


Figure 14. Example of a MANET.

MANET capable radios such as the Trellis TSM-950 are able to automatically establish communications of up to 16Mbps with other radios within LOS to create a mesh network where one radio can communicate via voice and data to any other radio within the mesh. Figure 14 presents a simple MANET where the nodes are separated into three groups based on their line of sight. In this instance, a node from Group 1 can communicate with a node in Group 3 without a direct line of sight using the center node in Group 2 as a relay. The PRC-163 and PRC-167 are also MANET capable.

The Android Tactical Assault Kit is a portable, android based system which can provide a variety of features including live video feeds, personnel tracking, image sharing, navigation, coordination, and chat using available data paths.

3. Processes

The three major processes involved with an operation are planning, execution and post-mission analysis and feedback. This section examines these three processes from the NSWTG and below perspective in the current environment, with an emphasis on which steps include major data and information requirements, and how those are currently addressed.

a. Planning

Planning is a process which falls into the decision-making element of control is typically initiated by a triggering event. Trigger events take many forms including the receipt of an order from the JSOTF or in response to a CCIR for an existing mission. Once triggered, the NSWTG staff will assemble an operational planning team (OPT) and commence the planning process. OPT membership varies dependent upon the specific mission, but includes representation from the administration, intelligence, current operations, logistics, communications, and plans departments who contribute their specialized knowledge to the overall process. Of note, the efficiency and effectiveness of an OPT depends on the collective experience of the group and the quality of their information which must be manually fused to provide an output.

(1) Mission Analysis

The first task is mission analysis where OPT members determine the objectives of the mission and manually break it down into a series of essential, specified and implied tasks as well as the mission's constraints (must do), and restraints (can't do). A thorough understanding is required by the members of the OPT of all relevant guidance and directives pertaining to the mission being analyzed. This can be a significant undertaking, dependent on the AOR as standing guidance can come from GCC, TSOC, JTF Commander, component, and any number of governmental and non-governmental organizations.

Once the OPT has established a common understanding of the mission and its objectives, they must examine the operational environment. As discussed in Chapter II, PMESII-PT is useful for strategic-level planning, while mission variables are more applicable to operational and tactical planning. Mission variables include the mission, as previously described, as well as the locations and dispositions of enemy forces, the location of friendly forces, the availability of friendly forces and logistics, terrain and weather, and the time available. This represents a tremendous amount of data and information without any shared foundation that must be manually analyzed and fused at the human level within the context of the defined mission with sources ranging from C2 systems, daily "products," all the way down to individual operational reports.

Operations and intelligence are two areas that are especially difficult to achieve operational understanding given current systems and processes. Operations intelligence can be seen as two sides of the same coin with operations concentrating on the location, movement, and capability of friendly forces on the location and employment of friendly forces while intelligence does the same for enemy forces and provides additional insight with the development of an assessment of the enemy's most likely course of action (MLCOA), and most dangerous course of action (MDCOA). Both require a thorough understanding of the current operational environment and leverage the historic data and past experience to predict a future state.

Current data structures inhibit the ability to obtain, or even be aware of, relevant data due to stovepiped systems or processes, no data dictionary, and manual information management practices. In order to use information, one must first know that information exists, and then be able to access and use it.

(2) COA Development

The OPT uses the mission analysis to create courses of action (COA) which is a sequence of activities or scheme developed to accomplish the missions. Three COAs are produced which provide the commander options. The COAs are differentiated based on commander's guidance. For example, the first COA provides an option that is air-heavy, a second COA that is land-heavy, and a third COA that combines the two.

COA development is a human intensive process where the OPT members manually fuse information from the previous step to produce a list of objectives, required forces, task organization, scheme of maneuver, timelines, sustainment, communications, and associated risks to produce a coherent representation of the recommended course of action, typically generated by hand in PowerPoint format.

Whereas mission analysis focused on knowledge discovery, COA development centers on understanding that knowledge and applying such understanding to the problem.

For example, force identification requires knowledge of the capabilities and limitations of that force within the context of the proposed task, a scheme of maneuver consider the mobility, sustainability, and supportability of that unit in the field, while all the while maintaining synchronicity with the rest of the force. Current systems and processes are in some ways extremely capable of providing specific information, but fall well short of providing the level of fidelity, continuity, and cause-and-effect knowledge required for effective planning.

(3) COA Analysis and Wargaming

COA analysis examines the proposed COAs in an attempt to gain additional insight into the problem and refine a specific COA prior to COA comparison. COA analysis is primarily accomplished through wargaming, which may consist of the current OPT members talking through a series of "what ifs," to a more detailed analysis conducted by a dedicated wargaming staff.

The input to this process is a well-developed COA which meets the basic requirements of the mission in accordance with the commander's guidance. As this thesis is concerned with NSW operations in a deployed environment, the assumption is that COA analysis will be conducted by the members of the OPT based on their operational experience. Members will step through the different parts of the COA in an effort to determine how to maximize the use of friendly forces, anticipate enemy reactions, focus intelligence and collection requirements, and identify gaps and seams with the plan, and create a synchronization matrix. Again, this is a human intensive process which relies on individual experience to analyze the COA which could result in an inexperienced team presenting an unsuitable COA. Additional outputs are potential decision points and their associated CCIRs and FFIRs and a list of the COA's advantages and disadvantages.

(4) COA Comparison

COA comparison is a relatively straight forward process whereby the different COAs developed and analyzed by the OPT are compared against each other in accordance with established evaluation criteria. This enables staff principles to recommend a preferred COA to the commander.

Evaluation criteria is determined by considering the commander's guidance and factors that affect the success of the mission. For example, three COAs may be presented which provide a speed-based option, a mass-based option, or a combination of the two. If the commander's guidance placed emphasis on agility and economy of force, but the speed-based option incurred an inordinate amount of risk, the balanced option may be the better choice. Without some form of digitization, this process becomes extremely subjective and is prone to confirmation bias or manipulation in order to arrive at a specific pre-determined outcome.

(5) COA Approval

After the staff is satisfied with the COAs presented by the OPTs, the COAs will be presented to the commander along with a staff recommendation. As the commander has provided guidance throughout the process, at this point he/she has the option to accept the staff's recommendation as-is, accept the staff's recommendation with modifications, choose one of the other COAs with or without modification, combine two or more COAs. In rare instances, the commander may elect to reject all of the COAs presented, which requires the OPT to start the entire process over. Since this is a manual process, many of the previous steps will have to be repeated. Once an acceptable COA has been approved by the commander, the staff will then move on to the final step of the planning process which is plan / order development.

(6) Plan / Order Development

Order development directly relates to the control function of direction which communicated information related to a decision to initiate and govern the actions of subordinate units. Orders are typically issued in record message traffic in the situation, mission, execution, admin and logistics, command and signal (SMEAC) format which was described in detail in Chapter II. A voice command (VOCO) can be used to initiate an immediate response, but is normally followed by an official message.

With very few exceptions, orders are "hand-jammed" into a text document. This process requires an inordinate amount of time and effort from the entire staff to generate, review, approve for release. The operations department normally initiates the message and translates the approved COA into text format which typically involves using the most recent order as a template. Once the operations department has created the draft, the message is staffed to the various departmental or functional action officers for their review and input. The message is then routed through the department heads and returned to the operations officer or chief of staff for final review before being submitted to the commander for approval.

Data and information play crucial roles in the planning process which includes several elements such as CCIRs, FFIR, and PIRs. During the execution stage, being aware of these key requirements will keep watch standers engaged.

b. Execution

Once the commander has determined a course of action, it must be executed. Execution is the manifestation of all the elements of control to manage and direct forces and functions in accordance with the plan and commander's intent. A useful way to analyze execution processes is through the use of the previously mentioned OODA framework which we use to examine execution from the NSWTG HQ and NSWTU/NSWTE forward element perspective.

(1) Observe

Observation is the required step for situational awareness as it is a process of sensemaking. Observational data comes in many forms including live sensor data, unit reporting, and intelligence products such as real-time alerts. Due to the nature of the sources of observations, observational data is, generally, organized spatio-temporally.

First, sensor data is obtained from array of sources ranging from organic capabilities all the way up to national technical means. The current data infrastructure inhibits access to certain sources as a result of classification levels, system stovepipes, and proprietary data formats. The NSWTG HQ is able to access many of these external resources through systems such as DCGS, however bandwidth limitations ordinarily prevent full exploitation of the capability. The problem is amplified at the tactical edge where external sensor data is generally not available. Conversely, deployed forces have limited ability to share organic sensor data with the larger intelligence community for the same reasons.

Unit reports commonly occur via voice, chat, or as part of a daily sitrep. The result is a bottom-up data flow from the NSWTE, to the NSWTU, to the NSWTG, where reports are evaluated and consolidated prior to reporting to the JSOTF. This creates a disparity in situational awareness among the different elements causing potentially useful data to be inaccessible at the tactical edge where it is, arguably, most needed.

Intelligence products can provide unprocessed operational data such as enemy movements, weather reports, open-source reporting digests which may be of interest to the individual NSW units. Again, bandwidth constraints inhibit the ability of the unit to receive and take advantage of these products. Further, while the HQ maintains a dedicated intelligence directorate, reduced manning at the lower levels limits the ability to process observational data into actionable forms by the NSWTUs and NSWTEs. Typically, tactical units must rely on HHQ as the conduit for processed external information and knowledge, which are then fused with organic data sources to improve resolution.

(2) Orient

Observational data feeds the processes that establish spatio-temporal situational awareness within a given operational area. The majority of C2 systems including GCCS-J, AIDE, and CIDNE fall into this category which collect, process, and display observational data into a visualized representation of the operating environment. As with DCGS, these systems require a certain level of IP connectivity and manning to employ which ordinarily limits their use to NSWTG HQ level and above.

The NSWTG normally maintains a 24-hour battle watch which serves as the primary operational point of contact. Watch compositions can vary, but generally consist of a battle watch captain (BWC) who oversees subordinate watch stations as required. BWC responsibilities include being the primary point of contact for operations, maintain situational awareness, enforce reporting requirements, and notify the commander and staff of significant changes or deviations in the operational environment in accordance with established procedures and CCIRs. Often, BWCs are tasked with additional reporting requirements by individual directorates which can result in cognitive overload and the loss of situational awareness during times of increased operational tempo.

The NSWTG HQ battle-rhythm drives the creation of products which center on fusing relevant data at a directorate and command level that affect operations. These products primarily serve to keep the commander informed and can then be distributed to subordinated units in an attempt to maintain shared situational awareness. This process is extremely manpower intensive as information must be obtained from different sources and then pieced together into a usable format. For example, a comprehensive red force product may consolidate data from GCCS-J, AIDE, message traffic, unit sitreps, voice reports, and live sensor data to populate and annotate a map on a PowerPoint slide. This is just one of many types of products which can take multiple people many hours to create and is often out-of-date before it is even released. The more time spent on creating products results in less time for detailed analysis in support of mission objectives. External units such as the JSOTF, TSOC, and NSW MSC, provide similar products and services as well, however tailored information gets progressively more difficult to produce as distance from the problem increases. Further, any support provided by higher echelons must be transmitted over communications paths that may not be available.

Provided they can be received, these products can be extremely useful at the tactical edge, but only able to depict a situation as it was at the time of their creation. Forward elements must rely on their own observations and sensory capabilities to maintain situational awareness. This can be further augmented through the use of field-wearable devices such as ATAK to enable tactical communications and information sharing at the individual level using available mobile RF communications paths.

(3) Decide

The decision-making process remains a predominately human activity as no systems currently exist that can consolidate all relevant data, place into an appropriate context, and then make decision recommendations. Decisions are made by taking the outputs of the observe and orient, processes and then exercising personal experience and judgment to determine if any changes are required to achieve mission objectives in accordance with commander's intent.

At the NSWTG HQ level, the BWC plays a key role in the decision-making process by applying existing policy and standing orders to situations as they arise. From a data perspective, decisions can easily be viewed in terms of the CCIRs and FFIRs which normally correlate with decision points. CCIRs and FFIRs are maintained at the BWC watchstation which must be manually applied to incoming reports to determine applicability. Certain CCIRs and FFIRs may trigger a simple procedural response such as a voice notification, or something more substantial such as the activation of a branch or sequel plan. Due to the tremendous amount of information processed by the BWC, there is an ever-present risk that a triggering event could be or overlooked, resulting in a failure to properly react to a situation.

Finally, decisions are often made on the fly without the benefit of a watch team for backup. In this instance, quality decision-making relies on a person's inherent understanding, competence, and experience within a given context. Deficits in any of these elements can result in the increased likelihood of a wrong decision being made or a decision being delayed until a better understanding can be achieved. For example, a simple decision by an inexperienced platoon leader such as the decision to go left or right may be the difference between taking a safe route to an objective or taking one that is regularly patrolled by enemy forces, inadvertently placing a unit at increased risk.

(4) Act

Once a decision has been made, it must be put into action. From an operational data perspective, this encompasses the control function of direction. Direction is enabled by the various communications and C2 systems to relay the results of a decision to initiate and govern the actions of subordinate units, thus completing the loop.

c. Post-Mission Reporting and Analysis

Mission debriefs are commonly conducted within the NSW community, however recording methods, submission requirements, and ensuing analysis vary.

(1) After Action Reports

Once a mission is complete, it is best to capture everything that was learned from that mission as soon as possible, for several reasons. First, after-action reviews permit participating units to conduct a thorough self-examination of all the facts, circumstances, decisions, and results to identify what was done well, what was done poorly, and what could be done better while experience is still fresh. Just as a student is often most receptive to learning immediately following a test, operating elements can learn a great amount in a post-mission debrief. Second, it is crucial to document and preserve lessons learned from previous experiences and then apply them toward follow-on missions to avoid making the same mistakes twice.

Often, post-mission analysis can produce realizations about erroneous assumptions, courses of actions, or other mistakes so adjustments can be made to future missions. Post-mission analyses can access other tools to help complete more in-depth analysis of the mission findings, perhaps with tools that enhance captured sensor information. Finally, post mission debriefs are used in event reconstruction by long-term analysts, who use these reports to achieve higher-level understanding in support of campaign and theater level planning. In many respects, the post mission analysis process ends up being a starting point for the planning process.

From a data and information collection perspective post mission analysis is a mishmash process. Some collection processes are digitized, but many spoken pearls of information are never collected. Much information is collected manually, and while the mission context at the post mission debrief is well understood by all involved, analysts and operators who come later may not be able to sufficiently discern the context to make the information valuable. Because the information is manually captured, much of it is just written on paper, never digitized, and locked away in an unknown filing cabinet for generations.

Ideally, AARs are created and stored in a centralized repository to inform future planning and execution efforts. For example, an NSW unit could have been a participant in a recent Cobra Gold exercise where key training objectives at a remote location were not met due to a lack of translators. The following year, a new NSW unit assigned to the same training event, can request the previous lessons learned which will enable them to engage early to get the appropriate support. Unfortunately, requests for previous AARs must be manually initiated and can quickly overwhelm any potential beneficiaries without significant human analysis and curation. This is especially true for smaller staffs and tactical units which lack the manpower to dedicate to sifting through AARs in search of something useful.

(2) Additional Reports

Other sources of reporting may be available incidentally as a result of normal operations. For instance, operational reports, situational reports, communications status reports, and casualty reports are among the various types of reporting required over record message traffic. Additionally, chat logs, system logs, deck logs, sensor data, voice recordings, archived files, and other types of data typically remain on their respective systems unless manually discovered and analyzed.

4. Summary

In the current environment, NSW leverages a permissive environment that depends on higher headquarter planning and execution support. Backup is readily reliable, and situational awareness is relatively easy to develop, maintain and share.

Data and information flows are often manual, but NSW and the rest of the SOF community have learned over the past 20 years to adapt and overcome. General McCrystal's book *Team of Teams* (McChrystal, 2015) is the prototypical example of a well-informed commander using every available source to command and control a myriad of forces successfully.

In the future, executing digital mission command in, especially in a non-permissive environment, promises to highlight the limitations of these manual methods. Table 6 outlines some potential trouble areas.

Table 6. Information and Data Flow Obstacles.

Process	Potential Data and Information Flow Obstacles
Planning	- Limited ability to receive intelligence and other inputs to establish an understanding of operational environment. - Manual analysis required to fuse available data into actionable information. - Additional effort required to coordinate plans with HHQ and subordinate units. - Inability to access historic lessons, trends and patterns of life.
Execution	- Observational data not evenly distributed across the force. - Current generation of C2 systems require robust network connectivity. - Manual analysis of data from multiple sources slows the decision making process and increases the time required to execute the OODA loop. - Manual data fusion techniques vary from location to location as data is not consistently catalogued and tagged. - Reliance on operational support provided by external sources such as HHQ or MSC. - Volume of data results in cognitive overload during periods of heightened operational tempo. - CCIRs, FFIRs, PIRs are not digitized and must be manually applied to events. - Quality of decisions largely dependent upon local competence and experience.
Post Mission Analysis	- Relevant experiences and insights common remain undocumented in an official AAR or lessons learned program. - AARs and lessons learned that are documented are generally difficult to exploit at the tactical level as it requires a significant amount manual processing and analysis. - Additional sources of historic data such as chat logs, deck logs, sensor data, voice recordings, etc., are generally stovepiped on their respective systems.
Other Data Related Influencers	- Processes heavily dependent on IP services and the availability of robust communications that are unsustainable in a DDIL environment. - Communications and network bottlenecks inhibit the flow of data. - Data often stored in a single location resulting in data siloes with limited consideration for COOP.

D. FUTURE ARCHITECTURE

The future C4I operational environment promises to be much different from the present. With the return of great power competition, future conflicts will involve adversaries who possess capabilities equal to or possibly even greater than our own, especially in the realm of electronic warfare. Operations within a communication denied, degraded, intermittent, or limited (DDIL) environment will become the norm, meaning the availability of high-capacity SATCOM links and the systems that rely on them will no longer be assured. Adversarial C4ISR systems will continue to grow in capability and hold friendly forces and infrastructure at risk. As the likelihood of isolation increases, mission command will once again be required to effectively C2 assigned forces. Digitizing mission command will ensure it preeminence on the future battlefield.

1. Future Organizational Relationships

As organizational relationships are designated by a proper authority in accordance with doctrine, the overall operational chain of command will remain the same, at least at first. Eventually, such relationships may change depending on how the digitation efforts evolve, but it is too early to tell. Changing both a data strategy and the command relationships simultaneously is a recipe for confusion. Figure 15 illustrates the anticipated operational chain of command, enhanced through mission command principles.

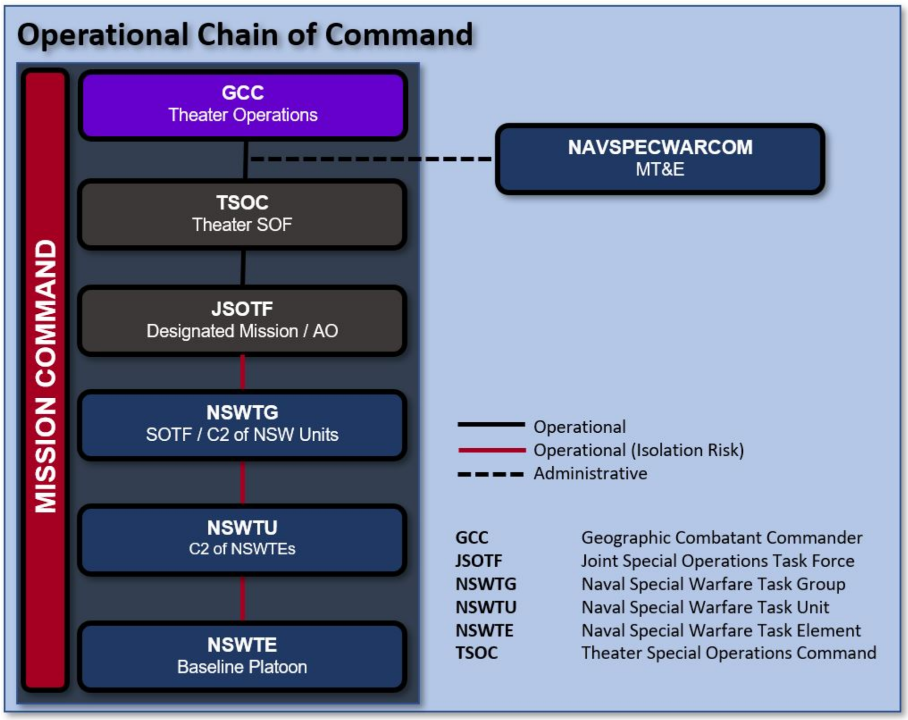


Figure 15. Future Operational Chain of Command.

However, due to the anticipated challenges of the future operating environment, the commander will no longer have a reasonable expectation of maintaining reliable communications with any unit that relies of SATCOM which for the purposes of this scenario will be below the JSOTF level. While NSW is arguably among the best at implementing the concepts of mission command, the methodology will move from optional to essential in order to maintain an acceptable level of C2 over assigned forces.

2. Future Communications Architecture

The overall future communications architecture is expected to remain relatively similar with the provision of USSOCOM managed IP services, augmented by tactical voice and data networks at its core. As digitization continues, data and information flows will be shifted to networks resulting in an exponential demand for bandwidth over terrestrial and satellite paths. Well-connected shore-based installations will experience the greatest benefit due to their ability to access ever-increasing levels of shared processing, storage, and network services within a robust cloud environment.

At the other end of the spectrum, tactical units, will experience a much different reality as previously described. Emerging technologies are being developed to provide assured communications in a DDIL environment. Software-defined radios and networks coupled with next-generation compression and service models will provide improved flexibility in support of electronic maneuver. Low probability of intercept / low probability of detect techniques (LPI/LPD) such as direct-sequence spread spectrum (DSSS), frequency hopping and communications below the noise floor will undoubtedly ameliorate some of these challenges, however one must assume that potential adversaries are working just as hard to negate these efforts. Therefore, it must be assumed that the more emissions a unit produces, the more likely it is to be detected, jammed, tracked, or targeted.

Regardless, as this thesis focuses on data flows and strategy, we will assume a similar level of communications capability and simply point out where data techniques could benefit users within a DDIL environment. That said, discussion of specific communications architectures ought to be the focus of a separate research effort.

3. Future Processes

This section will present a vision of how planning, execution, and post-mission analysis and feedback processes can be advanced to improve efficiency and capability in support of digital mission command.

a. Planning

The intent of the planning process will not change. Triggering events will continue to initiate the planning process and the OPT will remain at the core of the effort. However, in this vision, the planning process is significantly improved through the use of technology and data techniques to produce a better-quality product more quickly.

(1) Mission Analysis

One of the most difficult tasks is to establish a common understanding of the dynamic operational environment constructed by processes triggered by environmental and operational events for a task organized into causal sequences. Put simply, this consists of triggering events that place static entities into motion. Future ISR capabilities, especially in the realm of unmanned autonomous vehicles and small-form organic sensors, will provide an exponential increase in the availability of real and near-real time data. The future system should collect, tag, categorize, and assemble events and entities into contextual, well-structured information and knowledge populated into storage based on multi-dimensional arrays. Further, future systems should support the automated discovery based on the intelligent orchestration of access to data sources to ensure multi-source fusion, relevant to the operational area at the specified level of classification.

Additionally, future system developers should consider refraining from relying on mission variables. Unlike independent mission variables, future artifacts will depend on a multi-dimensional system of coordinates and aggregate functions which processing multi-coordinate spaces into meaningful operational information. Knowledge-graph techniques should be used to represent mission artifacts which apply known characteristics, capabilities, and limitations that add depth to the data by making information out of it. This should significantly reduce reliance on biased individual experience to achieve common understanding by the OPT. Locations and dispositions of enemy forces, friendly forces, logistics, as well as weather and terrain and other required inputs will be presented in a common, real world-based format that is simple, repeatable, searchable, fusible and visualizable.

Access to historic data will inform the OPT of pattern of life trends to model and predict possible future world model states within the operational area. For example, a heatmap based on recent reports can show relative enemy activity for consideration when entering the COA development phase. MDCOA and MLCOAs, informed by previous actions, will provide additional insight into possible enemy tactical movements and actions. As many planning efforts support similar missions, OPT members will be presented with consistent plans along with the best practice recommendations derived from the AAR process to assist as a starting point.

Planning activities should be tracked at the system level. This will enable the system to adapt to the individual preferences and processes of a staff, anticipate future requirements, and make suggestions based on past inquiries. There is even the possibility to use the data assets to better train staff officers serving on the OPT, by creating opportunities for new staff to create their own mock plans and develop their knowledge-set and more effectively provide insight and feedback.

(2) COA Development

A large part of future COA development will be accomplished through the use of specialized systems using second and third wave AI principles. In this step, COAs can be created by applying a series of profiles to the model of the operational environment developed in the previous step toward specified objectives. For instance, an ‘air-heavy” profile would be applied to identify and present units typically associated with air operations informed by their current tasking, availability, and conditions of readiness or suitability.

Once complete, a technically sound COA is generated which includes potential threats, complications, or other considerations for review by the OPT. Similar to mission analysis, the system should leverage historical data to adapt to staff processes and preferences. This will significantly decrease the time required for COA development and allow the OPT to focus on the big-picture issues instead of technical details. This process directly contributes to the mission command elements of competence and, if explainable, to a mutual trust between OPT members and machines as it is repeatable, fast, and leverages multi-source, non-biased, and predictable datasets. Mutual trust is further improved as subordinates and senior decision makers will know they are using the same future insights generated by a shared contextualized knowledge base.

(3) COA Analysis and Wargaming

Traditionally, specialized human knowledge and experience has been required for effective wargaming. While the human element will remain important, analysis and wargaming will benefit tremendously through a human / machine teaming relationship. Advanced data techniques will enable a COA to be examined within the context of a near real-time, dynamic battlespace environment. This will allow visualization techniques to be used to represent a number of factors including enemy capabilities, friendly capabilities, potential for interaction, and relative risk.

Contextual adaptation techniques based on historical data will provide the ability to project future world-state. For example, at the tactical level, statistical analysis has revealed an enemy unit generally conducts daily patrols from 0900–1300 along a known route. This information could be used to shift COA timelines to the left or right in order to avoid interaction with the unit and to create a CCIR which activates a branch plan in the event that an interaction does occur.

(4) COA Comparison

Again, COA comparison is a relatively straight forward process where the OPT evaluates the different COAs against established evaluation criteria. The future system should standardize the definitions of the various criteria and provide additional insight and objectivity when comparing COAs. Traditionally, suitability was determined by OPT members manually assessing the positives and negatives attributes of a COA with regard to commander’s guidance. For example, when comparing a mass-based COA and an economy-based COA, details could include a projected success rate, risk to mission, risk to force, or even how a specific COA impacts the overall ability to conduct follow-on actions. A digitized, automated process will enable a higher level of analysis with reduced bias. Plan digitization also makes the use of advanced game theory techniques possible.

(5) COA Approval

As previously mentioned, the commander may elect to change, combine, or reject all COAs. While approval is solely the prerogative of the commander, additional guidance or changes at this stage will no longer require starting the entire process over. As everything has been digitized and updated dynamically, the OPT only needs to incorporate the updated guidance into the existing model, analyze, compare, and re-submit.

(6) Plan / Order Development

Record message traffic will likely remain the primary method to initiate and govern the actions of subordinate units as they satisfy the various legal requirements for "official" communications and can be easily transmitted over any available communications medium. The digitization of the planning process will augment this capability in a number of ways. First, it must be acknowledged that orders generation is more art than science, however there are many standard inputs that can be derived from the approved COA. These inputs should be identified and then digitally combined through the use of a common application which uses standard phraseologies and approved formats to produce an eighty percent solution which is then staffed for final review and approval. Second, as the COA is already digitized, a standard report can be generated to produce a CONOPs that is optimized for distribution, similar to the traditional PowerPoint / pdf, to promote shared understanding and maintain unity of effort. Finally, an interactive version could be created and distributed to subordinate commands which provides a C2 system overlay in order to visualize key elements, objectives, and features that can be updated in real-time from available sensors and reports in support of execution.

A new product that might arise from orders development is the digitization of all the CCIRs, PIRs, and other suggested reporting requirements. This makes the possible use of smart agents much more likely.

b. Execution

The output of the planning process should be an improved plan which is based on a more accurate representation of the operational environment. Once approved, major C2 nodes such as the NSWTG HQ will be able to quickly visualize the CONOPs and implement the plan. Again, the future execution processes are analyzed through the lens of the OODA framework from the NSW perspective.

(1) Observe

As before, observational data remains a key input for situational awareness. Data strategies that facilitate collection, aggregation, storage, and discovery are key to getting the right data to the right place within a tactically relevant timeline. High level DOD initiatives, such as Joint All-Domain Command and Control (JADC2), seek to connect sensors to shooters across a tightly-coupled, integrated network. Observational data from sensors, unit reports, intelligence products and other sources will be digitized into a standard format that enables further processing by various units in accordance with their needs in support of Joint C2.

Enriched data will be curated via sanitization, correlation, fusion, and cause-effect analysis at the appropriate level of command based on the size-weight-and-power (SWaP) constraints and network bandwidth. Statistical analysis should be used to examine data usage patterns in order to identify which sources and data are most useful for operations at what periodicities. Critical operational data should then be optimized and automatically delivered at the appropriate resolution in accordance with a unit's mission, geographic location, and level of command. The challenge for operating units will be to improve their capacity in order to clearly and digitally define their critical data needs so they can benefit from these data processing improvements.

This will serve to reduce strain over already congested networks to ensure that all operationally relevant observational data is available while data that is not relevant is discarded. For instance, a unit may not need overhead imagery for an entire country, but would benefit tremendously from imagery within fifty miles of their position. Further, data can be optimized based on required periodicity. For example, an air track might require near-real time sensory data, whereas a ship might only require updates every ten minutes which would significantly reduce the data load across the network.

By standardizing the data, specialized processing techniques can be applied at scale in order provide tailored, optimized products for consumption. This assertion holds true from the NSWTG level, all the way out to at the tactical edge where bandwidth is at a premium. An increased level of discrimination over optimized and prioritized operational data will enable a range of delivery options and communications techniques in support of operations within a contested electromagnetic environment. Further, it is important that future systems be able to symmetrically transform and exchange data between the edge and higher levels to ensure that information natively born "at the edge" can be both processed locally and forwarded to higher level units for aggregation and future fusion.

As previously noted, timely, relevant, and complete observational data is the starting point of the execution process and serves as a primary enabler for the principles of mission command. Without it, there is no input into the orient process, no shared situational understanding, and no ability to apply commander's intent, assess risk, or to conduct disciplined initiative.

(2) Orient

Traditionally, the end product of a C2 system was limited to a track displayed on a common operational picture which must be interpreted by a qualified human expert in order to achieve situational awareness and anticipate follow-on movements and actions. Focus on a single target by one or few shooters is intrinsically unscalable. The real future fight is many-on-many. Future systems, however, will leverage analytical data techniques to enrich the track data within the context of enveloping environments (including A2AD) to shift a large portion of the orientation burden to the machine.

First, future C2 systems should provide the ability to represent a rich operational environment. Knowledge Base (KB) representations will create a world view that is interactive and based on an authoritative object and action where the latter assigns attributes to a static object to create a dynamic one per a task definition within the operational environment. Without getting into too much detail, fixed features such as an enemy garrison, a radar station, or a friendly logistical node might be represented, each with its own base characteristics that can interact with other objects. These features can be further modified by the inclusion and association of operational data to accurately depict an object's capabilities to threaten or enhance the force.

Once a steady state system behavior is achieved, operational data from the previous step can then be linked by sequencing the previous triggering event with the current one. The previous step may now be injected into the KB's representation by chaining previous and current steps together, thereby expressing a cause-and-effect relationship. The interaction of these two elements can then be used to calculate spheres of influence, relative capabilities of one over another, or other operationally relevant associations. Historical data will be used to make statistically informed assessments of future world-states such as probable flight or patrol paths of active units.

Interactive CONOPs developed and distributed in the planning stage can be applied to the current operational picture in order to provide an immediate representation of major movements, objectives, and key terrain in support of shared situational understanding. These interactive CONOPs will also configure the subordinate station to provide automatic feedback of relevant information based on organic capabilities such as sensor feeds or local assessments to HHQ. Further, HHQ can easily modify the plan by sending updates as required which could announce and implement changes without the need for excessive coordination.

NSWTG HQ battle-rhythm product creation would be streamlined as described in the previous section. Intelligence products should leverage visible, accessible, understandable, linked, trustworthy, interoperable, and secure (VAULTIS) data sources to automate the fusion of routine processes. This will serve to shift the burden of effort from the expert human to the AI/ML enabled machine to enhance speed, accuracy, and relevance of the final product. The human-in-the-loop / human-on-the-loop in human / machine interface (HMI) will enable superior understanding of cascading contexts. The time saved in the production cycle will result in more time available for detailed analysis activities that are more suitable for human intelligence.

At the tactical edge, an expedited product generation cycle will provide forward units with more accurate and up-to-date information to improve overall situational awareness. Further, disadvantaged units will be able to ingest optimized operational data into lightweight versions of the same systems used by HHQ to apply real-time data to a rich, tailored world model to provide a deeper understanding of the operational environment. In other words, a minimal amount of actual data will be distributed to the tactical edge, which could then be interpreted at the "last mile" to add depth and context. Additionally, this will open an opportunity to apply ML for distributed training at the edge, and AI for fusion of the output to continuously train a natively generated edge-model by combining this minimal amount of actual data which could potentially be further enriched with fused knowledge from higher-level command tiers.

(3) Decide

The decision-making process should remain a human centered activity, however one enabled by technology. Future processes should leverage AI / ML enabled C2 systems to fuse and summarize common sense data, historical data, standing guidance, policy, procedures, and doctrine within the context of the operational environment to enhance decision-making speed and quality.

At the NSWTG HQ level, CCIRs and FFIRs, created digitally as part of the planning process, are applied against incoming reports through the use of a digital cognitive assistant to automatically alert the BWC of any event that meets those criteria. As part of a collaborative HMI pair, the AI / ML enabled cognitive assistant will organize and queue relevant information for the review of the BWC with a list of recommended actions based on existing policy, procedures, standing orders, best-practices, and historical data. For example, a FFIR is triggered by the cancellation of a scheduled patrol due to a medical emergency. This AI / ML enabled system provides the BWC with the standing orders regarding reporting criteria, assesses the operational impact of the cancellation, identifies any available assets to fill the gap, or if the activation of a branch or sequel plan is required.

Decisions made at the individual level should be further enhanced through the use of cognitive assistants. A sufficiently capable, field-wearable device would provide an ideal platform to host a localized world view which is periodically updated using organic sensors or assured C2 links to maintain situational awareness. Mission, objectives, decision points, and other variables could be represented within the context of the overall plan in order to affect synchronicity, identify possible obstacles, and inform decisions so as to exercise disciplined initiative in accordance with the commander's intent.

Human-machine teaming will significantly improve the overall performance at the individual level. The digitization of historical data and experiences will provide a baseline of knowledge to produce a standard level of competence across the force in order to produce informed, appropriate, and repeatable decision cycles at all levels of command.

(4) Act

Again, the final step in the execute process is to act. Future systems should monitor activities and decisions to facilitate automatic reporting in order to maintain shared situational awareness and unity of action.

c. Post-Mission Reporting and Analysis

Future systems will open the door for a more comprehensive collection of mission debriefs, after action reports, and historic operational data.

(1) After Action Reports

After action reports will be collected in a similar manner as before, but future systems should provide additional functionality by using natural language processing techniques to better collect, analyze, and correlate findings. AARs tend to be repetitive, meaning things that were a problem this time, were a problem last time and the time before that. Future AARs should be digitized, centralized, categorized, and analyzed to identify patterns and trends and produce actionable information to inform future planning, operations or technical requirements.

As previously discussed, future plans will rely heavily on the analysis of digitized AARs. This will give an indication of what worked, what did not and under what circumstances so that it can be applied to future plans. AARs will further serve to validate the efficacy of a plan in order to provide an OPT with ranked examples of prior planning efforts. Additionally, since the planning process is digitized, the AAR process will enable the comparison of similar plans to identify which mission variables or circumstances cause one plan to fail while the other succeeded.

Operations will benefit from the ability to consolidate and analyze AARs to develop an operational profile for a certain area or mission type. Instead of sifting through a never-ending series of written reports, future systems should identify common subjects and recurring issues which constitute a risk to mission or risk to force, ranked by probability and severity. This will serve to inform future operations, increase long-term institutional knowledge, and feed back into the execution process. From a mission command perspective, this serves to reinforce mutual trust.

These processes can be used for technical purposes, as well. For instance, if multiple AARs report an inability to establish UHF LOS communications in certain operational area, this could prompt further investigation to identify a root cause such as local interference or jamming activities by the enemy. The same issue in multiple theaters could indicate an equipment or training deficiency which would prompt a separate response. Previously, this pattern would have required the notice of an individual with sufficient knowledge to understand what they were seeing. The same techniques could be used to identify deficiencies in training, operations, or even correct assumptions about the operational environment itself.

(2) Additional Reports

Digitizing incidental reporting sources such as chat logs, station logs, voice data, sensor data, and all manners of operational reports represent an untapped gold-mine in the development of historical data. Much like AARs, these data sources will be analyzed to identify trends, recreate events, and feed all manners of long-term data analysis projects. For instance, residual RADAR data can be analyzed to inform patterns of life within a geographic region. Another example would be the routine analysis of situational reports to recreate events over a period in an effort to achieve a higher-level understanding than is provided by a single AAR.

E. CHAPTER SUMMARY

This chapter examined the relationships between command and control, mission command, and how they relate to the planning, execution, and after-action reporting and analysis. Current C2 systems focus on providing situational awareness which allows some to proclaim that information advantage has already been achieved in support of the shared understanding element of mission command. This, in fact, proves to be somewhat premature as situational awareness and situational understanding can have many different levels, as previously discussed. Beyond this, little is done to support the remaining elements of competence, mutual trust, mission orders, commander's intent, disciplined initiative, and risk acceptance.

Digitizing NSW data in a mission command environment will lay the foundation for the in-depth analysis required to improve processes, optimize communications, and enhance the decision-making process through human-machine teaming. Competence will increase by analyzing and condensing tactical and procedural concepts down easily understandable information feeds based on current policy and previous experiences to enhance the proficiency at the individual level. Mutual trust will be enhanced when commanders, subordinates, and partners are able to assume a greater level of understanding and ability by their counterparts based on common inputs while performing assigned tasks. Shared understanding will obviously benefit as additional sources enrich the common operational picture within the context of the operational environment, well beyond basic track data and in accordance with mission orders. Further, digitization presents a golden opportunity to focus on the problem of the Third Wave of AI, also known as contextual adaptivity. Triggering events, as well as action and maneuvering events must become the first-class citizens of the future data architecture, replacing the entity-noun which has occupied that role since the advent of object-oriented design.

All of this will serve to put the individual and organization in a better position to execute mission and exercise disciplined initiative within the confines of commander's guidance while maintaining an acceptable level of risk, whether in a permissive or denied environment.

V. CONCLUSION

This thesis aims to increase understanding of the nature of command and control and how to implement a common foundational DIK layer and supporting network architecture in support of Digital Mission Command. To accomplish this, the author conducted an in-depth review of the relevant literature on command and control, command and control systems, digital mission command, the NSW operational chain of command, associated communications infrastructures and emerging technologies. This chapter presents the research conclusions, recommendations for growing a digital NSW force, and suggestions for future research.

A. RESEARCH CONCLUSIONS

Current C2 systems focus on the feedback, information, and communications functions of control which addresses only the "shared situational awareness" element of mission command. Future operations will take place within a non-permissive, DDIL environment, against adversaries who possess capabilities that are equal or possibly superior to our own. The current C2 model, which relies on robust communications networks, reach back, and high-capacity SATCOM links, will become untenable. This will be true especially at the tactical level which operates under the assumption that they will become isolated, meaning they will have to rely on their own organic systems, sensors, and expertise to accomplish mission objectives. Thus, mission command, as the primary command and control approach, will dominate operations.

Mission command depends on creating situational understanding for the participating units. Technology will play a central role in building out the DIK pyramid in order to achieve that situational understanding. A data strategy based on the implementation of a common, scalable, core data management framework must be defined to serve as the foundation upon which everything else is built. All relevant operational data must be identified and stored in a manner that is visible, accessible, understandable, linked, trustworthy, interoperable, and secure in order to automate routine processes and reduce cognitive load. A tremendous amount of effort and coordination will be required in the realm of data organization so as to synchronize NSW efforts both internally, and in conjunction with USSOCOM, TSOC, and DOD initiatives.

The mission command philosophy of centralized planning and decentralized execution and control is the key for NSW success in projected future operational environments. A new emphasis must be placed on digitizing and analyzing historical and operational data in order to provide additional insight to the operator in the form of rich track data, recommendations, alerts, and projected future states within the context of a given situation.

Moreover, the increase in unmanned systems and smart agents will require increased human-machine teaming concepts that must be employed in an effort to raise the relative competence of the force. Enabled by the digitization of knowledge and past experience, this more competent force will naturally increase mutual trust among commanders, subordinates, and partners. As the level of shared understanding amongst the various levels of command increases, the commander can delegate greater authority and decision-making ability to subordinate forces which will provide more opportunity for the execution of disciplined initiative in accordance with commander's guidance at a controlled level of risk.

Finally, communications, network, and data architectures must be developed that support operations in both permissive and non-permissive environments. Ideally, a tactical unit could receive raw data inputs from sensors or other sources and generate actionable information, however that will not always be possible. In those cases, data must be curated, correlated, fused, and sanitized at the higher level where processing and connectivity is readily available and then forwarded to the distant-end using available means. This can be accomplished through a variety of methods including next-generation, relatively high-capacity LPI / LPD communications channels such as DSSS, WCDMA or LEO satellite communications, or by alternate means such as MANETs, broadcasts, or UAV relays.

B. RECOMMENDATIONS FOR CREATING A DIGITAL NSW COMMUNITY

The question is simple: How does NSW proceed in creating digital mission command? Chapter IV envisions the future NSW fighting force leveraging a robust and adaptive data environment, where despite competing requirements for bandwidth, NSW's data strategy promotes the delivery of valuable information to the right place at the right time, supporting adaptive operations and a robust, quick cycle, decision-making process. Chapter IV analysis also suggests that the current data infrastructure, with stovepiped databases, reliance on purely manual processes, and reams of undigitized information, is unsuited to support digital mission command, especially at the tactical level.

Digitization of the planning process will ensure that efforts are more efficient, complete, and historically informed which will standardize and synchronize the inputs into the execution process. Execution will benefit by consolidating operational data and the use of automated and AI / ML enabled C2 systems to achieve a heightened level of situational understanding. Results captured by a robust after-action and historic data analysis function would feed back into planning and execution in order to refine the entire process. All data needs to be collected, ingested, catalogued, and curated with consistent representation, to allow platform-agnostic applications to access all relevant data in order to create the desired output. This requires a robust, flexible data flow architecture, so when communications and networks are not available, units still perform. The following recommendations suggest initial steps on how to implement such a data strategy.

a. Create a data-centric organizational culture across the NSW community

In order to fully realize the benefits and advantages afforded by data-analysis, automation, and associated AI/ML technologies, NSW must place emphasis on the creation of a data-centric culture. By developing local expertise in support of a comprehensive data strategy, NSW will not only enable organic data efforts, but also be in a better position to influence and participate in higher-level USSOCOM and DOD initiatives in support of NSW interests.

Recommend establishing an NSW Data Operations working group. This working group will be chaired by the N3 Department, co-chaired by the N2 Department, with remaining departments and functional leads as contributing members. The reason is that processes are driven by operations and intelligence, then further enabled by technology. As a center of gravity for the command, the operations department has both the insight and the authority to effectively manage the efforts of the working group and implement associated actions at the command level. The alternative would likely result in the N6 presenting technical solutions in search of operational problems.

Members assigned to the working group will serve as the data SMEs for their respective areas and should be educated in data strategies, data science methodologies, and be aware of current DOD and private sector capabilities and initiatives. The first order of business should be the creation of high-level NSW data strategy which formalizes the composition and purpose of the working group as well as its roles and responsibilities at NAVSPECWARCOM. This should include the appointment of an O-6 level steering committee who will provide high-level direction and guidance to the working group, and present findings and recommendations to the commander. Once the working group reaches a certain level of maturity, recommend additional working groups be stood up at subordinate commands in order to gain additional insight, develop expertise, and coordinate data-related efforts across the community.

Trained data scientists and engineers must be an integral part of these working groups. These people serve to solidify data operations processes, educate the users, and ensure the operational insights are melded with the new technologies in support of NSW objectives. They will ensure compliance with DOD data rules and regulations, help build a governance process, and ensure synchronization with the broader SOF community.

b. Establish a common data management framework

Creating a robust DIK layer that is able to ingest and store all operational data is essential for the development and use of advanced automated and AI/ML-enabled command and control systems. This layer will provide a shared, scalable, centralized data management framework that separates the storage layer from the database and processing frameworks and will provide a common foundation to promote increased interoperability at the contextual level.

The existing SIE / SOFNET cloud infrastructure provides an ideal environment for the construction of a data lake to hold large amounts of raw data in their respective native formats. Data must be collected, tagged, categorized, and indexed using formally defined lexicons, taxonomies and ontologies. In order to avoid the trappings of traditional relational databases, the heart of the DIK layer should be a well-structured, authoritative multi-dimensional array which enables the quick and efficient processing of data based on a variety of criteria including level of command, level of abstraction, classification, and spatial-temporal measures. The DIK layer should ingest data from a data lake that serves as an authoritative source of unaltered data which can then be leveraged by secondary applications in order to achieve desired results. These results are then returned back to the structured storage of the DIK layer's multi-dimensional array. Subsets can then be created from the primary DIK layer storage to support specific mission sets, functions, or, given the anticipated DDIL operating environment, to serve as local storage at the unit or individual system level.

Once the core framework is established, legacy databases and stovepiped data should be identified and converted to the multi-dimensional array formats using commercially available software such as TileDB or ZARR. This will transform hierarchical tables of legacy relational databases into a single entity comprised of multiple dimensions, viewed in the context of an array, that promotes data exploitation and the application of adjacency matrices to represent and process graphs. While beyond the scope of this thesis, such techniques will enable advanced knowledge operations in the future, such as current and projected world views.

c. Formally define and digitize C2 processes

Digitization of C2 processes requires in-depth analysis in order to fully identify the steps, inputs, outputs, and dependencies of the function being modeled. This can be a deceptively difficult task under normal circumstances, which is further complicated in the

NSW community as many processes are poorly documented, or require a high level of human interpretation to execute.

First, utilize the NSW Data Operations working group to identify and prioritize key processes that contribute to the execution of mission command. These can be items as simple as an individual CCIR, or something more complex such as the previously described planning process. Once these processes are identified, they should be further reduced into their constituent sub-processes through functional decomposition. It is unlikely that working group will possess a sufficient level of expertise or skill in data analysis to fully define the process, at which point the process will be turned over to the NSW data scientists, data engineers, or to a competent third-party who specializes in process analysis. However, continued close coordination with the operators is a must.

Operational data that feeds these identified processes should be digitized, labeled, and stored in a centralized location at the earliest opportunity. An interesting characteristic of data is that the more one accumulates, the more inferences can be drawn from it, and the more uses can be found for it. Unfortunately, once the opportunity to collect relevant data is missed, it is extremely difficult to recover.

As noted, there is considerable work to be accomplished, and adding data scientists and engineers requires resources and time. The payoff, though, will be a data-infused force that can out-think and respond more rapidly than the enemy, and will transform the NSW.

C. AREAS FOR ADDITIONAL RESEARCH

a. Human-machine teaming interfaces at the tactical level

Human-machine teaming will be a critical piece of the digital mission command initiative moving forward. While it is certainly important to develop systems that analyze, organize, categorize, and display information, it is equally important that this information is easily accessed and understood by operators. Nowhere is this truer than at the tactical level where events happen more quickly and can overwhelm an operator's cognitive ability to process or benefit from additional information. This requires an in-depth understanding of what information is useful, what is a distraction, under which circumstance cognitive saturation occurs, and what type of user interface best facilitates effective human-machine teaming.

b. NSW communications and network architectures

Due to the sensitive nature of NSW operations, the distribution of information communications and network architectures is extremely limited. Further research is required to fully understand the communication and network architectures of NSW and the SOF community at an appropriate level of classification and detail. This will inform subsequent research efforts by providing a realistic representation of transport capabilities to focus data collection, distribution, and analysis efforts in support of future systems and processes.

c. Data optimization in support of tactical C2 and communications systems in a DDIL environment

To realize the full benefits of digital mission command, digitized information and knowledge must be shared across all levels of command. This becomes increasingly difficult as one approaches the tactical edge where capacity is typically limited, if available at all. Traditionally, this has been addressed through the development of communications systems that increase bandwidth. A second approach is to optimize mission-specific data availability, by developing contextually aware C2 systems that are able to infer and push valuable information and knowledge updates about the operational environment for decision-making using a canonical, adaptive world-model, instead of explicitly relying on network traffic prioritization based on human-based pre-operational experience-driven decisions. In other words, saying a little to mean a lot. This will open the door for the use of a variety of LPI / LPD communications methods including DSSS, WCDMA, and broadcasts. Further, MANETs could be employed to exchange data at a peer-to peer-level in order to achieve local convergence in the absence a reach-back capability to established network infrastructure. Finally, NSW should explore the Navy’s new Communications as a Service capability which focuses on many of the same concepts.

d. NSW AI strategy and vision

As AI efforts within the DOD gather momentum, the NSW must keep pace to develop a comprehensive strategy for various applications including intelligence, surveillance, reconnaissance, and operations. This research considered opportunities and implications at a higher level, however future success will depend on the articulation of a clear vision for future capabilities that is backed up by a detailed plan of actions and milestones. This vision should address combat applications as well other functions such as MT&E, administration, and logistics.

LIST OF REFERENCES

Clarke, A., & Knudson, D. (2018). Examination of cognitive load in the human-machine teaming context. Monterey, CA; Naval Postgraduate School. https://calhoun.nps.edu/handle/10945/59638

Clausewitz, C. (2006). *On war*. Oxford University Press.

Coram, R. (2004). Boyd: The fighter pilot who changed the art of war. Time Warner Book Group.

Department of the Army. (2019). *Mission command, command and control of Army Forces.* (ADP 6–0). https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN19189_ADP_6-0_FINAL_WEB_v2.pdf

Department of Defense. (2019). Summary of the 2018 Department of Defense artificial intelligence strategy: Harnessing AI to advance our security and prosperity. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Department of Defense. (2021). *JEDI cloud.* DOD enterprise cloud. https://www.cloud.mil/JEDI-Cloud/

Department of the Navy. (2018). *Naval special warfare* (NWP 3-05).

Ergene, Y. (2016). *Analysis of unmanned systems in military logistics* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. http://hdl.handle.net/10945/51689

Haddick, R. (2016). Improving the sustainment of SOF distributed operations in access-denied operations. Florida, FL: Joint Special Operations Press.

Joint Artificial Intelligence Center. (2020, May 6). *Why data governance is critical to a successful JCF.* https://www.ai.mil/blog_05_06_20-why_data_governance_is_critical_to_a_successful_jcf.html

Joint Artificial Intelligence Center. (2020a, June 18). *A roadmap to getting AI-ready.* https://www.ai.mil/blog_06_18_20a_roadmap_to_getting_ ai_ready.html

Joint Chiefs of Staff. (2013). *Joint intelligence* (JP 2-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf

Joint Chiefs of Staff. (2017). *Joint operations* (JP 3-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910

Joint Chiefs of Staff. (2018). *Joint maritime operations* (JP 3-32). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_32pa.pdf

Joint Chiefs of Staff. (2018a). Charter of the Joint Requirements Oversight Council and implementation of the joint capabilities integration and development system (CJCSI 5123.01H). https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%205123.01H.pdf?ver=2018-10-26-163922-137

Joint Chiefs of Staff. (2019). *Joint communications system* (JP 6-0). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp6_0ch1.pdf?ver=2019-10-15-172254-827

Joint Chiefs of Staff. (2020). *Insights and best practices focus paper, mission command, second edition.* https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/csel_fp3rd_ed.pdf?ver=2020-01-13-083410-863

Joint Chiefs of Staff. (2020a). *Insights and best practices focus paper, commander's critical information requirements (CCIRs).* https://www.jcs.mil/Portals/36/Documents/Doctrine/fp/ccir_fp4th_ed.pdf?ver=2020-01-13-083331-097

Joint Chiefs of Staff. (2021). *DOD dictionary of military and associated terms* (DOD Dictionary). https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

Launchbury, J. (2017). A DARPA perspective on artificial intelligence [presentation]. Defense Advanced Research Agency. Arlington, VA, United States. https://www.darpa.mil/attachments/AIFull.pdf

Lo, B. (2021, March 18). PEO C4I Command and Control Systems Program Office (PMW 150) maritime C2 [presentation]. COMNAVWARSYSCOM PEO C4I march 2021 fleet C4ISR seminar. San Diego, CA, United States. https://sailor.navy.mil/blog/ViewMessages.cfm?Forum=277&Topic=1775

Lovering, T. (2014). Odin's ravens: From situational awareness to understanding. The Three Swords Magazine, 27(2014), 50–52. https://www.jwc.nato.int/images/stories/threeswords/NOV_SITAW.pdf

Marcus, G. (2020). The next decade in AI: Four steps towards robust artificial intelligence. https://arxiv.org/ftp/arxiv/papers/2002/2002.06177.pdf

McChrystal, S., Collins, T., Silverman, D., & Fussell, C. (2015). Team of teams: new rules of engagement for a complex world. Portfolio/Penguin.

McRaven, W. (1993). *The theory of special operations* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. http://hdl.handle.net/10945/14838

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800–145, U.S. Department of Commerce National Institute of Standards and Technology, Gaithersburg, MD. 1–3.

Rubel, R. (2015). Deconstructing Nimitz's principle of calculated risk. *Naval War College Review*, Vol. 68 : No. 1, Article 4. https://digital-commons. usnwc.edu/nwc-review/vol68/iss1/4

Reeves, Brian. (1997). *Navy SEALs: theory vs. reality* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/8728

Stone, A. (2019, August 14). *The network tech that U.S. Special Operations Command likes.* C4ISRNET. https://www.c4isrnet.com/battlefield-tech/it-networks/2019/08/14/the-network-tech-that-us-special-operations-command-likes/

Sweller, J. (1988). Cognitive load during problem solving: Effects on learning. *Cognitive Science, 12*(2), 257–285. doi: 10.1207/s15516709cog1202_4

Sweller, J. (2008). Human cognitive architecture. In J.M Spector, M. D. Merrill, J. Van Merriëboer, and M. P. Driscoll (Eds.), *Handbook of research on educational communications and technology* (3rd ed.) (pp. 369–381). New York, NY: Lawrence Erlbaum Associates.

Sweller, J. (2010). Element interactivity and intrinsic, extraneous, and germane cognitive load. *Educational Psychology Review*, *22*(2), 123–138. doi: 10.1007/s10648-010-9128-5

Sweller, J., Ayres, P., & Kalyuga, S. (2011). *Cognitive load theory* (1st ed.). New York, NY: Springer. doi: 10.1007/978-1-4419-816-4

Thomas, R. (2017, May 2). Statement of General Raymond A. Thomas, III, U.S. Army, Commander, United States Special Operations Command before the House Armed Services Committee, Subcommittee on Emerging Threats and Capabilities. https://www.socom.mil/Pages/posture-statement-hasc.aspx

Townsend, S., Crissman, D., & McCoy, K. (2019). Reinvigorating the Army's approach to mission command. Army University Press, Military Review. https://www.armyupress.army.mil/journals/military-review/online-exclusive/2019-ole/march/reinvigorating-mc/

Wilson, B., Porche, I., Eisman, M., Nixon, M., Tierney, S., Yurchak, J., Kendall, K., Dryden, J., & Critelli, S. (2016). *Maritime tactical command and control analysis of alternatives*. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1383/RAND_RR1383.pdf

United States Marine Corps. (1996). *Command and control* (MCDP 6). https://www.marines.mil/Portals/1/Publications/MCDP%206%20Command%20and%20Control.pdf

United States Marine Corps. (2017). *Marine Corps planning process* (MCWP 5-10). https://www.marines.mil/Portals/1/Publications/MCWP%205-10%20FRMLY%20MCWP%205-1.pdf?ver=2017-08-28-140131-227

United States Special Operations Command. (2021). *USSOCOM fact book 2021 [Fact sheet].* https://www.socom.mil/latest-factbook

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California