



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

SYSTEMS ENGINEERING CAPSTONE REPORT

**DATA MANAGEMENT FOR ARTIFICIAL INTELLIGENCE
MACHINE LEARNING IMPLEMENTATION ACROSS THE
DEPARTMENT OF THE NAVY**

by

Robert French, Wallace Y. Fukumae Jr., Kheng S. Hun, Obed Matuga,
and Caitlyn R. O'Shaughnessy

June 2021

Advisor:
Second Reader:

Bonnie W. Johnson
Scot A. Miller

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
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 Systems Engineering Capstone Report	
4. TITLE AND SUBTITLE DATA MANAGEMENT FOR ARTIFICIAL INTELLIGENCE MACHINE LEARNING IMPLEMENTATION ACROSS THE DEPARTMENT OF THE NAVY			5. FUNDING NUMBERS	
6. AUTHOR(S) Robert French, Wallace Y. Fukumae Jr., Kheng S. Hun, Obed Matuga, and Caitlyn R. O'Shaughnessy				
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) The private sector continuously harvests and curates key data and its sources so as to ensure the support and development of new operational insights, generated by leveraging data-intensive artificial intelligence machine learning (AI/ML) techniques. Industry culture affirms that all data are valued shared resources, an approach the Navy so far has failed to realize. This capstone explores the Navy's challenging task of creating data availability and quality through research, interviews, and personal expertise. Research focuses on process, technology, and governance, employing a detailed needs assessment, stakeholders' analysis, and functional design. The result is a conceptual framework for a centralized artificial intelligence library (CAIL), designed to match industry's resolute attention to data as a critical commodity. The Navy needs persistent and dynamic digital readiness, so this capstone team, with over 70 years of combined United States naval data expertise, recommends that OVERMATCH consider these findings and generate a system that ensures data availability and quality for the Navy.				
14. SUBJECT TERMS artificial intelligence, machine learning, AI/ML, data			15. NUMBER OF PAGES 135	
			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	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**DATA MANAGEMENT FOR ARTIFICIAL INTELLIGENCE
MACHINE LEARNING IMPLEMENTATION ACROSS THE
DEPARTMENT OF THE NAVY**

Robert French, Wallace Y. Fukumae Jr., Kheng S. Hun,
Obed Matuga, and Caitlyn R. O'Shaughnessy

Submitted in partial fulfillment of the
requirements for the degrees of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

and

MASTER OF SCIENCE IN ENGINEERING SYSTEMS

from the

**NAVAL POSTGRADUATE SCHOOL
June 2021**

Lead Editor: Caitlyn R. O'Shaughnessy

Reviewed by:

Bonnie W. Johnson
Advisor

Scot A. Miller
Second Reader

Accepted by:

Ronald E. Giachetti
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The private sector continuously harvests and curates key data and its sources so as to ensure the support and development of new operational insights, generated by leveraging data-intensive artificial intelligence machine learning (AI/ML) techniques. Industry culture affirms that all data are valued shared resources, an approach the Navy so far has failed to realize. This capstone explores the Navy's challenging task of creating data availability and quality through research, interviews, and personal expertise. Research focuses on process, technology, and governance, employing a detailed needs assessment, stakeholders' analysis, and functional design. The result is a conceptual framework for a centralized artificial intelligence library (CAIL), designed to match industry's resolute attention to data as a critical commodity. The Navy needs persistent and dynamic digital readiness, so this capstone team, with over 70 years of combined United States naval data expertise, recommends that OVERMATCH consider these findings and generate a system that ensures data availability and quality for the Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	PROBLEM STATEMENT	4
C.	PROJECT OBJECTIVES.....	4
D.	PROJECT TEAM AND ORGANIZATION	5
E.	PROJECT APPROACH	6
F.	CAPSTONE REPORT OVERVIEW	9
II.	LITERATURE REVIEW	11
A.	INTRODUCTION.....	11
B.	ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING SYSTEMS AND THEIR RELIANCE ON DATA.....	11
	1. Artificial Intelligence and Machine Learning	11
	2. Data Management for Developing Artificial Intelligence and Machine Learning Systems.....	13
C.	DOD AND DON DEVELOPMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS	15
	1. DOD and DON Artificial Intelligence Initiatives	15
	2. Defense Applications of Artificial Intelligence and Machine Learning	17
	3. Data Challenges for Artificial Intelligence and Machine Learning for Defense Applications.....	19
D.	ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS IN THE THREE NAVAL DOMAINS OF INTEREST	19
	1. System Maintenance	20
	2. Physical Security	20
	3. Battle Readiness	21
III.	NEEDS ANALYSIS.....	23
A.	STAKEHOLDERS	23
B.	NEEDS ANALYSIS FOR THE THREE NAVAL MISSION DOMAINS (DATA PROVIDERS).....	24
	1. System Maintenance	24
	2. Physical Security	27
	3. Battle Readiness	28

C.	NEEDS ANALYSIS FOR DATA NEEDS OF DON AI/ML DEVELOPERS (DATA USERS)	31
D.	NEEDS ANALYSIS ASSESSMENT AND RESULTS.....	35
1.	Insights from the Data Consumers.....	36
2.	Insights from the Data Providers	36
3.	DON AI/ML Data Management Requirements	37
4.	Needs Analysis Conclusion and Data Considerations	39
IV.	SOLUTION STRATEGY: CENTRAL ARTIFICIAL INTELLIGENCE LIBRARY (CAIL) SYSTEM	41
A.	CONCEPT OF OPERATION	41
B.	SYSTEM REQUIREMENTS	44
1.	Methodology	44
2.	Requirements Analysis	45
C.	CONCEPTUAL SYSTEM ARCHITECTURE AND DESIGN	48
1.	OV-1 Diagram	48
2.	Context Diagram and Subsystems.....	49
3.	Capability Views	52
4.	Operational Activities.....	55
5.	Assets.....	56
6.	Operational Activities / Event-Trace Descriptions (OV-5b/6c)	59
D.	SUMMARY	63
V.	EVALUATION AND ANALYSIS OF CENTRAL ARTIFICIAL INTELLIGENCE LIBRARY (CAIL) SYSTEM	65
A.	CAIL EVALUATION BASED ON THREE NAVAL MISSION DOMAINS	65
1.	CAIL Support for System Maintenance	65
2.	Evaluation of CAIL's Application to Physical Security Domain	68
3.	Evaluation of CAIL's Application to Battle Readiness Domain	69
B.	CAIL ALIGNMENT WITH THE DOD DATA STRATEGY	71
1.	Data Readiness	71
2.	Data Bias	73
3.	Data Curation.....	73
4.	Data Taxonomy	74
5.	Data Governance.....	74
6.	Data Security	74
C.	COST ANALYSIS	75

1.	CAIL Traditional Cost Assessment.....	75
2.	CAIL MBSE Cost Assessment.....	78
3.	Cost Summary	81
VI.	CONCLUSION	83
A.	TEAM TIME ZONE’S FINDINGS	83
A.	RECOMMENDATIONS AND FUTURE AREAS OF RESEARCH	86
B.	SUMMARY OF TEAM’S FINDINGS AND RECOMMENDATIONS.....	88
	APPENDIX A. INTERVIEW QUESTIONS.....	91
	APPENDIX B. DIAGRAMS	95
	LIST OF REFERENCES	101
	INITIAL DISTRIBUTION LIST	107

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	The Warfighter’s Complex Decision Space. Source: Johnson (2021).	1
Figure 2.	What Is AI? Source: Johnson (2021).	3
Figure 3.	Team Time Zone Organization Chart	6
Figure 4.	Capstone Project Approach.....	7
Figure 5.	DON Mission Domain	8
Figure 6.	Process Model for ML. Source: Raz et al. (2021).	12
Figure 7.	AI Trinity. Adapted from Raz et al. (2021).	13
Figure 8.	Challenges in Gather Data for Training AI/ML Systems in the Military Domain. Source: Johnson (2021).....	19
Figure 9.	Stakeholder AI/ML Data Considerations.....	40
Figure 10.	CAIL Concept of Operations	42
Figure 11.	CAIL System Conceptual Data Model	45
Figure 12.	Requirements Spider Diagram.....	46
Figure 13.	CAIL OV-1	49
Figure 14.	High-Level CAIL and Pre-CAIL System	50
Figure 15.	CAIL System	51
Figure 16.	CAIL CV-2	52
Figure 17.	Pre-CAIL CV-2.....	54
Figure 18.	OV-5a.....	55
Figure 19.	Capabilities to Operational Actions Mapping.....	56
Figure 20.	CAIL – SV-1	57
Figure 21.	CAIL System – SV-1	57
Figure 22.	Pre-CAIL System – SV-1	58

Figure 23.	CAIL – OV-1 modified.....	59
Figure 24.	CAIL – OV-5b/6c	60
Figure 25.	Pre-CAIL (Data Collection) – OV-5b/6c.....	60
Figure 26.	High-Level CAIL Capabilities – OV-5b/6c.....	61
Figure 27.	CAIL Governance – OV-5b/6c.....	61
Figure 28.	CAIL System – OV-5b or IDEF0	62
Figure 29.	System Maintenance – CAIL Event Trace	62
Figure 30.	Physical Security – CAIL Event Trace.....	63
Figure 31.	Battle Readiness – CAIL Event Trace	63
Figure 32.	CAIL Monte Carlo Simulation Results.....	80
Figure 33.	CAIL Sustainment Monte Carlo Simulation Results.....	81

LIST OF TABLES

Table 1.	Types of Data for Different ML Applications. Source: Boehm, Kumar and Yang (2019).	14
Table 2.	List of Stakeholders Interviewed	24
Table 3.	System Maintenance Interview Information.....	26
Table 4.	Physical Security Interview Information	28
Table 5.	Battle Readiness Interview Information	30
Table 6.	AI/ML Researchers (NPS) Interview Information	33
Table 7.	AI/ML Developer (NIWC) Interview Information.....	34
Table 8.	CAIL Traditional Cost Summary.....	77
Table 9.	CAIL Notional Human Resources Hours per Year	78
Table 10.	Schedule/Cost Risk Factor Multipliers	79
Table 11.	CAIL System – Model Parameters	79
Table 12.	CAIL System Cost Summary.....	82
Table 13.	Time Zone Prioritized Summary	89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	artificial intelligence
AIS	Automatic Identification Systems
AOR	area of responsibility
ATO	authority to operate
BUMED	Bureau of Medicine and Surgery
CAIL	Central AI Library
CASREP	casualty report
CDM	concept data model
CIO	Chief Information Officer
CIWS	close-in weapon system
CM	configuration management
CMI	component mission initiatives
CNIC	Commander, Navy Installations Command
COA	course of actions
CONOPS	concept of operations
DARPA	Defense Advanced Research Projects Agency
DIKW	data–information–knowledge–wisdom hierarchy
DISA	Defense Information Systems Agency-
DoDAF	Department of Defense Architecture Framework
DON	Department of Navy
ESS	electronic security systems
ESSM	Evolved Sea Sparrow Missiles

FTE	full time equivalent
HA/HR	humanitarian assistance, and disaster relief
IA	information assurance
ITSM	information technology service management
JAIC	Joint AI Center
JADC2	Joint All Domain Command and Control
LAWS	lethal autonomous weapons systems
LOGSA	Logistics Support Activity
MARCORPSYSCOM	Marine Corps Systems Command
ML	machine learning
N3S	Public Safety Systems
NAML	Naval Applications of Machine Learning
NATO	North Atlantic Treaty Organization
NAVAIR	Naval Air Systems Command
NAVFAC	Naval Facilities Engineering Command
NAVSEA	Naval Sea Systems Command
NAVSUP	Naval Supply Systems Command
NAVWAR	Naval Information Warfare Systems Command
NCARAI	Navy Center for Applied Research in Artificial Intelligence
NFFI	NATO Friendly Force Information
NIWC	Naval Information Warfare Center
NMI	national mission initiatives
NMP	Navy Modernization Process
NOC	Network Operations Center

NPS	Naval Postgraduate School
NRL	Navy Research Laboratory
NSWCDD	Naval Surface Warfare Center Dahlgren Division
ONR	Office of Naval Research
OPNAV	Office of the Chief of Naval Operations
PEO	Program Executive Office
PII	personally identifiable information
PMW	Program Manager, Warfare
R&D	Research & Development
RPM	revolution per minute
SCD	Ship Change Document
SE	systems engineering
SME	subject matter expert
SoS	system of systems
SoSE&I	system of system engineering and integration
SPIDER	System Command Program Executive Office Integrated Data Environment and Repository
SSDS	Ship Self-Defense System
SysML	Systems Modeling Language
TOI	targets of interest
USN	United States Navy

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Department of the Navy's (DON) interest in researching and developing artificial intelligence and machine learning (AI/ML) systems stems from the far-reaching and game-changing improvements these innovative capabilities will have across naval missions and in direct support to the warfighters. The AI/ML systems can be leveraged to improve mission planning, reduce manning, improve tactical decisions, streamline system maintenance and support, enhance security, and in some cases, remove warfighters from harm's way. Many aspects of a warfighter's daily activities will change, ranging from automating routine and labor-intensive work to supporting complex and time-critical battlespace decisions.

These advancements in AI/ML systems can only be accomplished if the DON harnesses the power of data by first unlocking it. Currently, many barriers exist to accessing or "freeing up" the DON data needed to develop AI/ML systems of the future. Data throughout the Navy largely resides in "silos" or hard-to-access databases, with each "silo" protected within its domain. The processes for locating, requesting, obtaining, and curating data are not formalized within the DON's data domains. Miller (2021) states, "The owners of the data are the American people. We in the Navy are just the caretakers and curators." This statement encompasses the need to "free" data from the silos in order to enable the DON to truly become a data-centric enterprise and achieve DON digital readiness.

This capstone project embarked on a study to understand the data needs of AI/ML developers within the DON and to develop a conceptual solution to address the data needs. Additional objectives were to:

- Study how AI/ML methods may be applied across DON missions.
- Understand whether data needs are generally standard across DON missions or whether data needs vary across DON missions.
- Develop a set of DON AI/ML stakeholder requirements.
- Develop a conceptual design for a system to support DON AI/ML data needs.
- Study potential cost and schedule benefits of implementing the conceptual solution system.

Team Time Zone applied a systems engineering analysis approach to study DON AI/ML developers' data needs and develop and assess a conceptual system solution to address this data challenge and ultimately support future DON digital readiness to address complex missions. The team performed a stakeholder needs analysis by interviewing subject matter experts (SMEs) across three different naval mission domains: system maintenance, physical security, and battle readiness. These three missions were deemed as representative of "data providers." Additionally, the team interviewed data researchers and AI/ML scientists to understand their data needs. The interviews provided the team with insight into the concerns, frustrations, lessons learned, and challenges based on the unique and diverse domains and experiences. Recurring themes from the data provider perspective included ownership demarcations, the need for information assurance, instances in which data are not collected or stored, and accessibility concerns. Pronounced anecdotes from the data user's perspective included the time-consuming effort to locate data, that promised data did not always come to fruition, and the critical importance of understanding the context for data even after it has been obtained. The team developed a set of data requirements for the DON AI/ML based on the stakeholder interviews and information gathering effort. The DON AI/ML data needs are:

- Data must be made accessible to outside organizations.
- Data must be translated into standard formats that are compatible with their domain application.
- Data must have identified owners.
- Data must be accompanied by descriptive metadata.
- Data must have governance for standardization.
- Data must be accessible in its "lowest common denominator" form.
- Data must have security for protection and proper sharing,
- Data must have obfuscation to protect personally identifiable information (PII).
- Data must be accompanied by contextual information.

To address the identified data needs of DON data researchers and AI/ML scientists, Team Time Zone developed a conceptual design of the Central AI Library (CAIL) system as the solution. The purpose of the CAIL system is to streamline data access and management within the DON to support AI/ML system development. The CAIL system is intended to decrease the time (and associated cost) that is spent accessing data and free up

more time for the actual development, training, and evaluation of AI/ML systems. The team proposes that in order to satisfy future program access and integration requirements, the CAIL needs to be a “Data Cloud.” Figure 1 is the OV-1 for the CAIL; it depicts the proposed process of streamlining DON data access and management for AI/ML development.

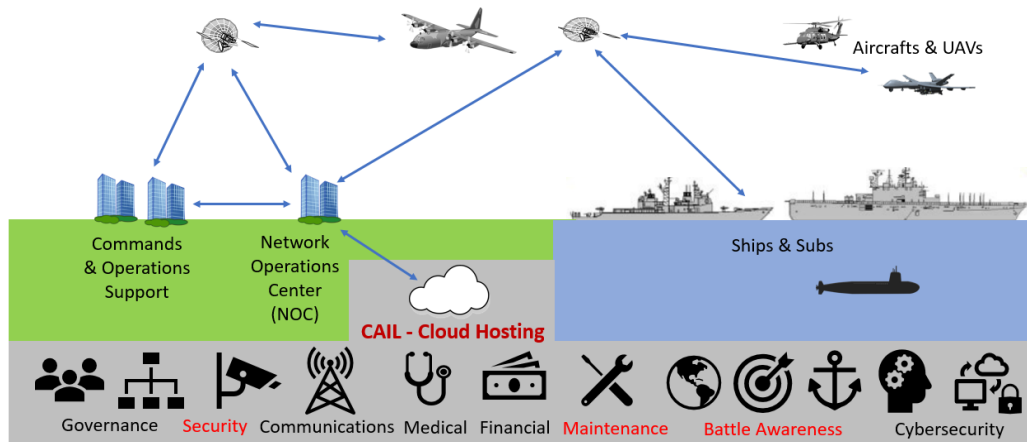


Figure 1. *CAIL OV-1*

The team developed CAIL system requirements according to six major categories: data readiness, data bias, data curation, data taxonomy, data governance, and data security. Each of these categories addresses a need that was identified during the stakeholder analysis. The CAIL system will primarily interface with external federated data, databases, documents, and content from authoritative data producers/providers. It will act like the “Google” for DON users to find data. The data will be structured and will be accompanied by metadata (descriptive information about the data) to allow the data to be searchable. A governing data community will provide rules to managed secure access and authorization to the data.

During the stakeholder’s analysis, it became apparent that there were vital activities that needed to happen before accessing data. The AI/ML developers explained the importance of understanding contextual aspects of how data is collected, where data originates, and other domain-specific aspects concerning the data. Team Time Zone

designated these processes as “Pre-CAIL activities” and captured them as part of the overall CAIL process.

Team Time Zone performed a cost analysis to estimate the cost of implementing the CAIL system for the DON. The team used two methods to estimate the cost: a traditional cost estimation and a model-based systems engineering (MBSE) approach. The team estimated a CAIL system cost (based on traditional cost estimation) of \$33.8M with a duration of five years and a reoccurring sustainment cost of \$4M per year. The team estimated a CAIL system cost (based on the MBSE approach) where ten thousand Monte Carlo simulations were ran had a mean of \$32.9M with a duration of five years. The operations and maintenance model had a mean cost of \$4.4M per year. A summary of the CAIL development and sustainment cost are shown below in Table 1.

Table 1. CAIL System Cost Summary

CAIL System Cost Summary				
	Traditional		MBSE	
Description	Duration	Cost	Duration	Cost
CAIL Development	5 years	\$33.8M	5 years	\$32.9M
CAIL Sustainment	1 year	\$4M	1 year	\$4.4M

In order for DON AI/ML programs to flourish and enable AI/ML advancements in the upcoming decades, the DON must ensure that data is managed and made accessible for AI/ML development. Team Time Zone’s proposed CAIL system solution will provide a single source integrated data environment for AI/ML programs to access a library catalog of data stored in various databases throughout the DON. Team Time Zone recommends that the Navy implement the CAIL system to support digital readiness by ensuring AI/ML developer access to persistent and dynamic digital data. The CAIL system supports a coordinated approach for DON programs and developers to gain secure access to the data they need. The team recommends that Project Overmatch consider these findings and implement the CAIL system and process to ensure data availability and quality for the Navy. The team developed a CAIL logo (in Figure 2) that shows the CAIL system as an important foundation for the Navy.

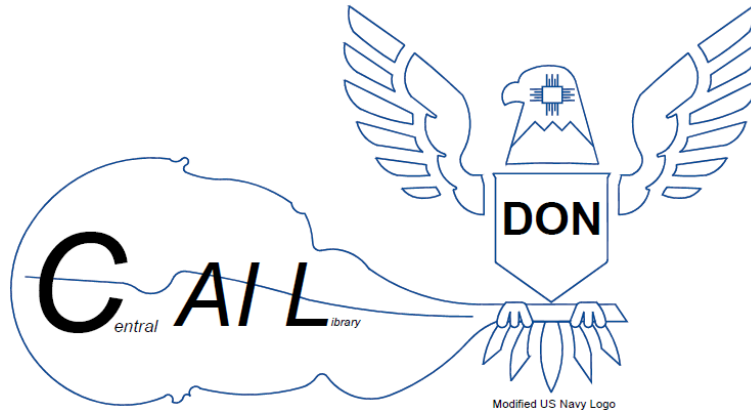


Figure 2: CAIL Logo. Adapted from U.S. Navy Logo.

References

- Department of Defense. 2020. *DOD Data Strategy 2020*. Washington, DC: U.S Dept of Defense. Accessed May 4, 2021. <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-Data-Strategy.pdf>.
- Johnson, Bonnie , and William A Treadway. 2019. “Artificial Intelligence — An Enabler of Naval Tactical Decision Superiority.” *AI Magazine*, March 28: 63–78.
- Johnson, Bonnie. 2021 “Artificial Intelligence Systems: Unique Challenges for Defense Applications.” *18th Annual Acquisition Research Symposium*. Monterey: Monterey: Acquisition Research Program.
- . 2020. “Predictive Analytics in the Naval Maritime Domain.” *Deep Models and Artificial Intelligence for Defense Applications: Potentials, Theories, Practices, Tools, and Risks 2020*. Virtual: AAAI. 69–77.
- Johnson, Bonnie, and John M Green. 2019. *Advanced Concepts and Applications for Predictive Analytics in the Maritime Domain*. Poster, Monterey, California. Naval Postgraduate School: Calhoun Home.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Team Time Zone would like to thank our families and friends for their support, as well as Dr. Bonnie Johnson and Captain Scot Miller, USN (ret.), for their continued time and guidance over the past year.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Advances in technology introduce new types of threats and improved versions of existing threats into the military realm. Adversarial threat advances require the Navy to improve existing capabilities and develop new ones to improve our defenses and address these threats. Capability enhancements require increased speed, stealth, maneuverability, countermeasures, extended range, earlier detection, and greater lethality. Those enhancements enable critical decisions under uncertain, complex, and time-critical conditions. Modern tactical warfighters face increasingly complex decision spaces. They need to gain situational awareness of dynamic battlespaces and determine effective courses of action (COAs) to meet mission demands. Figure 1 highlights factors that contribute to this tactical complex decision space. Decision complexity arises from the threat environment, from knowledge uncertainty, from the warfare and information systems themselves, from the challenges that arise from the warfighter's interaction with and use of automated and information systems, and the importance or severity of consequences with the mission decisions.

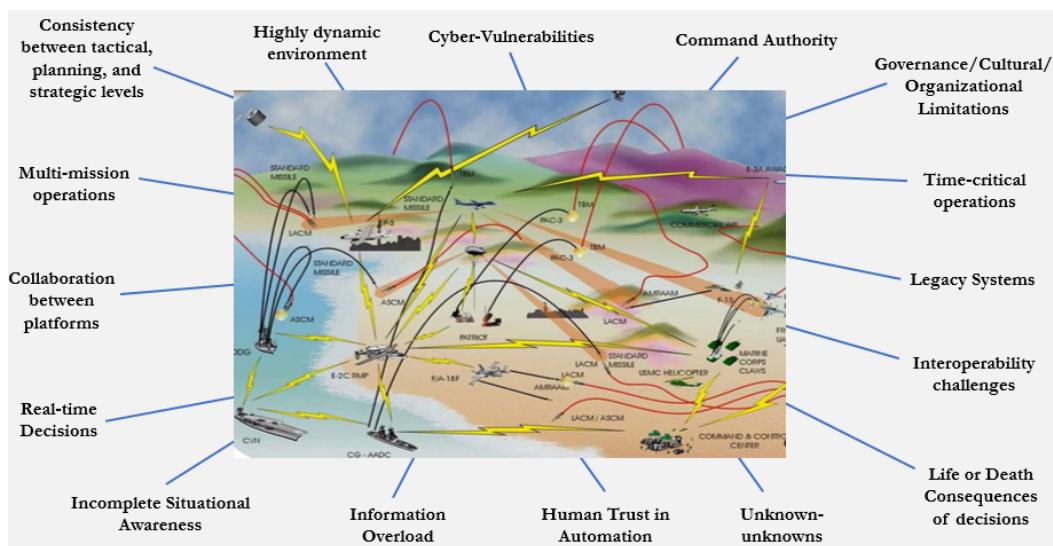


Figure 1. The Warfighter's Complex Decision Space.
Source: Johnson (2021).

The Department of Defense (DOD) and Department of Navy (DON) are investigating the use of artificial intelligence (AI) to address the complex tactical decision space by improving situational awareness and providing automated decision aids to support tactical warfighters. Advanced algorithms that leverage AI methods can lessen the warfighter's cognitive load by reducing information overload, improving situational awareness, increasing the pace of decision-making, and enhancing tactical decisions in general. Predictive analytics (PA) can support the prediction of system reliability and the probability of failures, which offers wide-ranging improvements to logistics (Zhao and Mata 2020). Technologies such as PA can enhance tactical decision-making by developing “what-if” and “if-then” scenarios to improve warfighter COA decisions by predicting the longer-term effects of decision alternatives (Johnson 2020). The AI methods can improve the physical security of naval bases by detecting anomalies and identifying possible threats from large amounts of security camera data.

Mitchell (2019) defines AI as a field that includes many different approaches to create machines with intelligence. Figure 2 shows that AI exists within an extensive set of automation methods that enable machines to perform tasks based on commands and rules. Artificial intelligence is the set of methods that enable systems to perform functions that mimic human intelligence. Machine learning (ML) methods are a subset of AI methods. The ML methods allow systems to learn from being trained on large sets of data. The ML systems learned from trained datasets. These “trained” ML systems are then used operationally to recognize patterns and produce predicted outcomes given new operational data (Johnson 2021).

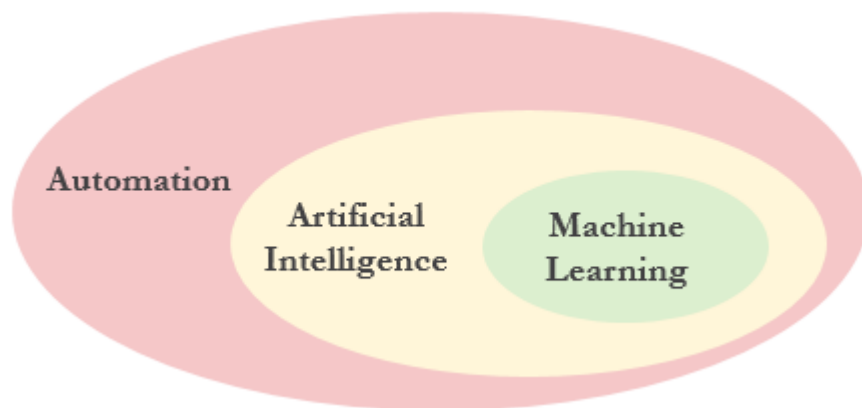


Figure 2. What Is AI? Source: Johnson (2021).

The AI algorithms are computer programs coded to classify, analyze, and draw predictions on data. Surveillance, traffic predictions, and virtual personal assistants are examples of applications that implement ML algorithms.

Developing AI systems, and particularly ML systems, is a challenging endeavor. The initial training of ML algorithms is a data-intensive evolution. The AI/ML systems are data-hungry, and their accuracy largely depends on the quality and quantity of the data training sets (Godbole 2020). As a reference point, it took approximately 40 days, including 29 million games, to train DeepMind's AlphaGo Zero system to learn to play the game of Go (Feldman, Dant, and Massey 2019). Imagine the additional complexity involved in an AI/ML weapons system algorithm that needs to factor in concepts such as war context (war games, cold war, peacetime), friend or foe, ethics, and legality (Feldman, Dant, and Massey 2019).

Unique data challenges arise as the DON begins to develop AI and ML methods. Developers need massive amounts of validated data to train their algorithms; this data needs to be accurate, secure, and complete to ensure the algorithms do not become corrupted or biased. The data sets must represent the appropriate operational environment. For naval applications, training data must represent a multitude of missions, including those in the maritime, air, space, underwater, littoral, cyber, and land-based domains. Although many DON commands and laboratories are researching and developing future capabilities based on AI/ML systems, there is no coordinated process for programs to

access the DON data they require. In many cases, the data exists, but it is a time-consuming and costly effort to identify DON data sources and gain access to the data.

This capstone project applied a systems engineering analysis approach to study DON AI/ML developers' data needs and identify and assess a conceptual system solution to address this data challenge and ultimately support future DON digital readiness to address complex missions.

B. PROBLEM STATEMENT

The DON's interest in researching and developing AI/ML systems has presented a data challenge for various applications. Although many DON commands and laboratories are researching and developing future capabilities based on AI/ML systems, there is no coordinated process for programs to access the DON data they require. The AI/ML systems need large amounts of validated data to support their development and train algorithms. In many cases, the data exists, but it is a time-consuming and costly effort to identify DON data sources and gain access to the data. This capstone studied this problem and conducted a needs analysis to identify the data needs of DON AI/ML developers and developed and evaluated a solution concept for addressing this aspect of DON digital readiness.

C. PROJECT OBJECTIVES

The primary objectives of this capstone project were to analyze the data needs of DON AI/ML development and develop a conceptual solution to address the data needs. Additional objectives were to:

- Study how AI/ML methods may be applied across DON missions.
- Understand whether data needs are generally standard across DON missions or whether data needs vary across DON missions.
- Develop a set of DON AI/ML stakeholder requirements.
- Develop a conceptual design for a system to support DON AI/ML data needs.

- Study potential cost and schedule benefits of implementing the conceptual solution system.

D. PROJECT TEAM AND ORGANIZATION

Team Time Zone consisted of five NPS systems engineering students with diverse academic and professional experiences. The team consists of:

- Robert French graduated in 2016 with bachelor's degrees in Computer Engineering and Electrical Engineering from Old Dominion University. He is currently the R.F. Engineer for the Special Sensors Technology division at Naval Surface Warfare Center Dahlgren Division-Dam Neck Annex in Virginia Beach, Virginia. Robert is also the Senior Enlisted Leader (USNR) for U.S. Fleet Forces Command, Maritime Operations Center N6 (Information Systems). He was an Electronics Technician on Active duty for over 14 years and has been an active Reservist for nine years.
- Wallace Fukumae has an electrical engineering degree from the University of Hawaii. He currently resides in Hawaii, working for the Naval Information Warfare Center Pacific as the Indo-Pacific Department Head. His experience includes the development and delivery of Command and Control (C2) systems and operations.
- Kheng Hun currently resides in Japan and has an electrical engineering degree from the University of Washington. He is presently working for Naval Information Warfare Center (NIWC) Pacific as a Project Engineer in the Hawaii Western Pacific (HWP) Branch in Yokosuka, Japan. His professional background includes designing and installing various C4I systems such as electronic security systems (ESS) and network systems and C4I systems planning for MILCON projects.
- Obed Matuga has an Industrial Engineering degree from Morgan State University in Baltimore, Maryland, working for Naval Sea Systems

Command in Washington, DC. Work with Aegis and Ship Self Defense System (SSDS) and currently resides in Maryland.

- Caitlyn O'Shaughnessy graduated in 2015 with a bachelor's degree in Computer Science from the University of Massachusetts at Dartmouth. She is currently the Lead Engineer for the CANES (S.S.) project at the Naval Undersea Warfare Center in Newport, Rhode Island.

Figure 3 depicts the Team Time Zone's organization structure and the primary responsibilities of each team member. The figure also shows the NPS project advisors, Dr. Bonnie Johnson (Systems Engineering Department) and CAPT Scot Miller, USN (ret.) (Information Sciences Department).

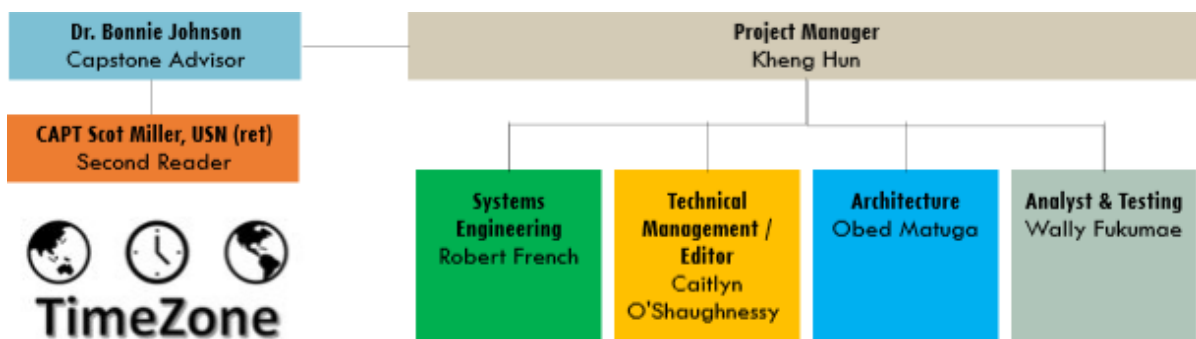


Figure 3. Team Time Zone Organization Chart

E. PROJECT APPROACH

Team Time Zone followed a system engineering approach to conduct this project. Figure 4 illustrates the team's process. The team began with a needs analysis to understand the problem and define the data requirements for DON AI/ML developers. During this phase, the team identified three DON mission domains as representative areas for AI/ML applications. Next, the team developed a conceptual design of a solution strategy called the Central AI Library (CAIL) system, based on functional analysis and system synthesis. The team modeled the CAIL system and used the three DON mission domains to analyze the utility and potential cost/schedule benefits of implementing the CAIL system. The team's

process involved several analytical methods, including qualitative investigation, quantitative investigation, modeling and simulation, analysis of data structures and formats, requirements analysis, and concepts of operation evaluation.

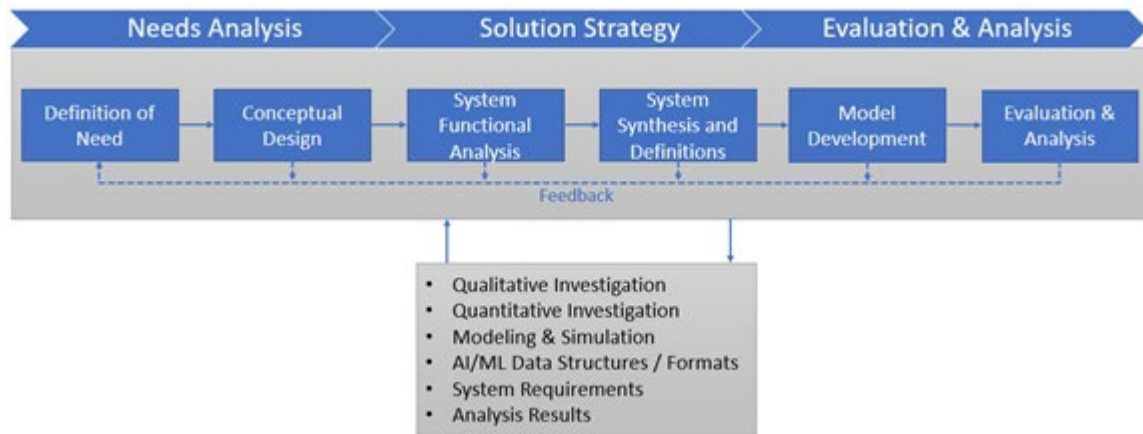


Figure 4. Capstone Project Approach

First, the team established the definition of need by conducting a needs analysis and developing a set of data requirements for naval AI/ML developers. The team identified stakeholders and met with AI/ML developers from diverse naval mission areas to understand their data needs. The team conducted a literature review to gather background information and to understand current AI/ML methods. The team compiled the information from the stakeholder meetings and literature review to understand the requirements and constraints, data owners, data sources, data systems, data elements, and data attributes related to supporting AI/ML applications for the Navy.

The team researched and identified stakeholders and unique data requirements on three naval mission threads: system maintenance, physical security, and battlegroup readiness. The team identified and interviewed subject-matter experts (SMEs) in the mission domains to understand the process of obtaining data for AI/ML implementation and to focus on what data needs to be gathered and stored from DON systems and organizations. Figure 5 illustrates the three naval mission threads and the direct underlying

importance of data, architecture, infrastructure, and interoperability capabilities are in support of these warfighter mission domains.



Figure 5. DON Mission Domain

Next, the team developed a conceptual design solution to address the Navy’s data needs for AI/ML development based on the needs analysis results. The team synthesized the CAIL system and generated a CAIL concept of operations (CONOPS) and CAIL functional model. Based on the DOD Architectural Framework (DODAF) and Systems Modeling Language (SysML), the team developed conceptual models that detail the CAIL’s system characteristics, functions, and operational concepts.

The final phase of the capstone project was the team’s evaluation and analysis of the CAIL solution approach. The team developed a model using Innoslate (a model-based systems engineering tool) to represent the use of the CAIL system in each of the three naval mission threads. The team evaluated the CAIL system’s ability to streamline and improve the process of gathering, formatting, curating, validating, and ensuring secure access to naval mission data sets to support AI/ML developers working in the three maritime mission thread domains. The model was evaluated to estimate potential cost and scheduling benefits

for the Navy's implementation of the CAIL system. The CAIL system model was employed to verify and validate requirements.

F. CAPSTONE REPORT OVERVIEW

Chapter I provided an introduction and motivation for the project, a description of the problem statement, project objectives, and the team's organization and approach to completing the project. Chapter II summarizes the team's literature review, which provided a foundation for the needs analysis, emphasizing the data required to train AI and ML algorithms. The literature review includes information exploration on data science, statistical learning, deep learning, taxonomy, and enterprise information technology solutions to support AI and ML systems. Chapter III contains the results of the team's needs analysis. Chapter IV contains a description of the team's conceptual solution, the CAIL system. Chapter V presents the results of the team's analysis and evaluation of the CAIL system as a solution to address the Navy's data challenges to support AI/ML development. Finally, Chapter VI discusses the impacts and conclusions of having a CAIL system and recommendations for follow-on research and efforts.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

Team Time Zone conducted a literature review to gain an understanding of (1) the data challenges involved in engineering AI/ML systems, (2) the current DOD/DON plans and approaches for implementing AI/ML, and (3) the AI/ML applications in the three naval mission domains of interest (system maintenance, physical security, and battlegroup readiness). The team identified and reviewed various articles and books on AI, ML, and related data concepts and management. The team reviewed DOD and DON reports and plans explaining how they organize and approach efforts to develop AI/ML systems. Finally, the team reviewed research papers on how AI/ML is being implemented in the three naval mission domains of interest.

B. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING SYSTEMS AND THEIR RELIANCE ON DATA

The team began the literature review by researching articles and books on AI/ML. The team found that a vast number of literature sources exist on AI since the field emerged in the 1940s when Warren McCulloch and Walter Pitts proposed a model of artificial neurons (Norvig 2021). The team studied the types and characteristics of AI and ML systems to understand and study how these systems rely on data.

1. Artificial Intelligence and Machine Learning

AI is the broad field that focuses on developing computer software code to create machines that can “think.” There is no “one thing, one technique, one algorithm, or even one objective” that encompasses AI. There are two primary types of AI: explicitly programmed systems and systems that learn from data. Explicitly programmed systems “use traditional, rules-based software to codify subject-matter knowledge of human experts into a long series of programmed if given x input, then provide y output rules” (Faisandier, Roedler, and Adcock 2020). The second type are ML systems that are trained and “learn” from large sets of data. The ML systems first “learn” from the trained datasets, and then

the “trained” ML system are used operationally to produce predicted outcomes given new operational data (Johnson 2021).

Both types of AI systems require data as input to function during operations; however, ML systems require significant amounts of data during development. Figure 6 illustrates the process of developing and deploying an ML system. The process begins with gathering and preparing data. The data is then used to train ML algorithms. The trained ML system is then deployed and can also be continuously improved through more “training” or “learning.” The three types of ML learning or training methods are supervised, unsupervised, and reinforcement. All three types of ML learning require training datasets.

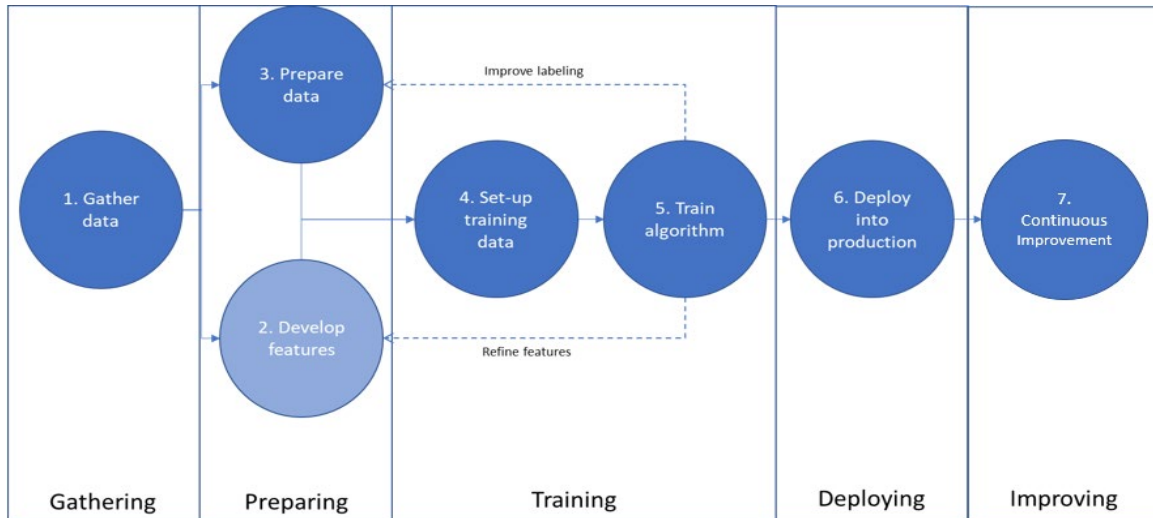


Figure 6. Process Model for ML. Source: Raz et al. (2021).

Johnson (2021) characterizes the relationship between ML systems data as “intimate” during the systems engineering and acquisition life cycles. Johnson (2021) explains that ML systems “emerge” from the process of learning on training datasets and that ML systems are a product of the quality, sufficiency, and representativeness of the data. If there are issues within the training datasets, they will negatively affect the developed ML system. Examples of failure modes that can occur due to this issue are biased, skewed, corrupt, and uncertain outcomes and predictions. Suppose the ML system

is trained on data that is not accurately representative of the intended operational use of the system and its operational environment. In that case, the ML system will produce output (often in the form of commands, courses of action, recommendations, predictions, etc.) that is either not useful for the operations or is just plainly wrong (Raz et al. 2021).

A useful way of thinking about the development and deployment of AI/ML systems is by the “AI trinity,” illustrated in Figure 7. The AI trinity consist of algorithms, data, and infrastructure. The three aspects are the cornerstones of AI systems. Algorithms provide the mathematical logic and data analytic methods, data is integral to AI development and operations, and the infrastructure of the computational hardware, architecture, and processing capabilities power provide the physical essence and foundation for AI systems. The AI systems will evolve and continue to improve in the future as advances are made in algorithmic methods, the harnessing of more datasets, and advances in computing power and cloud infrastructure.

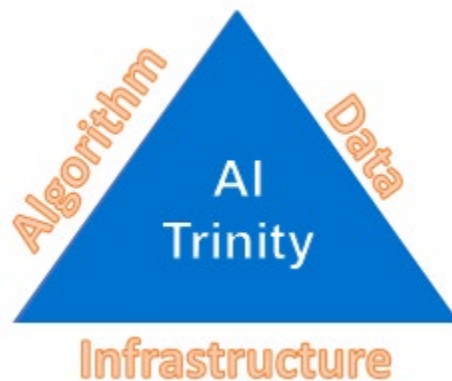


Figure 7. AI Trinity. Adapted from Raz et al. (2021).

2. Data Management for Developing Artificial Intelligence and Machine Learning Systems

Team Time Zone reviewed books related to data management and metadata to understand how these data concepts apply to AI/ML systems. These resources (Pomerantz 2015), (Boehm, Kumar, and Yang 2019), and (Bossé, Roy, and Wark 2007) provided

insights into the importance of governing and managing data and explaining data management methods and challenges.

Different types of ML systems use different types of data. The data type can affect how data is managed, organized, and accessed. Table 1 describes different types of data that are used for training different types of ML systems. Boehm et al. (2019), explain that the preparation of ML training datasets will be highly dependent on the type of ML system being trained due to the type of data that is used (Boehm, Kumar, and Yang 2019).

Table 1. Types of Data for Different ML Applications. Source: Boehm, Kumar and Yang (2019).

Types of Data for ML Systems	Description
Array-oriented	Large multi-dimensional arrays are a common form of data in many scientific data processing applications.
Time Series-oriented	Multi-variate time series datasets that often support forecasting methods to predict future values of variables
Text-oriented	Data in the form of text that often includes text from the Internet
Graph-oriented	Data in the form of “graphs” or relational data connected to other data (nodes or vertices and links). This data is often used in social media or Internet applications
Multi-media-oriented	Content-based data that often supports queries for the semantic content of images and videos

The development of ML systems relies on training datasets. Boehm et al. (2019) describe a “data generating process” as the first step in any ML development endeavor. This process involves gathering and “massaging” the training data into a form that can be used to develop the ML system. Boehm et al. (2019) emphasize the importance of this process and explain that ML is an example of “garbage in garbage out”—if the training data does not adequately represent the data distribution that the model will “see” operationally when the ML system is deployed, or if the training data is riddled with data errors, the ML models could fail in unexpected ways. The data generating process is called “sourcing” data for ML. This process requires a diverse set of tasks, including procuring data from their sources, representing the data in an “ML-friendly” manner, getting high-

quality labels for supervised ML, validating and cleaning the values in features and labels, overseeing and evaluating the ML predictions or outcomes, and overseeing and evaluating the operational data that will “feed” the trained ML system during deployment (Boehm, Kumar, and Yang 2019).

Team Time Zone also studied metadata, which is a set of data that accompanies datasets and provides information about the datasets, such as the source, origin, a timestamp, and other descriptive and contextual information. Metadata often plays a vital role in data management, especially when understanding the source of the datasets is needed. Pomerantz (2015) explains that “Metadata is a map. Metadata is a means by which the complexity of an object is represented in a simpler form.” Proper data governance and curation require structured data descriptions for the data set. The community of interest must adhere to this structure appropriately, thus providing a road map for data researchers to locate the data.

A simple example of training an ML system is the use of ML to identify targets of interest (TOI) from satellite imagery. In the maritime domain, the training process would require large datasets of satellite imagery of ships. For supervised learning, the training datasets would identify TOI’s within the satellite imagery training data. The ML algorithm would be trained to identify these TOIs. Once the training is complete, the ML algorithm can be deployed and used operationally to find TOIs from a real-time feed of operational satellite imagery. Some nuances in this example include making sure the ML can differentiate coastlines and clouds, and thus partial images of vessels. More advanced techniques in this example might expand detecting ships to adding an ability to classify whether the ship is a merchant, fishing boat, or warship.

C. DOD AND DON DEVELOPMENT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS

1. DOD and DON Artificial Intelligence Initiatives

Current DON organizations working on AI/ML applications include the Office of Naval Research (ONR), the Naval Research Laboratory (NRL), and the Naval Postgraduate School (NPS). ONR’s Division 333 is researching improvements to target acquisition,

imaging, and identification training by training deep neural networks (a type of ML system) using imagery data (ONR 2021). They are investigating the software and hardware implementation of deep learning algorithms and training algorithms with data optimization and regularization schemes that work with large data sets. The NRL has established the Navy Center for Applied Research in Artificial Intelligence (NCARAI) to focus on adaptive systems, intelligent systems, interactive systems, and perceptual systems (NRL 2021). Their mission includes basic and applied AI research on intelligent agents, human-machine teaming, machine learning, and autonomous systems. The NPS is pursuing AI research in a number of defense applications including data analytic methods for improving tactical situational awareness and weapon engagement decisions; predictive analytics and game theoretic methods for mission planning and tactical decision-making; and machine learning systems to support directed energy warfare, cyber warfare, naval logistics, air and missile defense, and many other applications.

DOD established the Joint AI Center (JAIC) in 2018 and released a report detailing the DOD AI strategy in the same year. The JAIC national mission initiatives (NMIs) include predictive maintenance, humanitarian assistance, and disaster relief (HA/HR). These initiatives were selected because of the shared cross-domain problem set. Furthermore, the JAIC also supported component mission initiatives (CMIs) which were tailored AI deployments specific to the need of the individual DOD agency (DoD, Summary of the 2018 Department of Defense Artificial Intelligence Strategy - Harnessing AI to Advance Our Security and Prosperity 2019).

The U.S. federal government is forecasted to spend 6 billion dollars in 2021 on AI research and development, a 50% increase from 2020 (Harper 2021). Congress' appropriation bill for 2021 provided \$137 million for the JAIC (Harper 2021). The increase in spending and large AI investment within DOD shows that the U.S. government is investing heavily in the future of AI/ML capabilities and understands the potential benefits for defense applications.

2. Defense Applications of Artificial Intelligence and Machine Learning

The DON is studying the rapid advances in AI and ML in the commercial sector and is researching ways to apply these methods to naval applications. The AI/ML systems offers potential capability enhancement as well as new capabilities in many naval applications. Johnson and Green (2019) describe how AI applications can enable naval tactical decision superiority, including “fusing and analyzing data to improve situational knowledge; generating and assessing decision options from multi-dimensional complex situations; and providing predictive analytics to identify and examine the effects of tactical courses of action.” The AI/ML methods can essentially improve all aspects of the tactical kill chain. Many research projects are studying the use of AI/ML to improve mission planning and military wargaming (Zhao and Mata 2020) (Ganzfried, Laughlin, and Morefield 2019).

Earlier references to the use of AI for defense include a report by Heinze, Simon, and Pearce (1999) that discussed the possibilities of integrating an ML agent in the complex domain of air combat. In this concept, the ML agent would ingest data to develop situational awareness and then develop and execute a tactical decision. This process first requires data to train the ML agent for it to recognize eight possible flight conditions. The Artificial Intelligence and National Security (2020) report detailed examples of AI/ML use in ISR, logistics, cyberspace operations, information operations, command and control, semiautonomous and autonomous vehicles, and lethal autonomous weapons systems (LAWS) (Sayler 2020). Project Maven “used computer vision and AI algorithms to automatically identify hostile activity for targeting” which was normally completed by a human analyst. The report also detailed the Army’s Logistics Support Activity (LOGSA) which had a tailored maintenance schedule for their Stryker fleet that was created by IBM’s Watson AI software. In the cyberspace domain, DARPA held a competition for the development of an AI that could detect, evaluate, and patch software vulnerabilities before a competing team have a chance to exploit them. The DARPA is also investing in AI that can detect realistic photo, audio, and video otherwise known as “deep fakes” to combat target influence or blackmail. The DOD is developing a Joint All Domain Command and Control (JADC2) system that will combine “planning and execution of air-, space-,

cyberspace-, sea-, and land-based operations” in order to provide decision makers with a single source of information. The Navy is currently testing the Sea Hunter, an Anti-Submarine Warfare Continuous Trail Unmanned Vessel prototype, that provides the ability to survey the open sea without the need for a human crew on board. The LAWS weapon system has the potential to disrupt modern warfare with the ability to have machines make kill decisions though the DOD does not possess nor support its use in live operations currently. A presentation by the JAIC detailed the use of AI in the medical field to improve warfighter health through efficiencies with health record analysis, medical imaging classification, suicide intervention and prevention, and point of injury treatment support (JAIC 2020). These domains converged on the importance of data as the enabler for data analytics and machine learning models.

In 2021, the DON held its 5th annual workshop in 2021 on Naval Applications of Machine Learning (NAML). The workshop has been growing each year and includes panels and tracks on a diverse set of topics including cyber security, computer vision, ML in operational environments, reinforcement learning applications, ML for radio frequency applications, maritime domain awareness, predictive analytics, and ML for naval biomedical applications. This workshop is another indication of the DON growing interest in AI/ML and the potential applications for the navy.

In all the scenarios mentioned above, the barrier for entry is not only identifying the data needed in advance but also how to best capture that data and present it to be used to train ML systems properly. To achieve even primitive ML recognition, there is a need to have enormous amounts of data upfront to train the ML programs. Without this initial data, any DON ML program will incur significant setbacks from its inception, which would include not being precisely trained or schedule delays waiting for data. This observation resonated with this capstone team and became the inspiration for studying this challenging problem.

3. Data Challenges for Artificial Intelligence and Machine Learning for Defense Applications

The AI/ML systems require large amounts of data for training and during operations and it turns out that the data generating process, or sourcing of data, is a time-consuming and challenging endeavor. Boehm et al. (2019, 101) write that “according to recent surveys of data scientists in practice, all data-related processes typically consume 80–90% (if not more) of the time and effort spent by most data scientists” to be trained and function accurately. The AI/ML researchers within DON are also finding that they are spending more time finding usable data than developing algorithms. The data generating process in the military domain has some additional challenges as shown in Figure 8. Johnson (2021) highlights that data may be classified, data may present cyber-attack vulnerabilities, and DON may need to conduct fleet exercises and/or wargames in some cases, to collect datasets. These challenges can be costly and time-consuming.

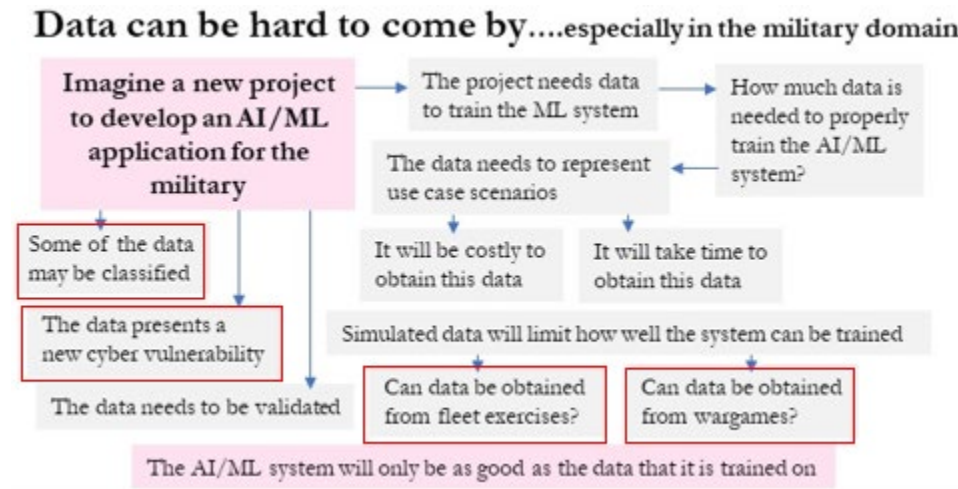


Figure 8. Challenges in Gather Data for Training AI/ML Systems in the Military Domain. Source: Johnson (2021).

D. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS IN THE THREE NAVAL DOMAINS OF INTEREST

Team Time Zone identified and explored three different naval mission domains to understand the similarities and differences in AI/ML applications for these domains. The

team wanted to study the similarities and differences to understand whether the three domains would each have a separate set of data needs for the development of AI/ML systems. This would help the team figure out if the DON could implement a standard process to gather and manage data for training ML systems or whether the process might have to be tailored to support different naval missions. The team conducted a literature review to gain more insight into the types of AI/ML applications being developed in three naval mission domains: system maintenance, physical security, and battle readiness.

1. System Maintenance

In the field of system maintenance for a naval ship, an “AI/ML-based prescriptive maintenance system...shifts the onus of prediction and expertise from the human to the assets or equipment” (Godbole 2020, 19). As such, the ship’s industrial equipment must have sensors that allow for the monitoring and logging of the equipment’s performance-related data. An article written by Coraddu (2015) gives examples such as ship speed, gas turbine shaft torque, gas generator rate of revolutions, and fuel flow data as example datasets to be factored into an ML model for the prescriptive maintenance of a naval gas turbine. These examples from literature support Team Time Zone’s premise that data at the lowest level are the ideal datasets for ML models because they are generated at the lowest levels, minimizing any data bias.

A report written by CDR Amrut Godbole (2020) of the Indian Navy detailed several military uses of AI/ML for the coming decades. For instance, benefits in inventory management could improve cost savings because the ML system could predict when equipment or sensors approach a high likelihood of failure. This enables the availability of spare equipment to apply a just-in-time model where items are not overstocked, leading to the excessive initial investment, storage, and transportation costs/space. Another AI/ML application in the maritime domain is an AI system that can find and identify rust, which is normally a time-consuming task (Atherton 2020).

2. Physical Security

Maritime surveillance is an essential aspect of port operation’s physical security mission. Typical systems deployed to assist with surveillance include video camera

systems, radar systems, and Automatic Identification Systems (AIS). Lei (2020) discusses data aspects for AIS and the many issues involved with using the data for visualization modeling, including size, error, reduction requirements, and normalization. The AIS data is a large dataset that could produce millions of data items in a single day (Lei 2020). Therefore, it was determined that data cleaning, by performing data reduction, data type mapping, and data normalization to organize the data in a useable form was required. This article provided the viewpoint that even though data was being generated at the sensor level, the information still required a methodology to clean it up involving human judgment, which produces human error and assumptions leading to data biasing. This article provided a great perspective that large datasets generated by sensors may not always be usable right away. Another example is the use of AI/ML to enhance perimeter detection and efficiency in coordinated security response times (Godbole 2020).

Lastly, AI/ML methods can help make security and surveillance become more reliable. The ML system could enhance real-time and continuous supervision of perimeters, alerting warfighters when a genuine threat is present such as a drone versus a bird.

3. Battle Readiness

In the domain of Battle Readiness, it is vital to develop and maintain superior battlespace knowledge to have the tactical advantage. Johnson (2019) developed a conceptual framework for an automated battle management aid which factored in a blue force model and a red force model for the AI/ML system to provide courses of action (COA) to the warfighters. Bodenmüller's (2013) article provides insights about the NATO format to exchange friendly force information called NATO Friendly Force Information (NFFI). The information included in NFFI includes data such as coordinates, target speed, bearing, time of measurement, and identification data. This information could assist an AI/ML system that is "always-on," allowing for response to threats that are beyond the capability of real-time human supervision (Feldman, Dant, and Massey 2019). The warfighters can focus on making decisions based on the AI/ML recommendations. In scenarios where decisions are required to be made in a limited amount of time, the decision-makers may not have the mental ability or technical capability to evaluate all applicable

variables within the battlespace. A final example is the use of AI/ML to improve the training of warfighters on a Navy ship to make training more efficient. The ML systems could train warfighters step-by-step through any type of training scenario.

III. NEEDS ANALYSIS

Team Time Zone conducted a needs analysis to understand the data needs of DON AI/ML developers and to understand how DON data is currently managed. The team conducted a series of stakeholder interviews in each of the three naval mission domains (system maintenance, physical security, and battle readiness) to find out what types of activities within each domain may be improved with the use of AI/ML capabilities, what types of data would be needed to support the development of those AI/ML capabilities, and the current status of data management for the data of interest. Current data management status included finding out whether the data currently exists, whether it is in a form that is useful for AI/ML developers, and what challenges exist in making the data available to AI/ML developers.

The team compiled and assessed the information from the stakeholder interviews to study the similarities and differences in the data needs across the three naval mission domains. The team produced a consolidated set of results which contain data considerations for DON AI/ML development.

A. STAKEHOLDERS

Team Time Zone interviewed both data providers and data users to acquire a holistic view regarding data challenges. From the data providers, information such as operational views, system integration views, and system user views were described to the team. This information provided context for each domain's current state of data and the daily problems they faced. The domain experts also expressed how AI/ML could make certain tasking more efficient which would reduce cost and labor for their respective programs.

The data users provided the team with firsthand anecdotes of the challenges that data scientists, data researchers, and AI/ML researchers faced. One common frustration was the challenging and time-consuming effort that was required to find data to support their research. They all agreed that it was critical to use real-world datasets to properly train ML algorithms. The developers could start with simulated data or data from table-top war

gaming exercises, but that ultimately real operational data would be required to train ML systems for actual deployment.

Some of the challenges that the AI/ML researchers faced in trying to obtain data included data classification, data ownership or governance issues, and security issues. In some cases, the data existed but was not stored, and so it was not possible to obtain. In other cases, the data did not yet exist, but AI/ML researchers could work with DON officers and engineers to obtain it. The AI/ML researchers agreed that obtaining useful data was a lengthy and often costly part of their projects.

Table 2 contains a list of the stakeholder experts that the team interviewed for the need's analysis. Appendix A contains the list of questions that the team asked each stakeholder.

Table 2. List of Stakeholders Interviewed

Interviews			
Data Category	Domain	Role	Organization
Data Providers	System Maintenance	N3S Director	CNIC
	System Maintenance	N3S Deputy Director	CNIC
	Physical Security	Shore Platform Integration Head	NIWC
	Physical Security	Lead Software Engineer	NIWC
	Battle Readiness	Technical Director	PEO IWS
	Battle Readiness	Security Systems Specialist	NSWC
Data Users	AI/ML Developer	Scientist	NIWC
	AL/ML Researcher	Research Professor and Data Scientist, Information Sciences	NPS
	AL/ML Researcher	Researcher and Data Scientist, Information Sciences	NPS

B. NEEDS ANALYSIS FOR THE THREE NAVAL MISSION DOMAINS (DATA PROVIDERS)

1. System Maintenance

Team Time Zone interviewed the CNIC N3S Director of Sustainment for public safety systems such as electronic security systems (ESS) and giant voice. Some of the main

issues they faced in the maintenance domain included configuration management, data collection quality, contract management, corrective maintenance tracking, and data sharing.

The CNIC N3 public safety program manages many systems supporting capabilities required for the public safety mission. Remedy, the information technology service management (ITSM) system, serves at the heart of their maintenance management system and provides the database and tools used to initiate, track, and close out tickets related to corrective maintenance actions. The method depends on user-entered data. Metrics such as operational availability, component failure rates, response times, and customer satisfaction are entered. User-entered data are susceptible to mistakes, and since users only enter information they believe is of value, the existing data is biased. Only portions of data captured are shared with customers via their Microsoft SharePoint as the front-facing website. The rest is deemed sensitive, such as failure rates and security information.

Configuration management remains a significant issue. The existence of different system types and baseline versions across the Navy enterprise complicates configuration management. They cannot monitor all the remote systems and are only 75%–80% sure of their information on the deployed Navy systems. Contributing factors include sites upgrading their system outside of the N3S program and leaving old systems in place after a technical refresh, which leads to inventorying the old methods as part of the deployed systems survey. These issues add to the resources needed to complete the Navy installations worldwide surveys. They stated that AI and ML could help provide analysis on predictive failures, which would help keep systems' operational availability high. They currently depend on contractors to advise on technical replacements as an option to mitigate issues. An AI/ML system could inform them of these failure rates and provide deeper reasoning for their failures. Table 3 summarizes the information gathered from the System Maintenance domain.

Table 3. System Maintenance Interview Information

System Maintenance		
State of Data	1	Maintenance data such as service times are currently entered by humans into databases.
	2	Data entered by humans needs to have a sanity check to filter out outlier data.
	3	Access to failure rates and security info that is still sensitive are restricted.
	4	Data is being collected to perform trends analysis for failure rates and service contractor performance based on metrics from the contract.
	5	Data is being collected from customers to assess their satisfaction level.
	6	Reports, analysis, and incident/trouble ticket data can be provided to customers.
	7	Limited physical security data for research right now due to policy such as cybersecurity requirements. (Should this be “maintenance” rather than “physical security”?)
	8	Contractor response times are tracked weekly, monthly, and quarterly.
Current Operations	1	Program tools exist to help manage program level stuff, PM, help desk, asset data.
	2	A Configuration Management (CM) issue is that legacy systems are often left in place after technology refresh or upgrades occur without informing the CNIC N3S Sustainment program.
	3	Current system information is only 75%-80% accurate. A real time AI/ML tool that could discover devices that are obsolete or not part of baselines would help remove human error.
	4	Connecting to a data repository that could provide end of life (EOL) or end of sales (EOS) data for equipment would provide much needed planning time for asset replacements.
	5	CNIC N3S currently has four separate sustainment contracts.
	6	RPM – Regional Project Manager, government personnel stationed in every navy region, perform QA in the field.
	7	Operational availability, monthly tickets, and derived report cards on contractors are based on metrics specified by SLA in contract.
	8	There is a current program to set up a customer portal to allow customers to submit their own tickets, pull trouble reports, and look up status on open trouble tickets.
	9	Work with customers at the region and installation level to understand what data the customers wants.
	10	AI/ML could help with predictive failures. For example, based on current and past data, the AI/ML system could specify a fail-by date allowing time to correct the issues.
	11	Program funds were allocated to gather information on current system conditions. If AI/ML could help provide this information, it could lower contracting cost and asset procurement.

2. Physical Security

In the physical security domain, the NIWC Pacific SMEs discussed challenges with the data collection process due to data ownership. The challenges upfront were characterized as “non-technical.” The physical security systems at the installation level belonged to Commander Navy Installation Command (CNIC). As such, stakeholders who want the data must go through CNIC’s approval process, which could take months and potentially up to a year. This back-and-forth period addresses issues such as personally identifiable information (PII). The SME believed the information was not PII, but CNIC disagreed, which put an end to their ability to achieve an Authority to Operate (ATO). This situation was an example of the data owners deciding based on data privacy impacts. Even if the non-technical aspects are addressed, an interconnection agreement must be in place for an external system to connect to CNIC’s system. Also, for research purposes, the data available is primarily unconnected. Access to data was only achievable through “sneaker-net” means, such as optical discs or external hard drives to transfer data to other computers.

On the plus side there was a community of interest in the physical security domain, which meant that standardization and data curation could be achievable. Integration of essential sensors such as cameras and radar tracks that provides situational awareness are integrated into a singular system.

The next step would be to leverage data from these passive visualization sensors in an AI/ML application to automate situation awareness instead of forcing watch standers to stare blankly at screens at all times. For instance, computer vision is applied to cameras to help users identify unusual events. When the expected results were precise, the human understands how the machine determined the effects as in a human versus a bear. When the results were more ambiguous, the human could not understand how the device concluded an unusual event. There requires some level of explanation from the machine to know why there was an alert. This explanation could then improve the trust level between the machine and humans. Table 4 summarizes the information gathered from the Physical Security domain.

Table 4. Physical Security Interview Information

Physical Security		
State of Data	1	Various electronic security systems (ESS) deployed in Navy.
	2	Data control and sharing depends on which commands owns the ESS.
	3	Approval to get access to data can take months or years because of policy.
	4	Video data is important. MIT Lincoln lab working on video analytics for classifying boats/person/animal.
	5	Data access requires sneaker net right now.
	6	Inter-connection agreement required to connect systems together.
	7	Limited physical security data for research right now due to policies such as cybersecurity requirements.
	8	Some surveillance data considered PII by CNIC
	9	Surveillance data is stored for about 30 days.
	10	Entry log data has indefinite storage.
Current Operations	1	Humans in the loop to look at logs of data such as entering, exiting, denied, scanning CAC, unusual traffic patterns.
	2	Navy bases use surveillance data after the fact for forensics not alerting real-time.
	3	DHS uses pattern of life analysis to detect unusual behavior in radar data. Operators say it is kind of weird or I don't care about this. Not an easy problem.
	4	Example surveillance system cannot explain to users how it concluded an unusual event was triggered. Operator unable to understand the alert.
	5	CNIC owns the physical security space.
	6	CNIC has challenges with obtaining authority to operate (ATO) for existing systems.
	7	CNIC has sensor monitoring cells project. Sensor data comes into single workstation and monitored at region level.

3. Battle Readiness

Team Time Zone interviewed subject-matter experts from the Naval Sea Command (NAVSEA) and Naval Surface Warfare Center Dahlgren Division (NSWCDD) in the battle readiness domain. Challenges faced in this domain included needing to move away from lookup tables for weapon selection criteria, determining if an adversary was spoofing, and needing to keep the system operationally available.

The ship self-defense system (SSDS) was created from requirements from the 1980s USS *Stark* (FFG-31) incident where missiles from an Iraqi jet aircraft were fired at the frigate class ship. The system operated by doctrine-based performance, meaning the kinematics were set up to respond based on rules and procedures. The weapon system currently works with rotating radars and is now being integrated with the close-in weapon system (CIWS). An AI/ML system could help integrate the ship's various systems to evaluate which weapons system would be the most efficient for that engagement versus the manual intensive current lookup table method, but the SMEs stated that OPNAV had no requirement from the fleet to incorporate a combat management system. This integration would dramatically impact the ship's longevity in battle since the evolved sea sparrow missiles (ESSM) could be reserved when needed. Weapons, such as lasers, allow for reloading opportunities that keep the ship's weapon choices high by sparingly using the ESSM, which has no at-sea reloading capabilities.

It was also discussed that the largest amount of time spent by sailors right now was determining if adversaries were trying to spoof as a commercial aircraft. The warfighters need to evaluate the following questions: does the aircraft profile match a commercial profile? Are they flying in a commercial air path? An AI/ML system could reduce the burden on the warfighter to make these analyses. It was noted that data from the war diaries was not saved and were only kept for a day or so. Also, data from the modern radars have no test point to collect raw data. There was local track information identified, but no data extraction capabilities currently exist. The SME's key point was the data storage requirement that would be needed if the ships were to start storing these sensors' data might be significant. How much storage would be enough? How much would data compression be required? The possibility to harness and mine data from the weapon system domain seems possible if the data collection points were implemented and proper storage was allocated. Table 5 summarizes the information gathered from the battle readiness domain.

Table 5. Battle Readiness Interview Information

Battle Readiness		
State of Data	1	Ship self-defense system data cannot be accessed externally.
	2	Many types of potentially useful combat data are not retained.
	3	Data is securely removed from ship when it needs to be delivered to DevOps.
	4	Modern radar does not have test points to collect data.
	5	Need the appropriate clearance level to access data for maintenance, combat systems performance and tracking, sensors and response, track data, and track quality.
	6	Data from sailor war diaries are not kept so there is a loss of contextual information.
	7	Data pipes don't exist on surface side, will need to start from scratch.
	8	Need to collect additional data that behave how our adversaries would behave.
	9	Future data collection needs to consider data storage solution.
	10	Data should be region specific.
	11	Need appropriate clearance to see weapon systems data.
	12	Collecting test data for Aegis system required sending someone out to ship to obtain data.
Current Operations	1	Not much time for human in the loop.
	2	Doctrine base performance, set up kinematics to respond.
	3	Weapon system still works with rotating radars.
	4	Ship Self-Defense System (SSDS) requirements derived from 1980s Stark incident.
	5	OPNAV has no requirement for combat management system to integrate.
	6	Lasers are already installed but not integrated in the overall weapons systems.
	7	SSDS currently operates on lookup tables. If decisions can be made from available data from sensors, it could help decide which weapons to use in order to save Evolved SeaSparrow Missiles (ESSM) which has no reload.
	8	Sailors manually try to figure out if an aircraft is really a commercial aircraft. Is it flying a commercial air route? Are there any anomalies with its speed, course, etc.? Lots of time spent determining if an adversary is trying to spoof.
	9	Vast majority of combat systems workload is keeping the system up and track picture are 'clean', sensors configured, bad tracks dropped, and tracks are identified.
	10	NSWC Corona is data manager for SSDS.

C. NEEDS ANALYSIS FOR DATA NEEDS OF DON AI/ML DEVELOPERS (DATA USERS)

Team Time Zone interviewed data researchers and an AI/ML SME to get insightful information from the data users' perspective. Their anecdotes helped frame the challenges they currently face during the data research phase. The AI/ML developers described the data gathering process as requiring "social engineering" because gathering was not a methodical process. The data researcher must spend time social engineering, or spending time with operators and organizations to understand their processes in detail. The process of social engineering allows the AI/ML developers to identify data sources and current operating processes and procedures, and to understand the context of the application in-depth. This process is time consuming and does not always yield a reward (of obtaining data) at the end due to a multitude of reasons. In one instance, data was promised by an organization's point of contact (POC) only to be later told that the POC does not have the authority to grant access to the data. In other cases, communications with organization's POC may go cold and persistent emails and phone calls may go unanswered. The AI/ML researchers expressed much frustration dealing with classified data because of the strict policies that were in place to protect the data. The stakeholders agreed that gathering data from classified projects will cost more and take longer due to the tremendous level of effort involved in getting permissions to use the data.

The stakeholders also discussed the challenges involved in preparing data for use once datasets are obtained. Data preparation takes time and AI/ML developers must ask themselves: Does the data make sense? Are there data outliers? Is the data in the right format? If the data researcher is not already a SME in the field of the application, they must consult SMEs to develop context for the data. The AI/ML developers have had success in working with operations that are directly involved in the data collection process of the application. This helps the AI/ML developers truly understand how the data originates, how it is handled, and how the owners use the data. In some cases, data comes from multiple compartmentalized owners. An anecdote was described to the team where data resided in multiple groups and not one organization understood the overall picture of how

their data would be used. This made it challenging for the AI/ML researcher because the end goal was not clear to all involved.

The team's discussion with a senior AI/ML scientist yielded fruitful context from the data user perspective. He reaffirmed that ML is a data driven process and in order to train the models correctly, the DON must start to collect more data about what the users do. This may seem simple, but the challenge arises due to privacy concerns. The DON has been reluctant to collect user data but to become a data driven enterprise, these issues must have resolution in the immediate future. Examples from the commercial industry were provided such as Google's and Amazon's bottoms-up approach with data. Google collects data from their users, analyzes what data they need for a particular application, then analyzes a different application and identifies where the data intersects. To contrast, the current DON model takes a top-down approach where capabilities and principles are defined. Both approaches introduce data bias. In the case of the top-down approach data bias occurs based on principles. On the other hand, the bottoms-up approach, bias data is based on how the data was collected. Also, it was stated that there is a need for a constant stream of data; he emphasized that AI/ML applications require a constant stream of data to remain current and relevant.

The senior AI/ML scientist discussed some important aspects of AI/ML that currently exist. For instance, the AI/ML field is not a settled science. Much work remains to validate that the distributions and statistics used in ML are correct. This problem is even more pronounced for complex C4ISR models. How do we know that the right math is being used? He stated this is currently a gap in the knowledge base that the AI/ML community must invest research in. He used the example of the game GO where all possible states in the game cannot be stored and changing one rule in the game, such as an extra row, would completely break the trained ML program. The Navy world is not a closed set and thus future DON AI/ML programs must be robust in dealing with change in the real world.

The frustrations, challenges, and insights presented to team Time Zone provided clear issues that needed to be solved in order for the DON to make major progress with AI/ML programs. Tables 6 and 7 summarize the information gathered from the data user's perspective.

Table 6. AI/ML Researchers (NPS) Interview Information

AI/ML Researchers from NPS		
Information Summary	1	Challenge with getting access to data because of permission. Ideally, data permission last forever (universal data permission).
	2	Social engineering is required in order to find the right people to get access to data.
	3	Having knowledge management assistance to get the data is great. Finding data should not be by accident.
	4	Recommend avoiding classified data. Look at proxies.
	5	Gathering data was not methodical at all.
	6	Question to ask during research stage: What data do I need? Can there be substitute data? Where to find data to help you?
	7	Data.gov is a source of data but need to get permissions.
	8	Need to consider ethical and DOD regulations.
	9	Synthetic data may prove what you want to prove.
	10	May need data from many sources. Data warehouse great place to start because it has tools and abstracts.
	11	Collect meta data and lesson learned if it exists.
	12	Takes about 1–2 weeks to speak to a point of contact. Then there is back and forth conversation regarding the time period for data and what build of the data. Need time to analyze these data requirements.
	13	Once data is obtained, there needs to be a sanity check. Does the data make sense? Is it in the right format? Needs exploratory analysis and a follow on conversation.
	14	Transactional data contain lots of garbage in it.
	15	Takes a couple of weeks to understand the data unless you are already a SME.
	16	Need to understand the process and people behind the numbers. Only then can you fully understand the data.
	17	Getting data is at least half of the job.
	18	Data can be used at different levels, tactical, operational, or strategic.
	19	Getting open source data is best.
	20	ML algorithms will eventually need operational data to be trained properly.
	21	Classified projects will cost more because it required more effort. May require data from more than one compartment.
	22	DMDC is a good place for HR data in addition to analytical tools.
	23	The source that has the data may not know how to keep you out of trouble from issues such as PII.
	24	JSON supports standard formats such as XML and CSV.
	25	Need to consider threat from opponents trying to poison our data.
	26	Consider using block chain as way to secure the data.

AI/ML Researchers from NPS		
	27	Try to find someone involved in the data collection process in order to gain insight to help improve analysis.
	28	Sometimes researchers want duplicated data so they don't need to access a real time repository.

Table 7. AI/ML Developer (NIWC) Interview Information

AI/ML Developer from NIWC		
Information Summary	1	Engineering practices for AI/ML, not a settled science in AI/ML particular in assessing in mission critical and safety using AI/ML techniques.
	2	Software Engineering traditionally, not necessarily the right path to develop capabilities.
	3	Air agencies in Europe showing a system engineering W now instead of V to use data driven solutions. NASA AMES is doing the same thing.
	4	ML is a data driven approach. Collecting requirements is not necessarily the right path.
	5	Centralized repository data for AI is like software standard, many to choose from. Many different folks are trying to develop centralized data repository (e.g. NAVSEA Corona).
	6	Need to collect more data about what the users do.
	7	Google and Amazon collect information on their users all the time to improve their systems.
	8	DON scared to collect data on users because of privacy concerns.
	9	Need to collect data in order to call ourselves a data driven enterprise.
	10	Need to have constant stream of data, not one time deal in order to have current data.
	11	Google does everything bottom up. Collect data and look for things in common.
	12	Going top down will bias data based on principles.
	13	Going bottom up will bias data based on how you collected the data. Was the operation the correct situation?
	14	ML is not a settled science. Worried about validity and statistics used in ML.
	15	Real world will contain models from many events for C4ISR. Model at each step will use different sets of data and distribution. What is the math bridging all of those models and distributions together? This is a GAP in knowledge currently
	16	Effects of uncertainty propagating through the chain of our model is not looked at right now in the Navy.

AI/ML Developer from NIWC		
	17	Even simple games have many different scenarios – so we cannot store information on every state. Naval operations even more complicated.
	18	Techniques that use self-play to explore decisions space are interesting but the problem is they will break instantaneously in the real world. For example, if you change the rules of GO right before start (third player, extra rows), it will break.
	19	Navy AI/ML must be robust enough to deal with change in the real world. Navy world is not a closed world/closed set.
	20	Lots of research on explainable AI -- Human intelligence cannot understand why they made that decision. Do not expect we can do it with AI.
	21	CDRs for the task force have been educated the same way. They train and can predict each other's decision. Likewise, AI agents, could be made to learn from each other.
	22	We may not know the right algorithm even for a simple supervise learning scenario. Need to try several ML algorithms such as neural nets, decision trees in order to see what worked best.
	23	Some AI techniques are not data driven. Model are hand crafted based on knowledge of the environment and use of doctrine in the area.
	24	NIWC Philadelphia—Natural Language – Navy 311, using models developed by learning what types of actions based on trouble reports. Retrain ML system once a month. Have luxury of time to retrain system – very different then real time decision making.

D. NEEDS ANALYSIS ASSESSMENT AND RESULTS

The AI and ML systems are data-intensive, requiring large amounts of data to train ML algorithms. The accuracy of AI/ML models largely depends on the quality and quantity of the data. As a reference point, it took approximately 40 days, including 29 million games, to train DeepMind's AlphaGo Zero system to learn to play the game of Go (Feldman, Dant, and Massey 2019). Imagine an AI/ML algorithm for a weapons system that needs to factor in concepts such as war context (war games, cold war, peacetime), friend or foe, ethics, and legality (Feldman, Dant, and Massey 2019). Such an AI/ML system will require vast amounts of training data based on the enormous numbers of permutations of weapon systems versus threat situations.

Data gathered at the lowest levels will be used to build higher-level concepts and complex structures to support AI/ML systems. Applications of these data for AI/ML methods include maintenance, physical security, and battle readiness, to name a few. All these application domains have the same barrier to entry in the DON for AI/ML programs: accessing sufficient, accurate, and representative data sets. Team Time Zone’s needs analysis and stakeholder interviews determined that the DON faces a huge challenge in making sure datasets are available to support AI/ML development.

1. Insights from the Data Consumers

The data consumers included ONR, NPS, NAVAIR, NAVSEA, NAVWAR, NAVSUP, NAVFAC, BUMED, MARCORPSYSCOM, warfighters, and industry. Data consumers need to fast-track their data exploration activities. In one example, engineers took more than a year to acquire data they had paid for from another program office. The team found that DON AI/ML data consumers use the following methods for gathering and sourcing data: social networking, problem space and needs analysis, requests for data, data collection, and data validation. The “data request” activity encounters the most variability and causes delays in obtaining the desired data sets. Data scientists struggle with this part of the process because of failed promises to provide the data. Further, many data engineers and scientists are introverts, so reaching out to others via social engineering is not a core competence.

After obtaining the data, AI/ML developers must groom the data and prepare it for use as well as determine dataset reliability. Interviews or conversations between the AI/ML developers and data owners is a critical part of the process—to understand the context and concept of operations of the application domain. The interview process should also be used to understand the reliability and representativeness of the data. Insightful stories will enable the data scientists to understand the data origins and possible biases.

2. Insights from the Data Providers

The DON CIO and DISA must establish policy for data governance guidelines. Each domain can define its data structures and data format requirements from these guidelines. The community of interest within each domain can start to standardize their

data. Descriptive metadata must be implemented within each environment. This metadata should be similar to a library catalog system (Pomerantz 2015), allowing people to find books based on descriptive metadata such as author, title, and date. An example metadata set should include domain, system command owner, date range, data origins, data description, data classification, number of records in the data set, and number of times data has been requested.

The requirements for access to the provider's dataset need to be established. Who can access the data? What are the access requirements? How much can data be shared? How long can the data be shared? Does follow on data require a separate request? How will PII data be communicated? These types of questions must be answered by the data providers to govern their data set properly. Requirements for data providers should include the establishment of governance guidelines, metadata requirements, operational requirements, data readiness, data bias reduction, data curation, data taxonomy, data governance, and data security.

3. DON AI/ML Data Management Requirements

Team Time Zone assessed the information gathered in the stakeholder interviews to study the data needs of DON AI/ML developers. The team evaluated the DON data needs in the three naval mission domains and the challenges involved in gathering data and translating data into useful forms for data analysis. The team observed that the information gathered in the stakeholder interviews fit into the data strategy categories identified in the DOD Data Strategy document. These categories are: data readiness, data bias, data curation, data taxonomy, data governance, and data security.

The team compared the information gathered for each of the three naval mission domains. The team concluded that the data needs for each domain range from slight differences to significant differences. All three mission domains produce classified data to some extent. The system maintenance domain largely produces textual data and associated quantitative data (such as failure rates); the physical security domain largely produces video surveillance data; and the battle readiness domain largely produces sensor tracking

data and system capability data. In the Weapon Systems domain, most of the data was classified and only certain people were privy to the information.

Information assurance (IA) was an example of a critical requirement in all three naval mission domains. Future systems that need to connect to any of these information databases would need to have an ATO along with obtaining an inter-connection agreement to clear the IA requirements.

Another data need across DON mission domains was the importance of understanding mission and data context. All AI/ML researchers need to have a deep understanding of how data originates, how data is used, how decisions are made, and what the concepts of operation are. Also, AI/ML researchers need a detailed level of fidelity in their contextual understanding to properly groom and prepare data and to train ML algorithms in a manner that is representative of the intended operations.

The following list of data characteristics and data management processes constitutes a high-level set of data needs for DON AI/ML data management:

- Data must be made accessible to outside organizations.
- Data must have standard formats that are compatible with the domain application.
- Data must have identified owners.
- Data must be accompanied by descriptive metadata.
- Data must have governance for standardization.
- Data must be in its lowest common denominator.
- Data must have security for protection and proper sharing,
- Data must have obfuscation to protect PII.
- Data must have context to properly understand its origins.

4. Needs Analysis Conclusion and Data Considerations

The stakeholder needs and requirements represent the views of “users, acquirers, customers, and other stakeholders as they relate to the problem (or opportunity), as a set of requirements for a solution that can provide services needed by the stakeholders in a defined environment” (Guide to the Systems Engineering Body of Knowledge 2020). The stakeholder interviews provided the team the necessary information to develop solution-based requirements and to identify the challenges of the data collection process for data accessibility, constraints, availability, validation, and governance. Figure 9 illustrates the DON’s data considerations for AI/ML.

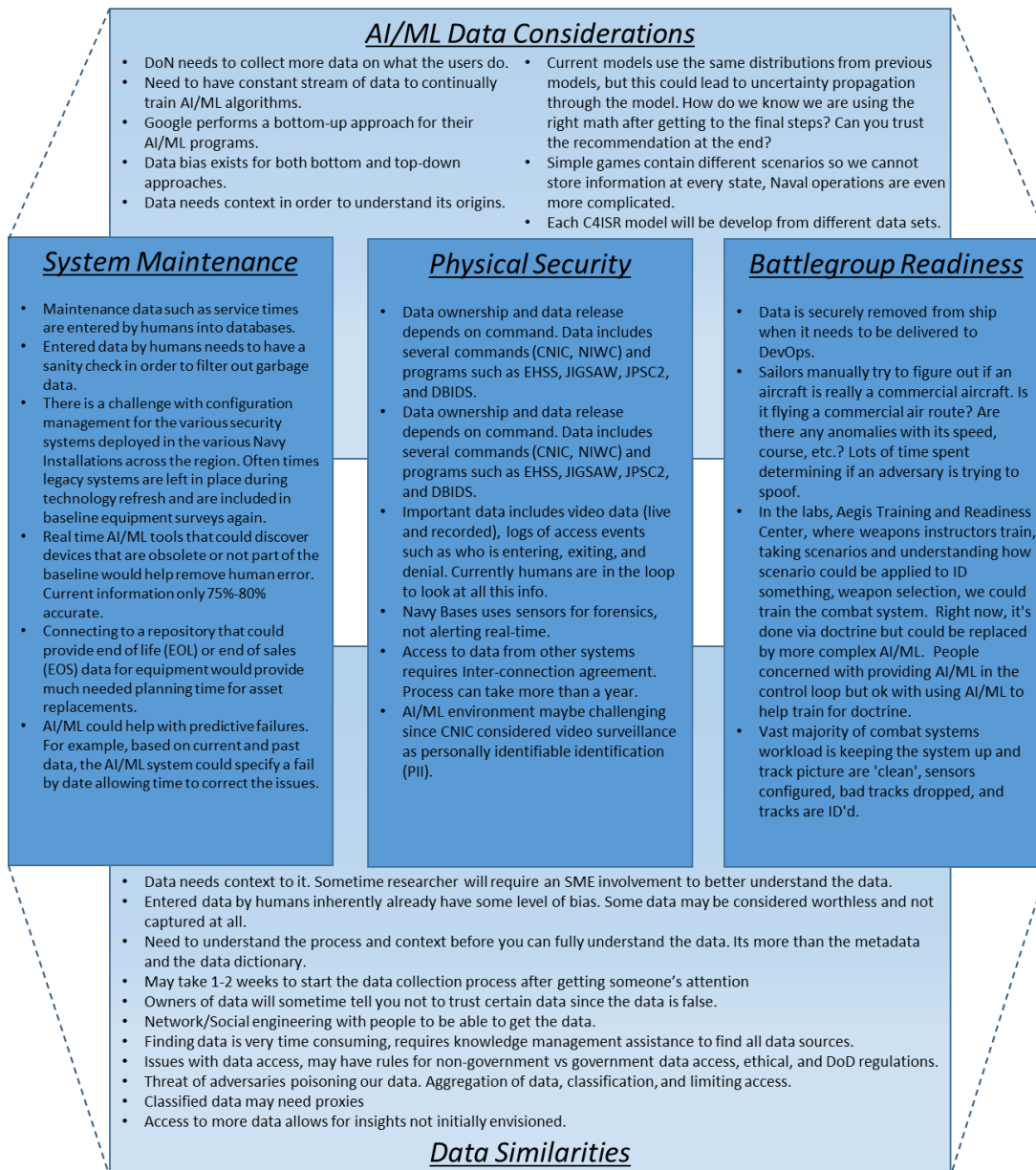


Figure 9. Stakeholder AI/ML Data Considerations

IV. SOLUTION STRATEGY: CENTRAL ARTIFICIAL INTELLIGENCE LIBRARY (CAIL) SYSTEM

Historically, the DON has collected data in many forms for many purposes during mission operations; mostly notably to document the operations and provide information to support the evaluation and maintenance of operational systems and to support developers that are designing system and process upgrades and future capabilities. With recent advances in AI and ML methods, a new and critically important use for operational data has arisen. Data in many forms is now needed to train ML systems. This prompted the capstone team to study data availability within the DON and develop a conceptual solution to effectively manage data and provide it to AI/ML developers.

Team Time Zone team employed a top-down system engineering methodology to conceptually design a solution to address the problem space explored in the needs analysis. The team developed a conceptual design of the Central AI Library (CAIL) system based on the requirements developed from the team's needs analysis. The team synthesized and defined the CAIL system concept by developing MBSE artifacts which fostered the team's ability to view and model the system from different perspectives including operationally, functionally, and holistically. The team developed CAIL system modeling views including DoDAF OV-2, OV-5b/6c, OV-2, and SV-1. The team used high-level CAIL system modeling and simulations to validate needs analysis requirements and provide insights into potential DON resource savings opportunities gained by implementing CAIL.

A. CONCEPT OF OPERATION

The team envisioned the CAIL system as a set of information systems and organizational processes for the DON to identify data sources, support data providers with an interface that allows them to provide metadata information, support data consumers (AI/ML developers) with an interface that lets them search for data and provide a process that enables data grooming activities in a secure environment.

The CAIL addresses the current problems that data is often too hard to secure; is sometimes not collected or stored; is often incomplete; and sometimes is not validated.

DON data is sometimes stored in separate repository databases, on board ships, and at times is not captured. Sometimes, large volumes of stored data could contain valuable metadata with the potential to contain information that could be analyzed to understand the history about the specific areas where data was collected. The DON faces a data “stovepipe” issue – with data captured and stored within different organizations and not readily available to developers. This denies creating major advances in naval capabilities. The CAIL system is envisioned as a solution that integrates the data stored in various DON databases and offers a single source integrated data environment for AI/ML developer access.

The CAIL concept of operations (CONOPS) is illustrated in Figure 10. The CAIL system includes an integrated data environment that provides data grooming capabilities including data optimization, normalization, and integration and provides a user interface to allow DON commands and AI/ML systems secure access. The CAIL system interacts with DON data sources, such as those that produce data in different naval mission domains, including operational data from ships, submarines, and weapon systems, as examples.

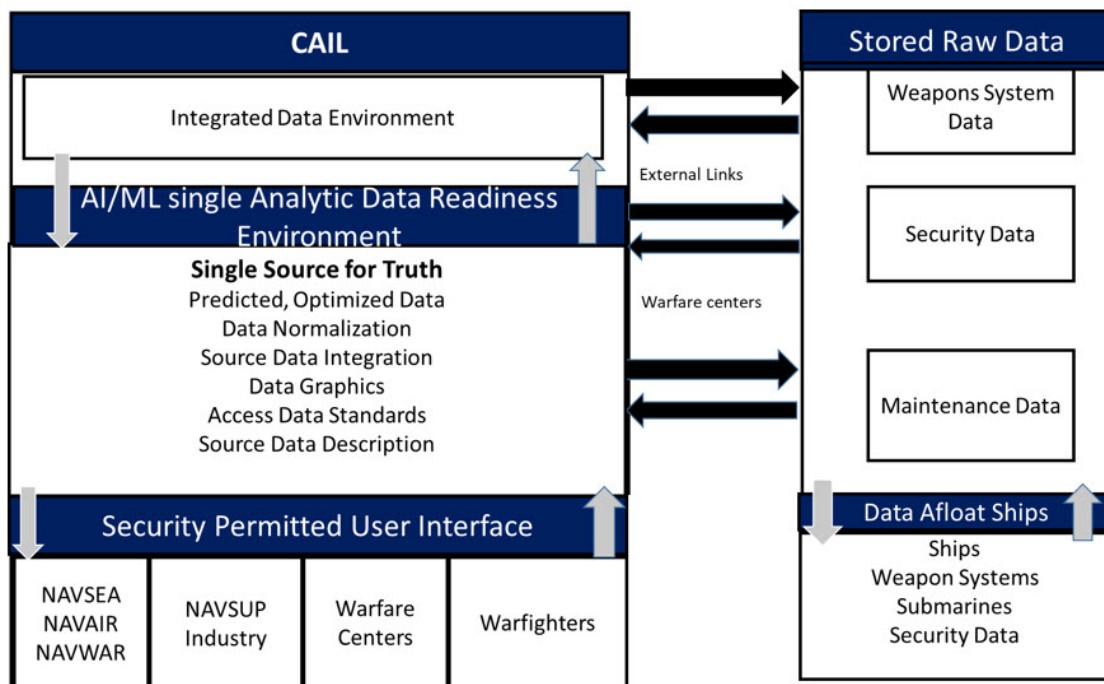


Figure 10. CAIL Concept of Operations

The CAIL CONOPS begins with the continuous and on-going identification of trusted data sources in the Navy. The CAIL system will keep track of the existence of data stored in independent databases throughout the DON and will support the evaluation of data to ensure authoritative sources and the current status of data. The CAIL system operations will include the following:

- a. Identify and keep track of data for naval missions of interest.
- b. Provide the ability to normalize data to enhance decision-making and mission readiness.
- c. Migrate temporarily data to CAIL architecture to use AI/ML to clean the data.
- d. Automate repetitive tasks using AI/ML.
- e. Provide secure user access to enterprise Navy data.
- f. Provide metadata and descriptive records.
- g. Provide a search engine optimization, which helps users discover and locate data of interest.
- h. Provide access to users with varying levels of permissions.
- i. Provide a standard way to access the approved data.
- j. Provide a user interface to collect data on who the users are and the intended use of the requested data.
- k. Provide users with closed-loop, access to normalized data with electronic documentation and audit trail (including origin of the data, history, and the current state of the data and audit the data when required).
- l. Increase the quality content of operational data available to various users by linking data from various databases. “The more records about entities connected together, the richer the knowledge represented by the data” (Pomerantz 2015, 173–174).
- m. Provide the contractual data necessary to support platform, system, and equipment through the life cycle.
- n. Inform the users of data availability so they know what data can be accessed or how long it will take to access data.

- o. Provide consistent, standardized, and formatted data when appropriate and provide data in a format that is suitable for data users.

B. SYSTEM REQUIREMENTS

Team Time Zone developed a set of system requirements for the CAIL system based on the results of the needs analysis and the concepts of operation.

1. Methodology

Team Time Zone started with defining the “need” and worked on the stakeholder analysis to identify the requirements for the CAIL system. The team used the concept of operations to conceptualize a design for the capabilities of CAIL. A systematic breakdown of the capabilities, tracing and analyzing each mission need and requirement was adequately mapped to the corresponding capability. Using a model-based systems engineering (MBSE) tool like Innoslate made this process much easier as concordance was maintained. Doctor Warren Vaneman states “Concordance is the ability to represent a single entity data such that data in one view, or level of abstraction, matches the data in another view, or level of abstraction, when talking about the exact same thing” (2021, 6).

It is this formal system engineering and systems modeling that recommends

- standard practice for defining, designing, and analyzing engineered models that represent the system
- provides a shared understanding of system in a virtual environment
- spans the entire life cycle from concept, development, and operations support. (INCOSE 2021, 24)

The team defined a Concept Data Model (CDM) upfront to provide a common vocabulary for the development of the CAIL MBSE model. Figure 11 captures the team’s CDM. The CDM provided the rules for how artifacts and documents were the sources of requirements for the CAIL system. The CAIL system statements or requirements trace to the the actions of a mission capability. Mission capabilities can be further decomposed into actions of operational capability. The CAIL assets can be further decomposed into asset of subsystem elements. Asset subsystems perform operational activities.

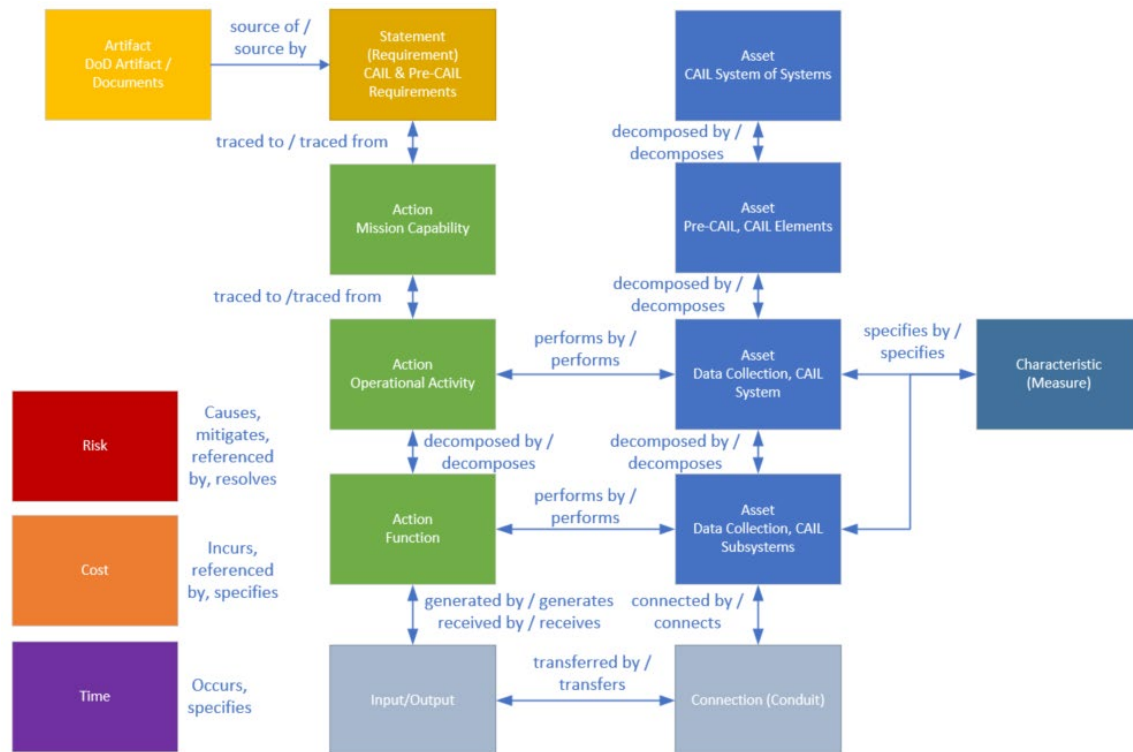


Figure 11. CAIL System Conceptual Data Model

2. Requirements Analysis

The CAIL system requirements were broken down into six major categories: data readiness, data bias, data curation, data taxonomy, data governance, and data security.

- Data Readiness – The system shall ensure data integrity to include the necessary identification of data standardization, validation, and availability of data sources. Data is visible, accessible, understandable, linked, trustworthy, and interoperable.
- Data Bias – The system shall break down AI data from authoritative sources to the smallest elements to minimize data bias.
- Data Curation – The system shall prepare and share AI data and reference authoritative data sources and/or store AI data for sharing and identifies, describes, fit into the taxonomy, and catalogs all the meta-data for the data.
- Data Taxonomy – The system shall maintain structured data and provide standard formats and data types for other systems/programs to use.

- Data Governance – The system shall have a community and/or authoritative governing body to manage and provide rules to govern access and authorization to the data.
- Data Security – The system shall have a community and/or authoritative governing body to manage and provide rules to govern access and authorization to the data.

The team used the requirements spider diagram (shown in Figure 12) as a guide to decompose and trace the high-level requirements and to validate that each requirement was traced to a capability.

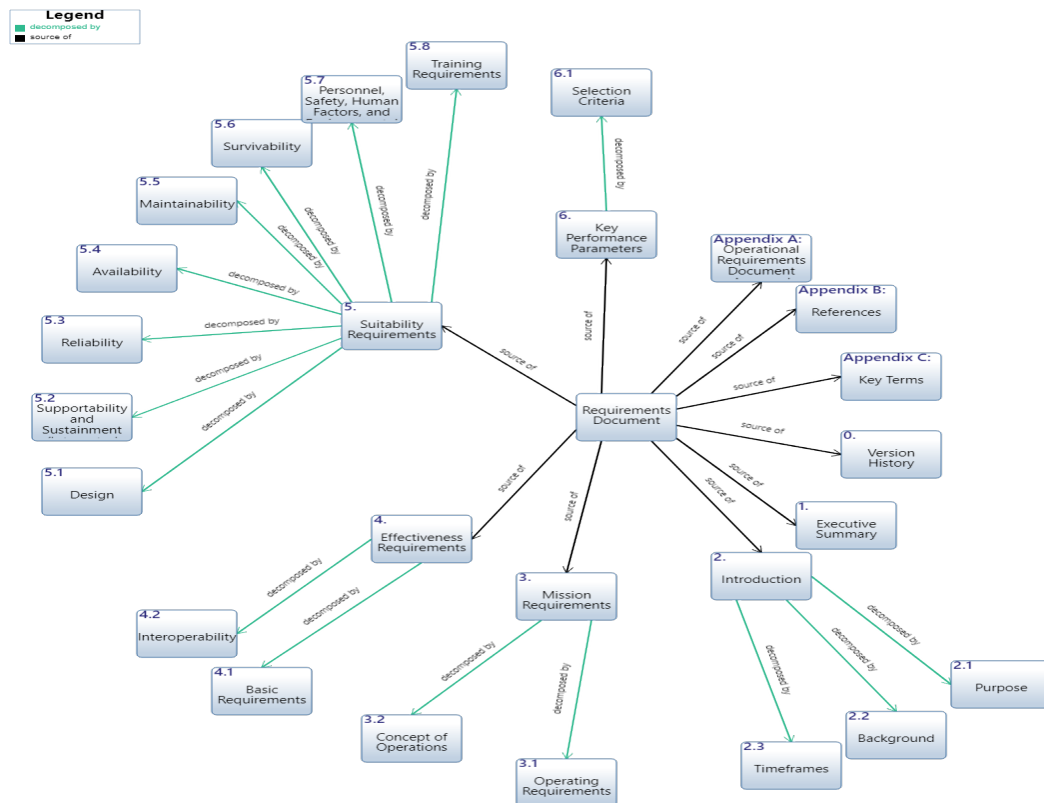


Figure 12. Requirements Spider Diagram

In looking at the DOD Data Strategy released in Oct 2020 the CAIL requirements are in line with the 8 Guiding Principles:

1. Data is a Strategic Asset – DOD data is a high-interest commodity and must be leveraged in a way that brings both immediate and lasting military advantage.
2. Collective Data Stewardship – DOD must assign data stewards, data custodians, and a set of functional data managers to achieve accountability throughout the entire data life cycle.
3. Data Ethics – DOD must put ethics at the forefront of all thought and actions related to how data is collected, used, and stored.
4. Data Collection – DOD must enable the electronic collection of data at the point of creation and maintain the pedigree of that data at all times.
5. Enterprise-Wide Data Access and Availability – DOD data must be made available for all authorized individuals and non-person entities through appropriate mechanisms.
6. Data for Artificial Intelligence Training – Data sets for AI training and algorithmic models will increasingly become the DOD’s most valuable digital assets. We must create a framework for managing them across the data life cycle that provides protected visibility and responsible brokerage.
7. Data Fit for Purpose – DOD must carefully consider any ethical concerns in data collection, sharing, use, rapid data integration, as well as minimization of any sources of unintended bias.
8. Design for Compliance – DOD must implement IT solutions that provide an opportunity to automate the information management life cycle, properly secure data fully, and maintain end-to-end records management. (2020, 1)

The team identified a requirement for a data-centric enterprise “Data Cloud” that allows future programs to access and integrate data to train ML systems rapidly. Some programs may not have the funds to incorporate ML initially but identifying ML data and developing standards across the Navy enterprise will optimize training between the human and the machine, support human trust in AI systems, and provide substantial cost savings in the DON through enhancements of resource management for both personnel and engineered systems. That “Data Cloud” is identified as the CAIL system.

However, after several SME interviews and speaking with various experts, it was apparent that even these Pre-CAIL activities were necessary. SMEs explained it was complicated to determine what data and/or systems are being used, who the authoritative owners are, what data is available, how often it is updated, if that system interface with other external systems, how you gain data access, licensing agreements, whether the data is classified, and if there are any data distribution constraints. The CAIL system was

reworked to incorporate this exploratory effort (Pre-CAIL) which included finding data/ social networking solutions, identify sources, understanding context, analyzing the problem space, and requesting and collecting data.

C. CONCEPTUAL SYSTEM ARCHITECTURE AND DESIGN

Alan Faisandier, Garry Roedler, and Rick Adcock from the SEBoK describe system architecture:

The purpose of system architecture activities is to define a comprehensive solution based on principles, concepts, and properties logically related to and consistent with each other. The solution architecture has features, properties, and characteristics that satisfy, as far as possible, the problem or opportunity expressed by a set of system requirements (traceable to mission/ business and stakeholder requirements) and life cycle concepts (e.g., operational support) and which are implementable through technologies. (Faisandier, Roedler, and Adcock 2020)

Team Time Zone developed a conceptual architecture and design for the CAIL system. The team set out to envision a system and process to address the needs and challenges discovered during the stakeholder and needs analysis. The team’s objective for the CAIL architecting process was to “communicate across the gap from the user/sponsor/ client to the engineer/developer” and to ensure that the architecting process was “complete when a system is well-enough defined to engage developers” (Maier and Rechtin 2009, xvii).

The team used the CAIL system requirements to envision an operational view and context diagram. The team decomposed the requirements to develop a hierarchy of capabilities, operational activities, asset capabilities, and event-trace descriptions. This section contains the team’s conceptual system architecture and design artifacts

1. OV-1 Diagram

The team developed a high-level operational view of the conceptual CAIL system (shown in Figure 13). The OV-1 depicts how data is transferred among the naval fleet through a central network operations center (NOC) and/or ashore command center to the

CAIL system. The ribbon located at the bottom of the chart has icons representing the data domain areas that will be improved by having this CAIL data cloud or new emerging technologies like a “data fabric.” A “data fabric is an interconnected, network-based design that’s functionally similar to the human brain; data fabric eliminates traditional integration efforts and dramatically reduces build times” (DeMers 2021).

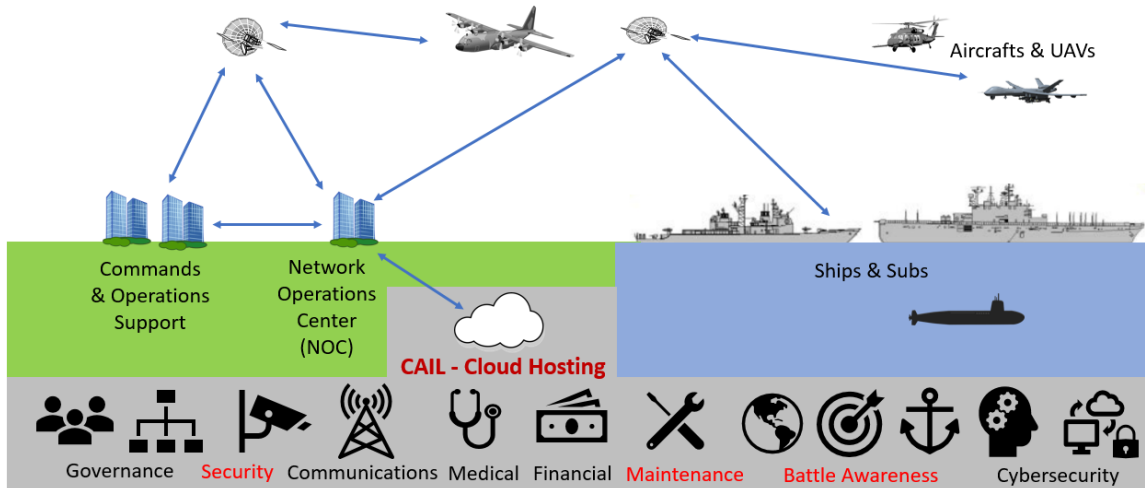


Figure 13. CAIL OV-1

2. Context Diagram and Subsystems

The team developed a CAIL context diagram (shown in Figure 14) that includes Pre-Cail processes and activities. The Pre-Cail includes processes to research, socialize, and to identify data sources, understand the context and use of the data, analyze the data problem space, request the data and receive approvals for its use, retrieve and collect the data, and then ensure data is used for its intended purpose. The Data-Centric enterprise “Data Cloud” or “Data Fabric” of the CAIL system will allow quicker access for AI/ML developers to integrate data and train ML systems.

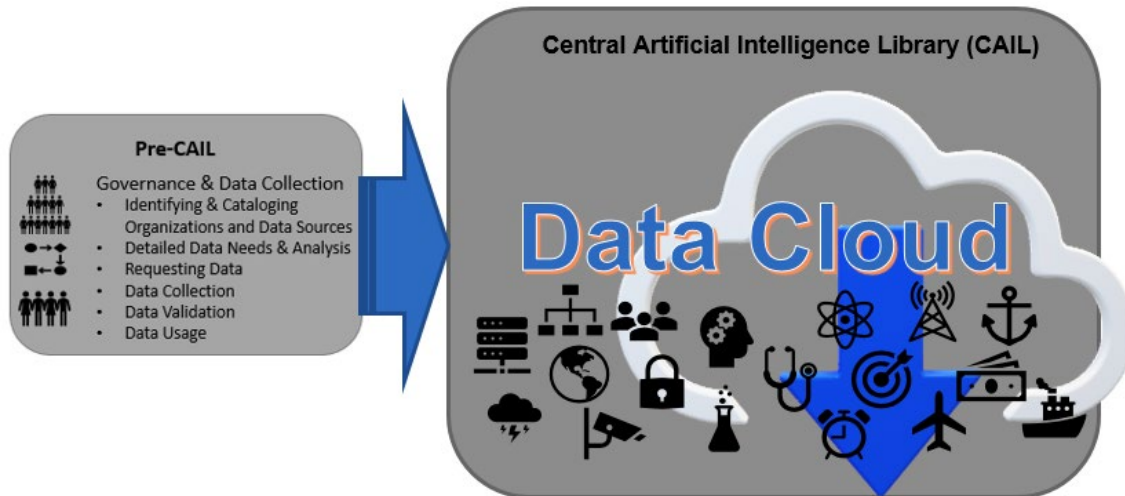


Figure 14. High-Level CAIL and Pre-CAIL System

The CAIL system interfaces with external end-users, system applications and/or services (developed by the Program Offices), organizations like DON CIO, DISA, NRL, and/or NPS, which support the governance and policy development from which data standards, authorizations, and governance that is required to support the CAIL eco-system derives. The external interfaces connect to federated data, databases, documents, and content repositories from authoritative data producers/providers. Figure 15 illustrates the high-level capabilities and external interfaces of the CAIL system. The figure also illustrates the three naval mission domain use cases (system maintenance, physical security, and battle readiness) that the team used for CAIL domain analysis.

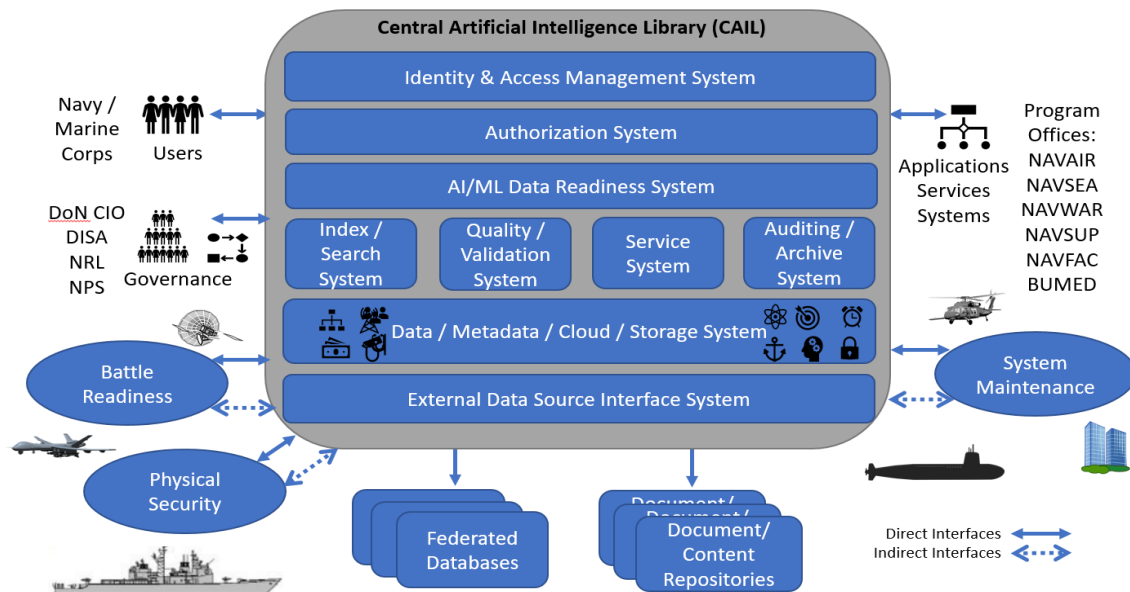


Figure 15. CAIL System

Team Time Zone identified the following CAIL subsystems (there are shown in Figure 15):

- Identity and Access Management System – this subsystem identifies and manages users/services access to the system. It interfaces with the Authorization System to manage access to the authoritative data based on source criteria, policies, and governance for data utilization and safeguarding, and to manage the relationships between data resources and users/services requiring access.
- Authorization System – this subsystem authorizes user access to the CAIL.
- AI/ML Data Readiness System – this subsystem provides data readiness services to help manage, validate, and support the overall CAIL System
- Index/Search System – this subsystem provides services to search, index, and list data and elements.
- Quality/Validation System – this subsystem evaluates CAIL quality checks validates data and metadata.
- Service System – this subsystem provides core services to maintain and administer all CAIL services.

- Auditing/Archive System – this subsystem audits and manages data changes and data access, and archives data when data is no longer being used.
- Data/Metadata/Cloud/Storage System – this subsystem provides data cloud storage and an IT infrastructure for data and metadata as well as data and system associating, linking, and “blueprinting.”
- External Data Source Interface System – this subsystem provides external interfaces to all authoritative data sources

3. Capability Views

The team developed architectural views based on the Department of Defense Architectural Framework (DoDAF) to capture capability views of the CAIL system and Pre-Cail activities. The team developed a Capability Taxonomy (CV-2) for the CAIL system (shown in Figure 16) and for the Pre-Cail activities (shown in Figure 17).

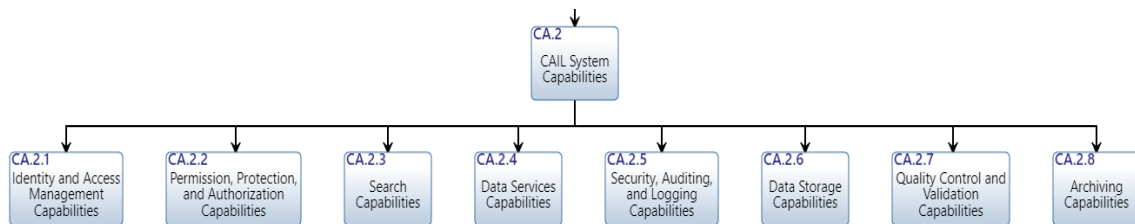


Figure 16. CAIL CV-2

Figure 16 shows decomposes the CAIL system into a number of capabilities including: identifying and accessing management capabilities, managing permission, protection and authorization, providing search functions, providing data services, providing security, auditing, and logging functions, enabling data storage, providing quality control and valiation, and providing data archiving.

The following provides more detail for the CAIL system capabilities:

- Identifying user/system/service is critical to then determine who is requesting access to data. Various identifying capabilities using username and password, public key infrastructure (PKI) certificates, biometric

information, or other multi-factor authentication are examples for authenticating information technology systems to identify who the individual and system claim to be. This is usually implemented with an Identity and Access Management (IdAM) system.

- Once the user/system/service has been authenticated, the process can verify that the user, system, or service is authorized to access the data. This authorization capability is that access control is typically implemented with either discretionary access control (DAC), mandatory access control (MAC), rule-based access control, role-based access control (RBAC), or attribute-based access control (ABAC).
- A search capability to provide the listing of data, data elements and to filter the data retrieved.
- Data services can administer all CAIL system services from maintaining the data, managing the infrastructure, providing external data interfaces, system and data readiness status, and other administrative services necessary to operate the CAIL system.
- Security, auditing, and logging capabilities to ensure cybersecurity protection of the data. Data breaches are a critical risk, so the system must incorporate technologies in a layered defense architecture that considers data encryption, firewalls, antivirus, anti-malware, file/database system monitoring, web session monitoring, and other cybersecurity tools.
- Data storage and infrastructure capabilities to dynamically monitor and increase storage when required, data requests that are frequently accessed are optimized in storage areas to maximize efficiencies in providing the data in the shortest time possible.
- Quality control and validation capabilities to ensure CAIL is providing good data that satisfies that requirements of its intended use for users,

downstream applications, and processes. Shen (2019) explains the steps needed to ensure data is sustainable as follows:

- -Accuracy: for whatever data described, it needs to be accurate.
- -Relevancy: the data should meet the requirements for the intended use.
- -Completeness: the data should not have missing values or miss data records.
- -Timeliness: the data should be up to date.
- -Consistency: the data should have the data format as expected and cross reference-able with the same results. (Shen 2019)

Archiving capabilities to move data to offline storage and optimize the CAIL system to be as responsive to the data requests that are most relevant to the users it is supporting.

The Pre-CAIL capabilities are shown in Figure 17.

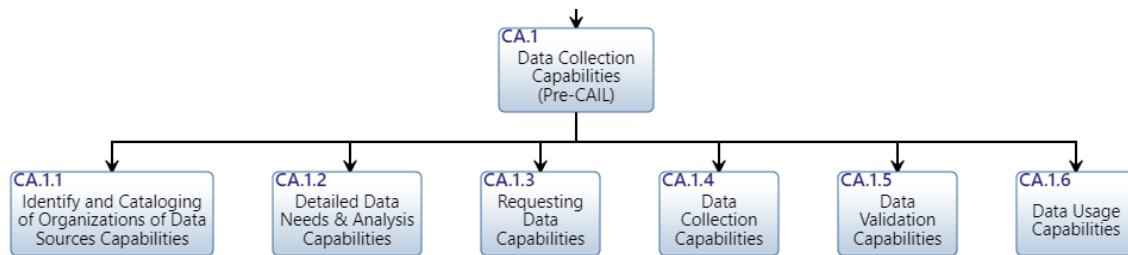


Figure 17. Pre-CAIL CV-2

The Pre-CAIL capabilities include:

- Identifying and cataloging of data sources and organizations managing and operating those authoritative data sources
- Detailing data needs and analysis to understand the data, metadata description details of the data, how it was created, managed, used, and updated
- Requesting access to the data, whom to contact, receiving approval for use

- Collecting the data and understanding the process and procedures to get the data and any special security measures to ensure the protection of that data
- Validating the data once to ensure the data is correct and meaningful
- Ensuring the data received is appropriately handled, meeting any security and/or agreements brokered with the data source on the data usage

4. Operational Activities

Team Time Zone created an operational activity decomposition tree (OV-5a) to bridge operational activities in a hierarchical structure and to correspond these activities to the capabilities. Figure 18 conveys the overall hierarchical structure of the OV-5a and a larger and readable version of the figure can be found in Appendix B. Figure 19 contains a mapping of the CAIL capabilities to the operational activities. A larger version of Figure 19 can also be found in Appendix B.

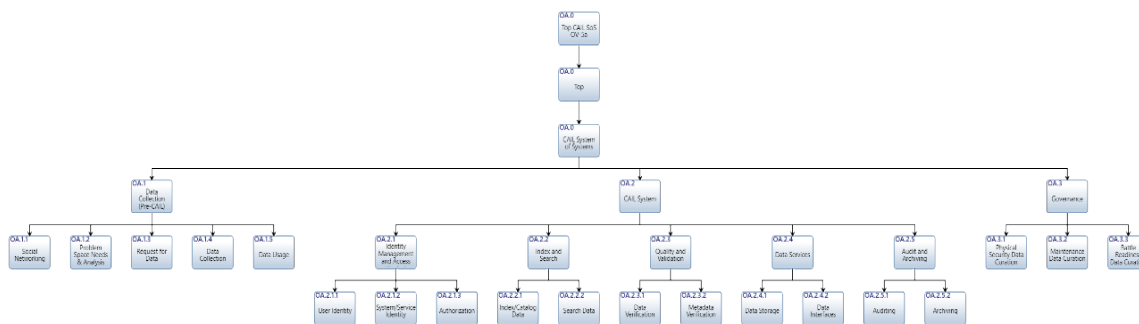


Figure 18. OV-5a

	OA.0 CAIL System of Systems	OA.0 Top	OA.0 Top CAIL SoS OV-5a	OA.1 Data Collection (Pre-CAIL)	OA.1.1 Social Networking	OA.1.2 Problem Space Needs & A...	OA.1.3 Request for Data	OA.1.4 Data Collection	OA.1.5 Data Usage	OA.2 CAIL System	OA.2.1 Identity Management and ...	OA.2.1.1 User Identity	OA.2.1.2 System/Service Identity	OA.2.2 Authorization	OA.2.2.1 Index and Search	OA.2.2.2 Index/Catalog Data	OA.2.3 Search Data	OA.2.3.1 Quality and Validation	OA.2.3.2 Metadata Verification	OA.2.4 Data Services	OA.2.4.1 Data F	OA.2.4
CA.0 CV-2 CAIL SoS Capabilities	X	X	X																			
CA.1 Data Collection Capabilities (Pre-CAIL)				X																		
CA.1.1 Identify and Cataloging of Organiz...				X	X	X																
CA.1.2 Detailed Data Needs & Analysis Ca...				X	X																	
CA.1.3 Requesting Data Capabilities						X																
CA.1.4 Data Collection Capabilities						X																
CA.1.5 Data Validation Capabilities						X	X															
CA.1.6 Data Usage Capabilities							X															
CA.2 CAIL System Capabilities								X														
CA.2.1 Identity and Access Management C...									X	X	X	X										
CA.2.2 Permission, Protection, and Author...										X	X	X										
CA.2.3 Search Capabilities													X	X	X							
CA.2.4 Data Services Capabilities																		X				
CA.2.5 Security, Auditing, and Logging Ca...																						X

Figure 19. Capabilities to Operational Actions Mapping

5. Assets

The Operational Resource Flow (OV-2) and System Interface Description (SV-1) were created to identify the physical systems, system items, and interconnections for CAIL, as shown in Figure 20, CAIL System Figure 21, and Pre-CAIL System Figure 22.

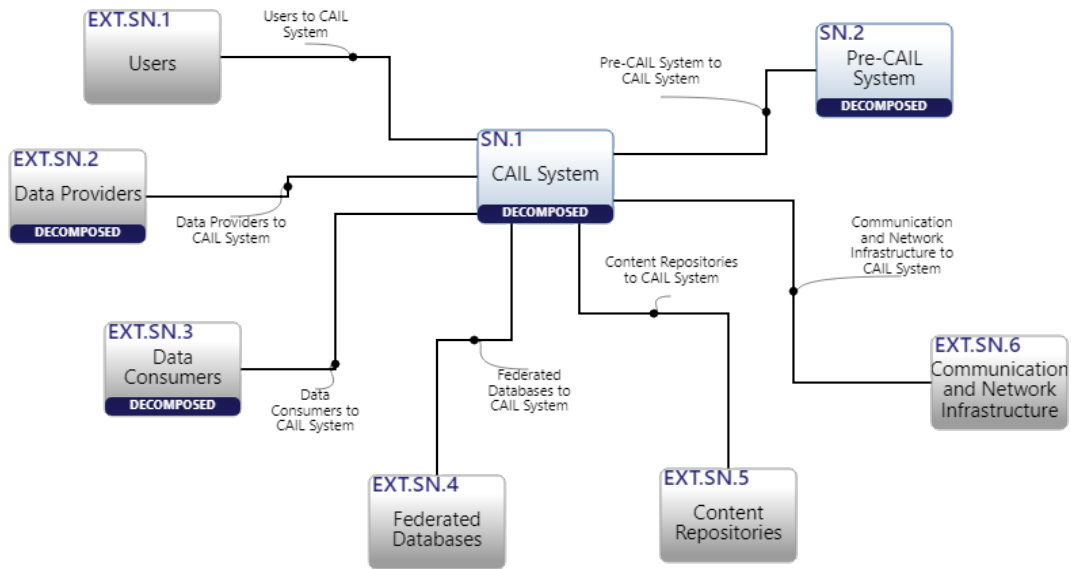


Figure 20. CAIL – SV-1

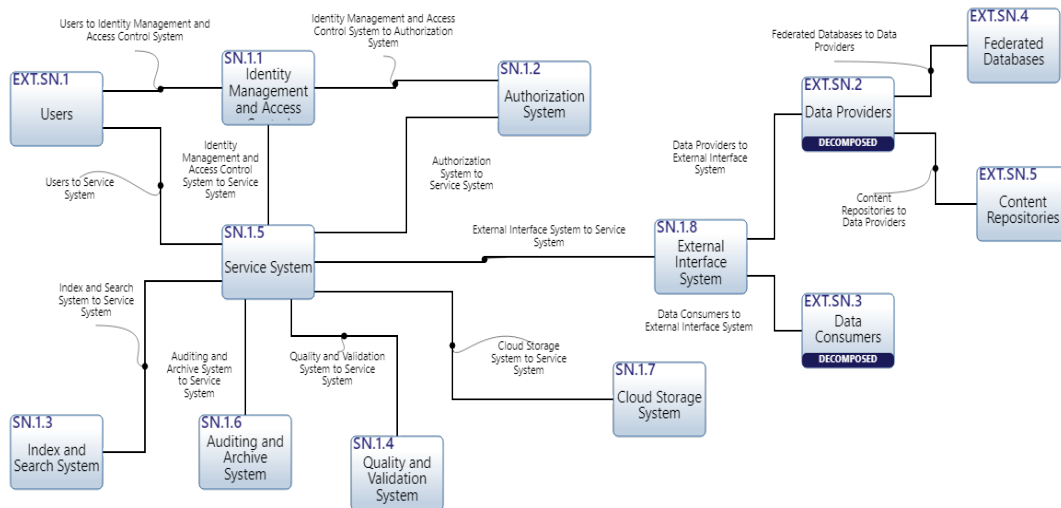


Figure 21. CAIL System – SV-1

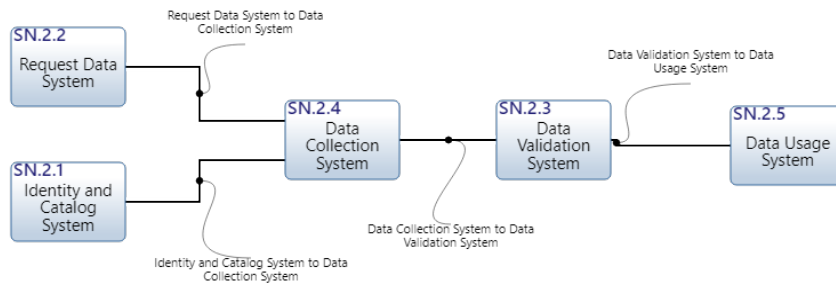


Figure 22. Pre-CAIL System – SV-1

Additionally, a modified OV-1 with the assets overlaid was created, as shown in Figure 23. Other DoDAF views for Capability to Operational Activities Mapping (CV-6) and Operational Activity to Systems Traceability Matrix (SV-5b) were used to associate and link Capabilities to Operational Activities and Operational Activities to the Systems (Assets) to build a complete model representation of CAIL. The team used this system engineering approach to create the CAIL architecture that defines “a set of abstractions and models that simplify and communicate complex structures, processes, rules, and constraints to improve understanding, implementation, forecasting, and resourcing” (Dam 2014, 5).

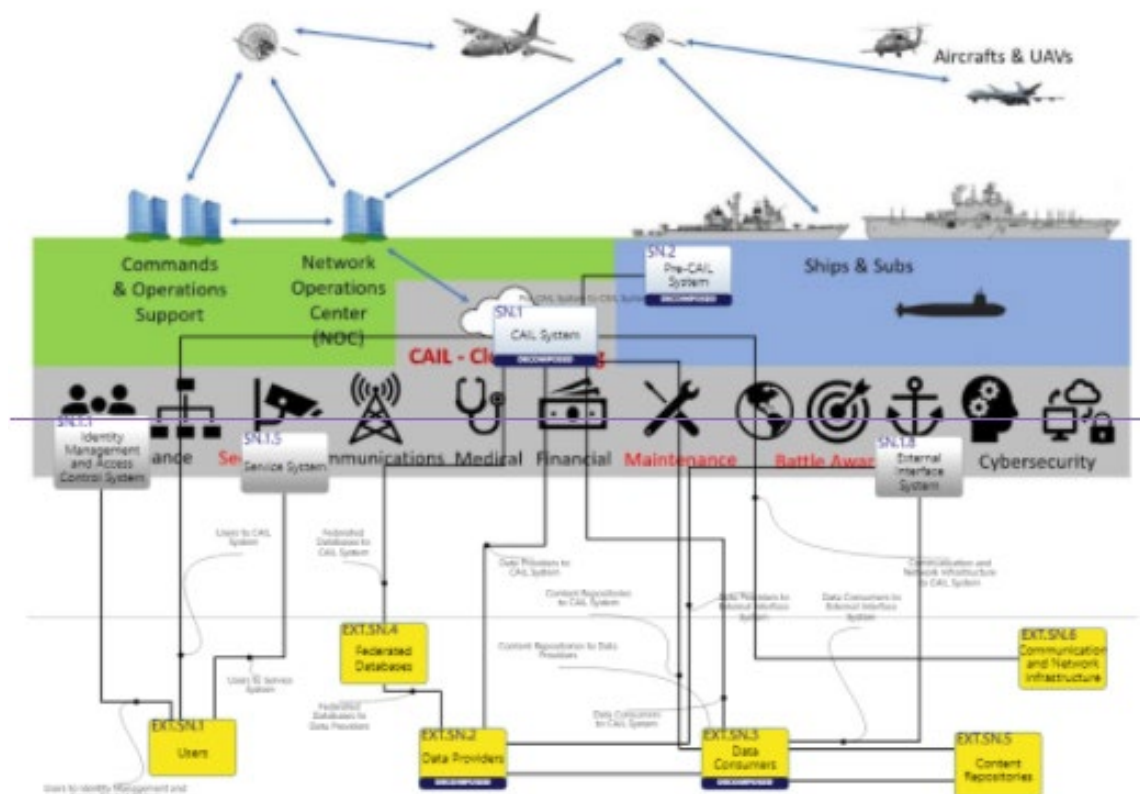


Figure 23. CAIL – OV-1 modified

6. Operational Activities / Event-Trace Descriptions (OV-5b/6c)

The team used the operational activities and sequences to capture event-trace descriptions (OV-5b/6c views) of the CAIL system. These descriptions are shown in Figure 24 (CAIL), Figure 25 (Pre-CAIL), Figure 26 (high-level CAIL capabilities), and Figure 27 (CAIL governance). This process incorporated timing and sequencing with the operational activities. The team used these descriptions as part of the CAIL cost analysis to run discrete-event and Monte Carlo simulations to summarize durations and costs.

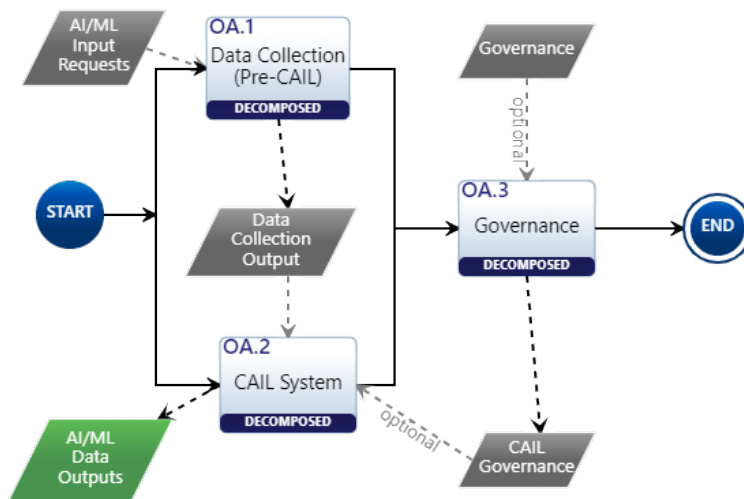


Figure 24. CAIL – OV-5b/6c

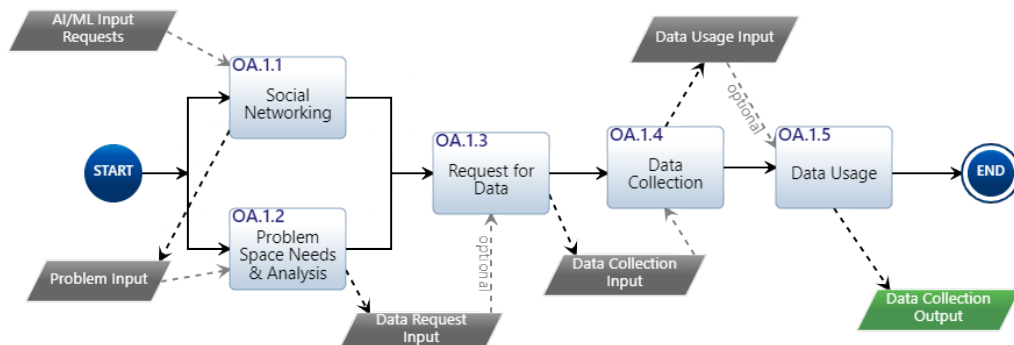


Figure 25. Pre-CAIL (Data Collection) – OV-5b/6c

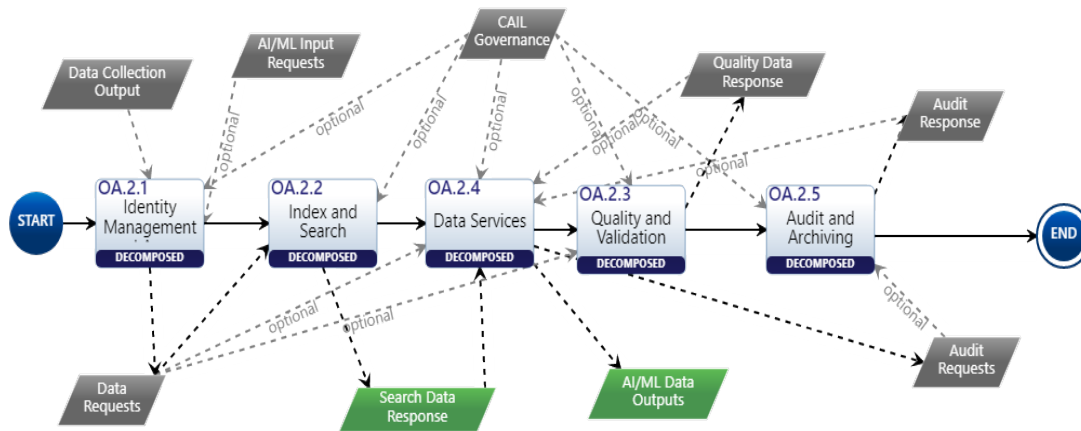


Figure 26. High-Level CAIL Capabilities – OV-5b/6c

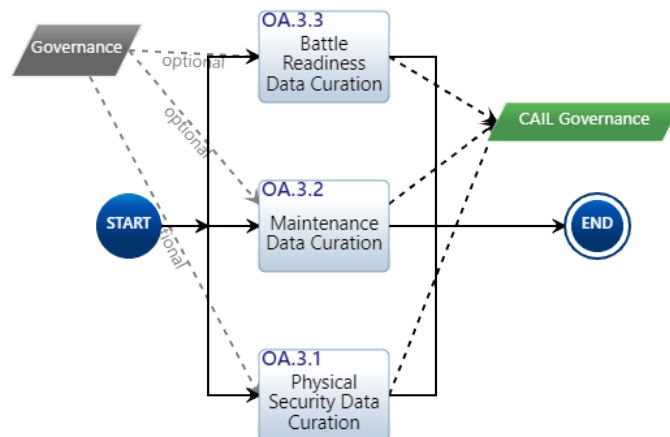


Figure 27. CAIL Governance – OV-5b/6c

The team developed an operational activity model (OV-5b) or IDEF0 (shown in Figure 28) to tie together the inputs, control, outputs, and the systems (assets) to the operational/functional activities. A larger version of the figure is also included in Appendix B.

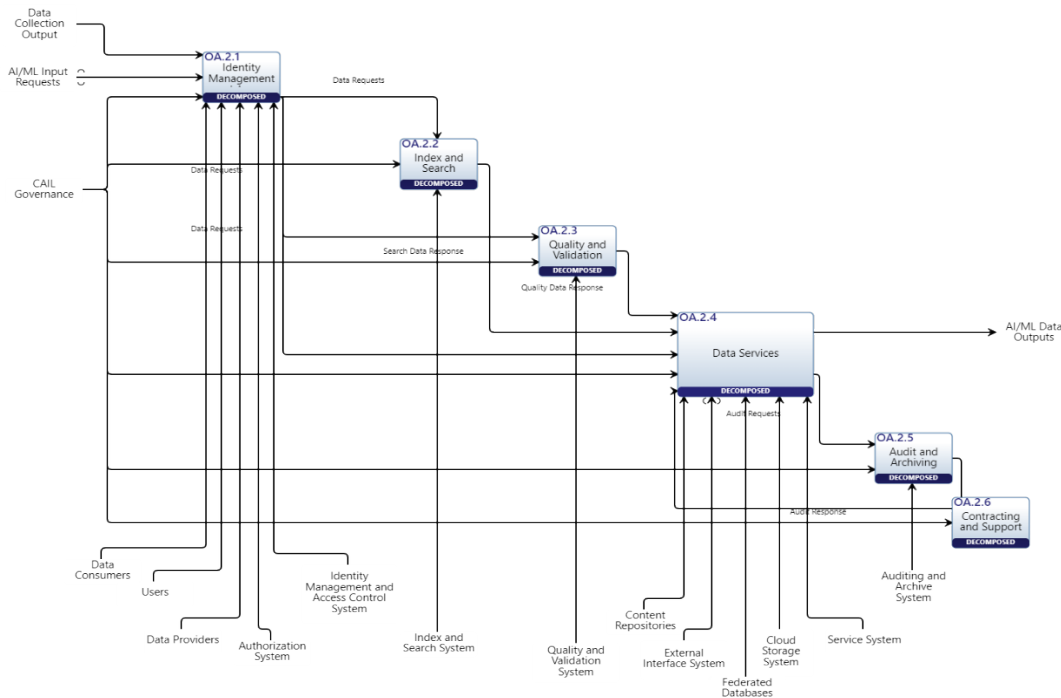


Figure 28. CAIL System – OV-5b or IDEF0

The team produced event trace descriptions for how the CAIL system might function within each of the three naval mission domain use cases. These descriptions are shown in Figure 29 (system maintenance), Figure 30 (physical security), and Figure 31 (battle readiness). These diagrams also supported the team’s cost analysis by setting duration and cost parameters for the operational activities for the discrete-event and Monte Carlo simulations to analyze durations and costs.

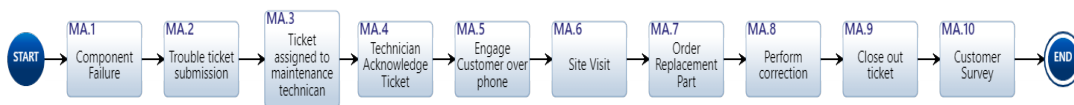


Figure 29. System Maintenance – CAIL Event Trace

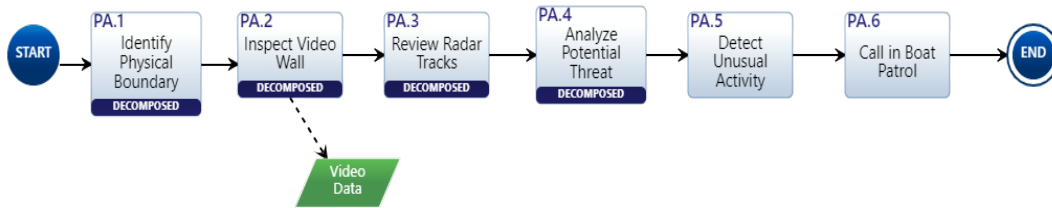


Figure 30. Physical Security – CAIL Event Trace

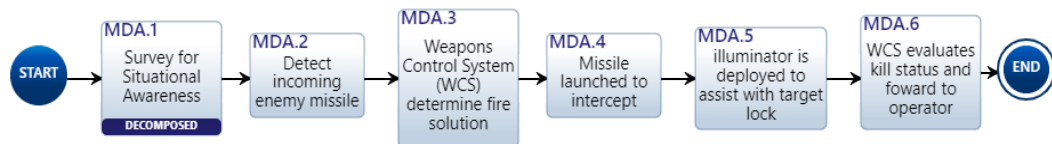


Figure 31. Battle Readiness – CAIL Event Trace

D. SUMMARY

The systems engineering and architecture process started with a stakeholder analysis from three separate domains to capture a comprehensive view of data needs across the system maintenance, physical security, and battle readiness domains. A CONOPS and CDM were each developed based on the needs and requirements. A top-down approach was taken using DODAF views to architecture the CAIL system. An OV-1 was developed to show the high-level operational view of CAIL. Other views such as the CV-2, OV-5a, SV-1, OV-2, OV-5b, and OV-5b/6c were included to model the various aspects of the CAIL system. These views help define the capabilities, input/output flow, external interfaces, and operational activities for the CAIL system. “Systems engineering and analysis reveals unexpected ways of using technology to bring new and improved systems and products into being” (Blanchard and Fabryky 2011, 23).

THIS PAGE INTENTIONALLY LEFT BLANK

V. EVALUATION AND ANALYSIS OF CENTRAL ARTIFICIAL INTELLIGENCE LIBRARY (CAIL) SYSTEM

Team Time Zone evaluated the utility and cost of implementing the CAIL system for DON. The team conducted three types of evaluation. The first evaluation assessed the utility of CAIL's application in the three naval mission domains of interest. This evaluation considered the benefits of implementing AI systems in the three domains as well as how the CAIL system could support the collection and grooming of data with each domain to support AI development. The second evaluation assessed how well CAIL aligned with the DOD Data Strategy. The third evaluation estimates the cost of implementing the CAIL system for the DON. The cost analysis was based on two methodologies: a traditional cost analysis and an MBSE cost analysis.

A. CAIL EVALUATION BASED ON THREE NAVAL MISSION DOMAINS

Team Time Zone evaluated the conceptual CAIL system's ability to support the data needs of the three DON mission domains of interest: system maintenance, physical security, and battle readiness. The team selected these domains early in the project based on their diverse missions, diverse data types, and diverse AI/ML applications. The team developed the CAIL system concept to support and enhance DON digital readiness across the Navy, so the three diverse mission domains were studied to analyze the data needs and challenges from a very broad perspective. This section presents an evaluation of how the CAIL system solution may be implemented within the three mission domains to support their uniquely taxing needs and individual objectives.

1. CAIL Support for System Maintenance

Naval system maintenance and logistics support requires near real-time access to a myriad of currently uncorrelated datasets to determine the proper routing and replacement of supplies necessary to support fleet operations. The priority for routing supplies can be prioritized by speed of delivery, cost of delivery, or to minimize availability vulnerabilities in the supply chain. Maintenance activities on ships underway would require future AI/ML

Algorithms to function autonomously using data from CAIL, given the limited communications capabilities of naval vessels underway.

The CAIL's contributions to logistics support would revolutionize how the Navy acquires, transports, stores, and delivers goods worldwide. The CAIL system could connect a diverse set of logistics datasets and use previous performance data to support AI/ML system predictions of future performance correlated with real-time information concerning current supply status. The AI/ML systems could track the current locations of vessels and both optimize delivery plans and predict delivery times. The CAIL data on current inventory levels could provide a real-time global inventory of any supplies requested. The CAIL data on known shipping routes, average route completion time, and cost could provide a complex matrix of alternative routing options.

The data from CAIL could support system maintenance by predicting spare part repair needs and planning the acquisition and delivery of spare parts. The CAIL could support the gathering of data regarding repair parts, their delivery, their locations, their inventory, and system failure rates. The AI/ML systems could correlate this data to provide an automated system that tracks and predicts the needs for spare parts and plans ahead for providing spare parts and forecasting when and where they might be needed. This capability could support battle groups as well as entire fleets. Such capabilities could circumvent supply choke points such as the 5th Fleet AOR. The ability to instantaneously compare the inventory and free available inventory space of each vessel in the battle group, the shore supply facilities in the U.S. and forward-deployed alone is too complex for humans. The AI/ML systems relying on the CAIL could observe possible issues, such as an engine part operating beyond its historic average useful lifespan with no spares onboard, notify appropriate personnel, and provide additional data to support several courses of action.

The CAIL could also support the development and implementation of AI/ML systems that predict supply and inventory needs across naval fleets. Since ship schedules are drafted several years in advance, the CAIL could act as a repository of this data. The CAIL could gather and provide data concerning a vast number of spare parts, failure rates, vessel and fleet inventories, and system characteristics. The AI/ML systems could use this

data to predict spare parts inventory needs for each system, ship and fleet and identify the source and location of spares and estimate when they might be delivered. This can support proactive logistics that predict the spare part needs of the navy.

The CAIL's contributions to maintenance would alter the DON's mindset and approach to preventative and corrective maintenance across the navy. The Navy's current approach to preventative maintenance appears to be "Status Quo." For instance, communication systems with cleanable/reusable filters require an "M" or monthly maintenance check; if the system has a removable filter accessible from the exterior, this check can be completed in roughly 30 minutes. Regardless of whether the filter is dirty or not, the technician must clean that filter monthly. Considering the number of filters on a U.S. Navy vessel, a significant amount of time is spent cleaning filters every month. As an example, ships have communication systems in multiple units stacked in standard equipment racks mounted at various heights relative to the floor and ceiling. Often the filters in the units on the bottom of the rack need to be replaced more often as they get soiled more quickly due to dust from the deck. In contrast, units located under the turbulent air of an air conditioning deck often show no indication of dust at all. Upgrading the standard fan assemblies with an airflow sensor would quantitatively reflect the cleanliness of the air filter. This introduces a new type of data that could be collected in CAIL and provided to intelligent systems that could observe the results and make this preventive maintenance task more efficient and cost-effective.

The CAIL system could support the development of streamlined AI/ML systems for shipboard maintenance. The CAIL's unique ability to gather, organize and deliver data to AI/ML developers would enhance their ability to train, test, and deploy algorithms. Maintenance algorithms could be developed for each vessel before its routine deployment; algorithms could reside within systems capable of sensing and logging all priority equipment data values like the airflow sensor mentioned previously. Intelligent systems could compare real-time incoming sensor values to historical values the algorithm was trained against to predict underperforming components and notify sailors to investigate the ailing components. Intelligent systems could detect failed parts, compile onboard data of failed systems and notify sailors and logisticians along with any casualty reports

(CASREPs) required for priority repairs. The CAIL's collection of this data would be invaluable in assisting shore-side personnel with diagnosing failure root causes and delivering the right personnel and equipment for immediate repair. Given the limited bandwidth of ships underway and the continual rotation of vessels in/out of port visits and returning from/preparing for deployments, CAIL could receive uploads of all pertinent equipment data from vessels while in onshore port services and returning to homeport from deployment. All AI/ML algorithms could have a standardized baseline before deployment, and then be retired after each deployment. Instead of retraining each older algorithm, a shore facility like DESRON could create and train a new algorithm for each vessel before an upcoming deployment. If there were an emergent need to retrain an original algorithm, a vessel could download a new algorithm during the next scheduled port visit or underway if necessary. Another option could be receiving an updated algorithm for ships underway via DVD or DAT tape. However, the idea of needing to retrain a maintenance algorithm throughout a routine deployment would be abnormal.

2. Evaluation of CAIL's Application to Physical Security Domain

The CAIL's integration with physical security practices would be a virtual force multiplier. Using commercially available imagery of animals and their movement, an algorithm could be trained to differentiate the movement of humans versus animals along perimeters and vast expanses. This enhancement alone would significantly improve the situational awareness of our physical security forces. Two areas where CAIL would excel that standard commercial data would not are in real-time data from diverse locations and the ability to query law enforcement databases. CAIL's infrastructure would provide a level of connectivity between all or most of our permanent/semi-permanent base enclosures, allowing events detected at one facility to influence the algorithm detection of other facilities. For instance, if there is an increased amount of small boat traffic outside one facility, then CAIL would correlate with the increase of traffic at other facilities and provide a better level of confidence if both seemingly isolated incidences are related. The AI algorithms to monitor cameras and foot traffic have been commonplace in the retail sales area for years. Retail businesses use this data better to arrange new arrival and sale items and predict the amount of foot traffic in the following months.

Connecting the algorithm to law enforcement/ state databases that physical security already has access to would provide an enhanced level of awareness for the limited physical security team (Gutierrez 2018). The security personnel have to call in a plate number to dispatch to verify the driver and vehicle history. By implementing an algorithm connected to CAIL, the security personnel could get detailed information like whether or not the vehicle owner has a licensed concealed weapons permit, or if the vehicle/owner has any outstanding warrants, simply by training the algorithm to query after simple if-then conditions. For instance, if the police lights are on, and the vehicle is stopped, and there is a license plate identified from the dashboard camera. By incorporating AI in this seemingly routine situation, the need for a dispatcher seated next to a computer to access the database is no longer necessary. The security forces have needed information available before they have to approach the driver to request his identification. A scenario in which a CAIL-enabled algorithm could provide currently unavailable assistance would be in deep learning from persistent tracking. There is known continual routine monitoring happening daily outside most of our naval bases and research facilities. By outfitting a camera system with CAIL access, the camera system could be trained to differentiate the operator and passengers of boats and cars routinely observed, not to cross over the complex laws of surveillance of citizens within the U.S. but to simply identify that a particular vehicle has an increased presence or has multiple different operators at different times would provide an added layers of information to security forces to assist in determining if the boat floating in the channel is a threat or not. The CAIL would also allow the information such as boat type and license information to be quickly queried to determine if that boat is genuine or if the operator placed a combination of random numbers and letter decals on the side to appear as being adequately credentialed.

3. Evaluation of CAIL's Application to Battle Readiness Domain

The CAIL system has great potential for supporting AI/ML developers working within the battle readiness domain. The AI/ML applications in this domain can improve the tactical picture and provide automated battle management aids to warfighters. Applications leveraging AI/ML can also enhance mission planning.

Data in this mission domain can be challenging to obtain. Much of the operational data comes from deployed platforms such as ships, submarines, and aircraft. Data may come from a variety of operational sensors and weapon systems. Data may take the form of threat track and identification data, fire control data, raw sensor data, and tactical link data. Another type of data needed represents the human decision process involved in the kill chain and mission planning processes. Much of the data in this domain does not exist or is classified or is not stored.

In order to obtain data to support AI/ML development in the battle readiness domain, developers are relying on training data or simulated data. Both of these types of data are not operationally representative enough to train AI/ML systems that are intended for operational use. Implementing the CAIL system can highlight gaps in required data and can support DON programs to obtain the data.

Once the DON is able to acquire operational tactical data, the CAIL system can streamline this process to ensure secure access and validated data to support AI/ML development.

One of the first authoritative database that could integrate with CAIL is the SYSCOM PEO Integrated data environment and repository (SPIDER). A RAND report from 2012 detailed the following information in SPIDER:

- Information on PEO C4I programs as they proceed through the NMP
- Descriptive data
- Program or system name
- PMW number (indicating who owns the program)
- SCD number
- Type of job being performed
- Installation duration. (Porche III 2012)

The data from this database would provide CAIL with the necessary operational data needed to assess the fleets C4I readiness at any given time. The data would help an AI/ML algorithm generate COAs based on operational availability of systems that would be critical to the mission. Also, this data could provide insightful correlation to mission success that might have otherwise been overlooked by the decision makers.

B. CAIL ALIGNMENT WITH THE DOD DATA STRATEGY

Team Time Zone analyzed the CAIL system through a qualitative evaluation of the system requirements. Each of the six major requirement categories were decomposed and evaluated to verify CAIL's ability to fulfill and maintain alignment with the DOD Data Strategy: data readiness, data bias, data curation, data taxonomy, data governance, and data security.

1. Data Readiness

The CAIL system would be capable of maintaining data readiness. CAIL's initial requirement was to ensure data integrity to include the necessary identification of data standardization, validation, and availability of data sources. Data is visible, accessible, understandable, linked, trustworthy, and interoperable. CAIL's ability to standardize data originating from a mission of interest during the ingest process ensures that all incoming data is complete. The data ingest process includes but is not limited to:

Standardization:

- Verifying sensor data uploads are complete while isolating and deleting any unverified uploads to ensure CAIL does not process partial or incomplete data.
- Verify all metadata is captured and tags are appended to each data entity.

Validation:

- Verify metadata tags match expected tags for each mission area.
- Verify data values are of the proper format and within expected parameters.

Source Availability:

- Verify uploaded data matches expected variation of data types for each mission area.
- Verify data size matches expected size for the duration of data captured for each mission area.

A typical data ingest example for a shipboard maintenance action would be as follows: CAIL receives an upload for the main reduction gear of DDG-XX; this maintenance action is expected to include data from 20 different sensors and contain performance data for 24 hours before and after the action was completed; CAIL receives the upload and using current error correction measures then ensures that all data transmitted was received and complete; if an upload is interrupted for any reason, all received data is isolated and discarded with an error logged and a notification sent to the data owner.

The CAIL system validates the data received by inspecting each entity value within each dataset. For example, a dataset for a revolution per minute (RPM) sensor attached to the turbine is received and CAIL tags that data as being turbine RPM data and each value is verified to be within an expected range that would correlate to the parameters of that turbine. If the system expects values between 100,000 and 500,000 but the dataset range is 50 to 100 then the data is flagged and an error logged with a notification sent to the data owner. This would ensure for instance that temperature data is not miscategorized as RPM data thus corrupting that data in CAIL.

The CAIL system verifies the source available for maintenance actions by ensuring 20 unique datasets correlate to the 20 sensors expected. The CAIL system also ensures that each dataset contains the correct number of fields per dataset that correlate to the test's sensor sampling frequency and duration. For instance, the RPM sensor takes a sample every second, and the duration is 24 hours, then there should be 86,400 values in the dataset ($60 \times 60 \times 24$). If the received data does not include the correct number of data records or the dataset do not contain the correct number of values, the data is flagged in an error log with a notification sent to the data owner.

The data is then trustworthy and integrated into the rest of the data available within CAIL with the completion of the ingest process. The CAIL users can now access this data provided proper user permission and approval are in place. This process completes the requirements of Data Readiness by making the data visible and accessible to user interfaces that are linked to the proper datasets that are interoperable within CAIL.

2. Data Bias

The CAIL system would be capable of mitigating data bias. The CAIL's initial requirement was to break down AI data from authoritative sources into the smallest elements to minimize data bias. The ingest process mitigates data bias by initially appending each dataset with all appropriate metadata tags and validating the depth and breadth of the associated datasets. This ensures that each dataset is decomposed to the smallest component value, contains all associated metadata, and is accessible for correlation as needed. An example that illustrates the fulfillment of this requirement would be determining engine performance. Suppose the engine performance was the only metric captured. In that case, the data could be biased to either enhance or degrade the actual performance depending on the motives of the user collecting the data. To calculate engine performance, CAIL must know the amount of fuel consumed and the engine's RPM at that instance in time and correlate that to the instantaneous load on the engine. If these three unique data points were not separate from the instantaneous correlating values, then the data could be significantly skewed. If the bias were to show enhanced performance as in the case with the engine running under no/light load then showing low fuel consumption for the given duration would be an alert. If the goal were to degrade the performance and the engine would be run under a heavy/full load then showing high fuel consumption for the given duration would be expected. By not capturing a complex data value like performance CAIL would not be able to mitigate that bias.

3. Data Curation

The CAIL system would be capable of performing Data Curation. The initial requirements for CAIL included: sharing AI data and referencing authoritative data sources; storing AI data for sharing and identification; descriptions on how the data fits into the taxonomy; detailed catalogs on all the metadata on the data.

All data in CAIL must complete the ingest process to prepare the data correctly. The CAIL user's interface contain all permissions associated with each CAIL user. The user can access all data ingested in CAIL with the proper permissions approved. Data ingested into CAIL does not necessarily mean the data is duplicated for use in CAIL. All

federated databases are organized to store data so as to avoid duplication. The CAIL system would maintain a pointer to the location of this data, a hash of the data would be used to ensure data integrity, and all associated metadata tags would be maintained about the data. If the data authority marks the data for archival or deletion, then CAIL would copy the data before deletion or update the pointer to the location of archived storage. Archived data will be compressed in the standard archival process. When CAIL is requested to provide archived data then CAIL would follow the pointer to retrieve the archived data, unpack the data and reassociate all relevant metadata tags. If the original data ingested into CAIL is not stored in CAIL, a copy of the ingested data with all associated information will be loaded into CAIL. The goal is to ensure all federated databases are CAIL compliant; however, at this time it is unrealistic to expect all current databases would be converted to CAIL.

4. Data Taxonomy

The CAIL system would be capable of maintaining data taxonomy. CAIL's initial requirement was to maintain structured data and provide standard formats and data types for other systems/programs. All data accessible to CAIL will have standard formats and types. Requests for data not currently stored in CAIL would be flagged and a notification sent to the data owner.

5. Data Governance

The CAIL system would be capable of maintaining data governance. A community and authoritative governing body is necessary to manage and provide rules to govern access and authorization to the CAIL data. The CAIL will be incorporated into the Navy Cyber program to ensure successful deployment and maintenance of the CAIL. In addition to maintaining all Navy cyber program requirements, CAIL will have a team of experts to maintain hardware and software operations and plan for future expansion of new data sources.

6. Data Security

The CAIL system would be capable of maintaining data security. A community of security experts is necessary to manage and provide rules to govern access and

authorization to the CAIL data. Access to CAIL would be available through registered government-furnished equipment and registered government or civilian users that have been approved in the Navy cyber program. For instance, CAIL would require that all IA and ATO's are maintained with a list of authorized users and terminals. This will ensure that access to CAIL would be restricted to only the users and terminals deemed necessary. The CAIL terminals may include a shipboard or shore-based server designed to collect, organize, and upload sensor data.

C. COST ANALYSIS

The team used two approaches to estimate the cost and time required to implement a CAIL system for the Navy: (1) a traditional cost estimating approach and (2) an MBSE approach. The MBSE approach used Innoslate to model CAIL and perform dynamic analysis of execution on the system actions over time using discrete-event and Monte Carlo simulations to determine the duration and cost for the CAIL system development and sustainment support.

1. CAIL Traditional Cost Assessment

The traditional cost estimate approach used an engineering buildup based on hours needed. The assumption is that the initial CAIL development and integration will be done by industry, so the team assembled a notional organizational chart of human resources that would be required in CAIL Non-Recurring Engineering (NRE) phases and in the CAIL sustainment. The percent hours of contribution to CAIL for each employee was then assumed.

- a. CAIL Non-Recurring Engineering (NRE) - This is the initial investment required to implement the CAIL system consisting of two phases. In both phases there is additional government oversight cost, based on historical Department of Defense programs and contractor fee/profit.
- b. Phase 1: CAIL Development - This section's requirements is software development required to make CAIL operational involving events such as design and development of the integrated data environment, development

of an AI/ML data analytical environment, and implementation of a security user interface platform.

- c. Phase 2: CAIL Integration - This section builds and extends phase 1, with software required to link the CAIL system to external databases where raw data is stored. In our specific examples this links the CAIL system to stored physical security data, maintenance data, and weapon system data.
- d. CAIL Sustainment - This is the recurring CAIL per year cost to continue operating CAIL, linking CAIL to more databases, updating CAIL with new data, and providing CAIL continuous maintenance and improvements.

Assumptions:

- a. CAIL costs are contained in a high-level Work Breakdown Structure
- b. CAIL cost schedule is broken into three different phases
 - i. Phase 1 – CAIL development.
 - ii. Phase 2 – CAIL integration.
 - iii. CAIL Sustainment – steady-state cost.
- c. CAIL cost was developed in Base Year 2021 dollars (BY21\$), then adjusted to Then Year dollars (TY\$), to show cost in outer years
- d. Labor rates risk-adjusted; the rates would go as low as \$158 per hour to as high as \$222 per hour. Mean was used = ~\$190 per hour
- e. Government Support factor of 0.32 * the total development based on a percent of total contractor costs were used, it is based on historical data
- f. Notional cost schedule profile for development and integrating efforts phasing of fiscal years (FY) FY 22 to FY26 was assumed
- g. CAIL Sustainment cost has been provided in cost per year needed for CAIL continuous operation
- h. The inflation factor is based upon February 2020 joint inflation calculator from the Naval Center for Cost Analysis (NCCA)
- i. One FTE is assumed to work 1920 hours per year, that is total hours in a year less 4 weeks for holidays and vacation
 - i. 52 weeks per year – 4 weeks = 48 weeks

- ii. 48 weeks * 40 hours per week = 1920 hours per year
- j. Methodology
 - i. Development = FTE * 1920 *% hours worked * Labor rate *
Inflation factor
 - ii. Government cost = 0.3177 * Total contractor costs
- k. Contractor Fee/Profit = 9% * total contractor costs

Table 8. CAIL Traditional Cost Summary

CAIL Cost Summary						
NRE	FY22	FY23	FY24	FY25	FY26	Total TY\$M
Total NRE	Cost in TY\$M					\$ 33.8
Phase 1						
Total CAIL Development						\$ 16.57
CAIL Development Cost	\$ 4.54	\$ 4.63	\$ 2.37			\$ 11.54
FTE hours	23,328	23,328	11,664			
Contractor Fee/Profit	9%					\$ 1.04
Government Support Phase 1						\$ 3.99
Factor	0.3177					
Phase 2						
Total CAIL Integration						\$ 17.19
CAIL Integration			\$ 4.73	\$ 4.83	\$ 2.46	\$ 12.02
FTE hours			23,328	23,328	11,664	
Contractor Fee/Profit	9%					\$ 1.08
Government support Phase 2						\$ 4.08
Factor	0.3117					
CAIL Recurring/Sustainment	FY22	FY23	FY24	FY25	FY26	Total
Per year recurring cost						\$ 4.01
Steady State Operation					\$ 4.01	

Table 9. CAIL Notional Human Resources Hours per Year

CAIL Human Resources	FTEs	Development % per year work	Development Hours	Sustainemnt % per year work	Sustainment Hours
Project Manager	1	100%	1,920	100%	1,920.00
Financial Management Lead	1	20%	384	20%	384.00
Software Lead	1	100%	1,920	75%	1,440.00
Software Engineer	1	100%	1,920	100%	1,920.00
Software Engineer	1	100%	1,920	75%	1,440.00
Database Engineer	1	100%	1,920	75%	1,440.00
System Lead Engineer	1	100%	1,920	75%	1,440.00
Design Engineer	1	100%	1,920	75%	1,440.00
Network Engineer	1	100%	1,920	75%	1,440.00
Logistics and Support Lead	1	100%	1,920	75%	1,440.00
Procurement Specialist	1	20%	384	20%	384.00
Technical Writer	1	100%	1,920	75%	1,440.00
Drafter	1	100%	1,920	75%	1,440.00
Information Assurance Lead	1	75%	1,440	75%	1,440.00
Total Hours	14		23,328		19,008

The traditional approach for the development of the CAIL system had a duration of five years with a cost in then year of \$33.8M. The CAIL sustainment per year recurring cost was \$4.01M.

2. CAIL MBSE Cost Assessment

In the book *Real MBSE*, Steven H. Dam (2019) states the following concerning cost simulations:

Many simulation techniques can be used, but discrete-event and Monte Carlo simulations are essential to systems engineering. Discrete event simulation allows us to use the process models developed during the functional analysis and constrain them with the physical limitations and resources to determine if the process models work. ... Executing discrete event simulations repeatedly to ensure that all potential paths are explored ... is called Monte Carlo. (115)

The Operational Activities and sequence of those activities to capture the event tracing and provide further details for the CAIL system were modeled in Innoslate. The team set duration and cost parameters for the operational activities that allowed us to run discrete-event and Monte Carlo simulations to summarize durations and costs.

Team Time Zone used Table 10, Schedule/Cost Risk Factor Multipliers, to determine risk factor multipliers. These risk factor multipliers were then used to create Table 11, CAIL System - Model Parameters, to input the duration and cost values into the CAIL System Innoslate model.

Table 10. Schedule/Cost Risk Factor Multipliers

Schedule/Cost Risk Factor Multipliers				
Sense of Risk Estimation	Risk Factor Multipliers	Min	Most Likely	Max
Routine Task	Low	0.90	1.00	1.10
Fairly Routine Task (minor uncertainty)	Low+	0.90	1.05	1.15
Development-type task, no particular technical difficulty expected	Moderate	0.90	1.10	1.25
	Moderate+	1.00	1.15	1.30
Development-type task, some technical difficulties could occur	High	1.00	1.20	1.50
	High+	1.00	1.30	1.80
Significant technical difficulties expected	Very High	1.25	1.50	2.50
No experience in this area	Very High+	1.50	2.00	3.00

Table Above: From CDR Mark Rhoads, Navy Deputy PM, GPS JPO.

Derived from the "Quantity Risk to Manage Cost and Schedule" by Fred Raymond, Acquisition Review Quarterly, Spring 1999

OS4010 Engineering Risk Benefit Analysis "Cost & Schedule Risk" CAPT Douglas E. Otte USN(Ret.) Week 8 - 25 Aug 2020

Table 11. CAIL System – Model Parameters

CAIL System of Systems - Model Parameters																	
Operational	OA Name	Schedule	Units	Risk Factor	Min	Most Likely	Max	# People	OA - Unit	OA - Cost	Risk Factor	Min	Most Likely	Max	Min	Most Likely	Max
OA.0	Top CAIL SoS OV-5a	0		Low	0	0	0	0	0	0	Low	0	0	0	0	0	0
OA.1	Data Collection (Pre-CAIL)	0		Low	0	0	0	0	0	0	Low	0	0	0	0	0	0
OA.1.1	Social Networking	90	hours	Moderate+	90	103.5	117	2	15	30	Moderate+	15	17.25	19.5	30	34.5	39
OA.1.2	Problem Space Needs & Analysis	90	hours	High	90	108	135	5	15	75	High	15	18	22.5	30	36	45
OA.1.3	Request for Data	200	hours	Very High+	300	400	600	5	15	75	Moderate	13.5	16.5	18.8	27	33	37.5
OA.1.4	Data Collection	120	hours	Very High+	180	240	360	5	15	75	Moderate	13.5	16.5	18.8	27	33	37.5
OA.1.5	Data Usage	90	hours	High	90	108	135	5	15	75	Moderate	13.5	16.5	18.8	27	33	37.5
OA.2	CAIL System	0	hours	High	0	0	0	0	100	0	High	100	120	150	200	240	300
	Identity Management and Access Control	0	hours	High	0	0	0	0	190	0	High	190	228	285	380	456	570
OA.2.1.1	User Identity	150	hours	High	150	180	225	5	190	950	Moderate	171	209	238	342	418	475
OA.2.1.2	System/Service Identity	150	hours	High	150	180	225	5	190	950	High	190	228	285	380	456	570
OA.2.1.3	Authorization	150	hours	High	150	180	225	5	190	950	High	190	228	285	380	456	570
OA.2.2	Index and Search	0	hours	High	0	0	0	0	190	0	Moderate	171	209	238	342	418	475
OA.2.2.1	Index/Catalog Data	150	hours	High	150	180	225	4	190	760	Moderate	171	209	238	342	418	475
OA.2.2.2	Search Data	150	hours	High	150	180	225	4	190	760	Moderate	171	209	238	342	418	475
OA.2.3	Quality and Validation	0	hours	High	0	0	0	0	190	0	High	190	228	285	380	456	570
OA.2.3.1	Data Verification	150	hours	High	150	180	225	5	190	950	High	190	228	285	380	456	570
OA.2.3.2	Metadata Verification	150	hours	Very High	188	225	375	5	190	950	High	190	228	285	380	456	570
OA.2.4	Data Services	0	hours	Very High	0	0	0	0	190	0	High	190	228	285	380	456	570
OA.2.4.1	Data Storage	150	hours	High	150	180	225	4	190	760	Moderate+	190	218.5	247	380	437	494
OA.2.4.2	Data Interfaces	150	hours	Very High	188	225	375	4	190	760	High	190	228	285	380	456	570
OA.2.5	Audit and Archiving	90	hours	Moderate+	90	103.5	117	0	190	0	Moderate	171	209	238	342	418	475
OA.2.5.1	Auditing	60	hours	Moderate+	60	69	78	2	190	380	Moderate	171	209	238	342	418	475
OA.2.5.2	Archiving	40	hours	Moderate+	40	46	52	2	190	380	Moderate	171	209	238	342	418	475
OA.2.6	Contracting Support	2000	hours	Low	1800	2000	2200	2	190	380	Moderate	171	209	238	342	418	475
OA.3	Governance	0	hours	High	0	0	0	0	190	0	High	190	228	285	380	456	570
OA.3.1	Physical Security Data Curation	90	hours	High	90	108	135	1	190	190	High	190	228	285	380	456	570
OA.3.2	Maintenance Data Curation	90	hours	High	90	108	135	3	190	570	High	190	228	285	380	456	570
OA.3.3	Battle Readiness Data Curation	90	hours	Very High+	135	180	270	6	190	1140	Very High+	285	380	570	570	760	1140
OA.4	CAIL System Sustainment	0	hours	Moderate	0	0	0	0	190	0	Very High+	285	380	570	570	760	1140
	Sustain Identity Management and Access Control	1920	hours	Moderate+	1920	2208	2496	2	190	380	Moderate+	190	218.5	247	380	437	494
OA.4.1	Sustain Index and Search	1920	hours	Low+	1728	2016	2208	2	190	380	Moderate+	190	218.5	247	380	437	494
OA.4.2	Sustain Quality and Validation	1920	hours	Moderate+	1920	2208	2496	2	190	380	Moderate+	190	218.5	247	380	437	494
OA.4.3	Sustain Data Services	1920	hours	Moderate+	1920	2208	2496	2	190	380	Moderate+	190	218.5	247	380	437	494
OA.4.4	Sustain Audit and Archiving	1920	hours	Low+	1728	2016	2208	2	190	380	Moderate+	190	218.5	247	380	437	494
OA.4.5	Sustain Contracts Support	1920	hours	Low+	1728	2016	2208	1	190	190	Moderate+	190	218.5	247	380	437	494

Ten thousand simulation runs were performed, and the results are shown in Figure 32 for the development of the CAIL system. The CAIL system had a duration mean of 5.06 years with a standard deviation of 2.68 months. The mean cost was \$32,903,309 and a standard deviation of \$896,484. The duration ranged from ≤ 4.63 years to 5.68 years. Cost ranged from $\leq \$29,821,726$ to \$35,295,433. The Data Interfaces activity took the longest time.

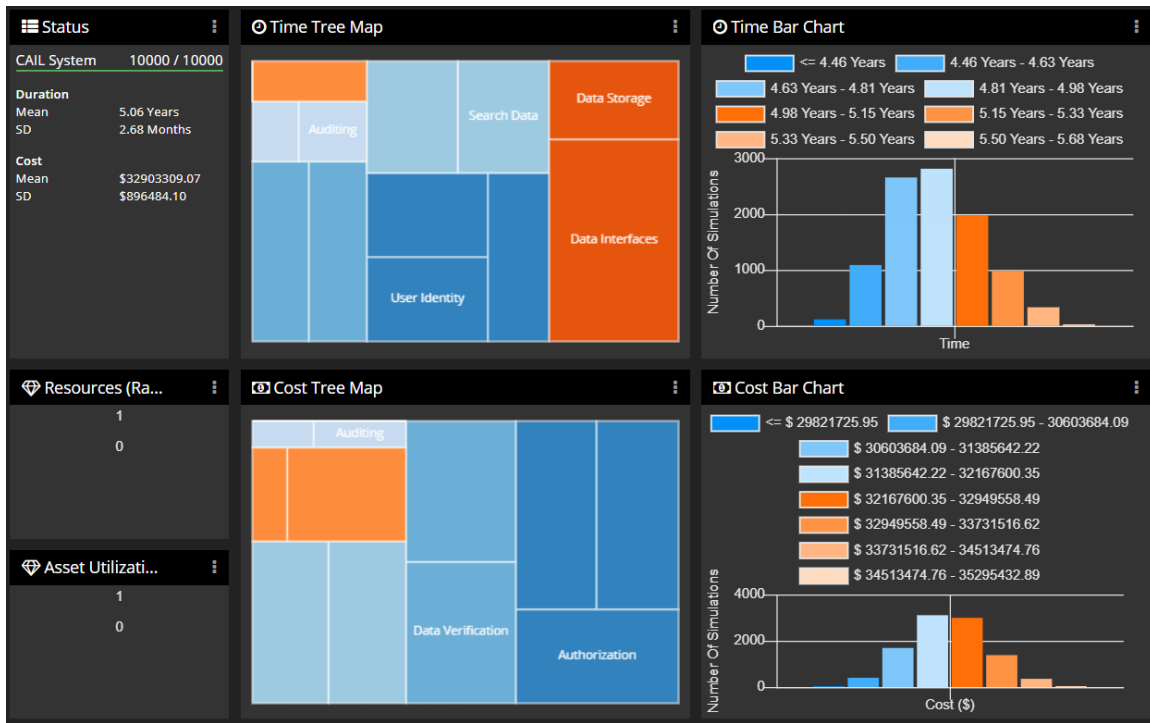


Figure 32. CAIL Monte Carlo Simulation Results

Additionally, the level of effort to support the CAIL system as part of the operations and maintenance support was modeled for a year, with the results shown in Figure 33. The CAIL sustainment support had a duration mean of 1.21 years with a standard deviation of 10.33 days. The mean cost was \$4,402,500 and a standard deviation of \$96,025. To capture the sustainment effort for one year, the team used triangle distributions to represent each sustainment activity duration to account for potential variations in execution times for the sustainment activities. This is then translated to cost values that the team could then determine the level of effort and cost to support the CAIL system. These results provide a

range of sustainment costs that will be required for the operations and maintenance for the CAIL system.

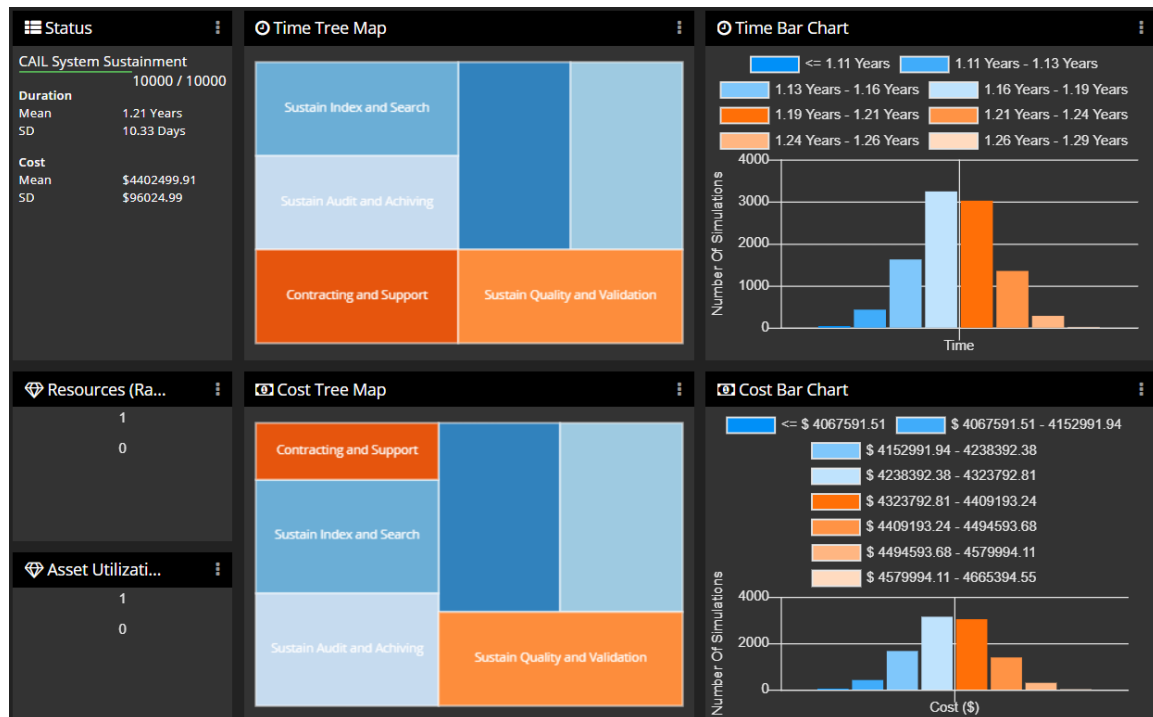


Figure 33. CAIL Sustainment Monte Carlo Simulation Results

3. Cost Summary

The traditional approach considered the total number of full time equivalent (FTE) hours based on the number of FTE positions and percent of the time expected to execute the development of the CAIL system. That FTE, labor rate per hour, and an inflation factor was used to determine the cost for each execution year required to complete the CAIL system.

The MBSE approach used the same cost labor per hour but focused on the modeled system activities required to develop the CAIL system but used a triangle distribution based on the hours estimated to complete the system activity and a risk factor translating complexity of that activity to a min, max, and most likely distribution parameters that could be used in the Monte Carlo simulation. This MBSE approach could have used a triangle

distribution for the cost but team Time Zone decided to keep it simple and only varied the duration. To account for multiple personnel required to complete each system activity the cost was multiplied by the number of personnel required. The total number of personnel was adjusted so to match the traditional total number of positions. The MBSE approach did not update the cost per year with an inflation factor compared to the traditional approach.

The CAIL system development and sustainment duration and cost summaries are shown in Table 12.

Table 12. CAIL System Cost Summary

CAIL System Cost Summary				
Description	Traditional		MBSE	
	Duration	Cost	Duration	Cost
CAIL Development	5 years	\$33.8M	5 years	\$32.9M
CAIL Sustainment	1 year	\$4M	1 year	\$4.4M

The differences were due to the assumptions on the approaches. The traditional approach used positions and percent per year work required for that position. The MBSE approach used system activities which is the beginning of one's work breakdown structure to determine the duration required to complete and accounted for the number of personnel required by adjusting the cost per hour corresponding to each system activity.

It is best to use both approaches to help check and validate duration and cost estimates. If more time were available, the team could have refined both approaches to improve the cost and durations results.

VI. CONCLUSION

Team Time Zone concludes that based on the needs and stakeholder analysis and systems engineering analysis approach of modeling and analyzing the DON's data needs to support AI/ML development, that a CAIL system and process is needed to support DON digital readiness. The needs and stakeholder analysis highlighted the critical importance of gathering and curating data for AI/ML development and also highlighted the current gap in providing this data throughout the DON's mission domains. Team Time Zone approached this problem by (1) conducting a needs analysis that included stakeholder interviews with SMEs from three diverse DON mission domains, (2) developing a set of requirements, (3) synthesizing a solution by developing a conceptual design for the CAIL system, and (4) evaluating the CAIL based on its application to the three mission domains, its ability to meet requirements, and its estimated cost. This conclusion contains the team's major findings and recommendations for future research to support the DON's implementation of the CAIL system and process to foster "data as a strategic asset" (DOD 2020).

A. TEAM TIME ZONE'S FINDINGS

Finding #1: Navy must follow industry's bottom-up approach to data.

According to a senior NIWC AI/ML scientist (interview from February 16, 2021), ONR met with experts from Google to understand their process for managing data for AI development. Google said they do everything from the bottom up. They have stopped looking at the problem from the top down. However, leadership in the Navy have not adopted this practice yet. The Navy needs more experiments to see if a bottom up approach will work.

The Navy must institute a bottom-up approach to data, using the best practices of industry (Google, Amazon, Microsoft). The Navy must identify data at the system and operational levels to provide a data foundation for AI/ML development. By locating these data sources and making an effort to have this data made accessible to data scientists and developers, the Navy can streamline the data management process. Boehm et al. (2019,

101) write that “according to recent surveys of data scientists in practice, all data-related processes typically consume 80–90% (if not more) of the time and effort spent by most data scientists.” to be trained and function accurately. The Navy can save significant time and money by supporting data collection from the bottom up.

Finding #2: Navy programs/systems need to identify data and develop interfaces to access the data

The team found that many obstacles that currently exist to supporting Navy AI/ML developer data needs. In many cases programs and systems are unknowingly restricting data access through cumbersome approval processes, data “stovepipes,” security challenges, and governance issues. In other cases, programs and systems are not saving and storing data that could be useful.

The team found that Navy programs and systems need to support the process of identifying data that could be useful for AI/ML development and making the data accessible. These programs and system need procedures and methods for securely sharing data. The team found that data needs to be accompanied by metadata that contains information about the source and context of the data.

Finding #3: Navy needs persistent and dynamic digital data

The team found that many commands and laboratories across the DON are researching and developing AI/ML capabilities, but there is no coordinated process for all programs and developers to access the data they require. Through the needs analysis, the team found that naval AI/ML developers require needs persistent and dynamic digital data that is validated and representative of operational naval missions.

Finding #4: Navy data needs to be catalogued and organized

The team compared information gathered for each of the three naval mission domains (system maintenance, physical security, and battle readiness) and found that the data needs for the domains range from slight differences to significant differences. All three mission domains produce classified. The system maintenance domain largely produces textual data and associated quantitative data (such as failure rates); the physical security

domain largely produces video surveillance data; and the battle readiness domain largely produces sensor tracking data and system capability data. The team found that naval data needs to be catalogued and organized. Naval data needs to be accompanied by metadata that contains information for the source of the data, where to locate it, and how it was collected. Metadata provides critical descriptive and contextual information concerning the data.

Finding #5: Navy needs to identify data sources throughout naval mission domains

The team found that useful data exists (or could be obtained) throughout the Navy. The team's study of the three naval mission domains revealed that the domains have very specific types of data that could be useful to AI/ML developers. The team found that in many cases, it is a manually intensive effort to obtain data and may involve naval domain operators (warfighters in some cases) working directly with AI/ML developers to gather data. The Navy can start by reviewing programs and systems in all naval mission domains to identify applications for AI/ML methods and by identifying data that could be useful.

Finding #6: There is a limited understanding of AI/ML applications to future naval mission domains

The team found that there is currently a limited understanding of the future applications of AI/ML methods across naval mission domains. The team recognized that the capabilities will evolve over time and that this may change the Navy's data needs. The team also recognized that future AI/ML methods, models, algorithms, and rules may operate together in the future to offer more capabilities for the Navy to address complex multiple mission domains.

Finding #7: CAIL will require a system of systems approach

As the team developed a conceptual design of the CAIL system, they realized that a system of systems engineering (SoSE) may be appropriate for implementing the CAIL system. The team discovered that the CAIL will involve close integration with a large number of disparate and diverse Navy systems throughout naval mission domains. By taking an SoSE approach the Navy could better manage data governance challenges and

the challenges involved in managing a complex set of organizations with many system “owners” that have diverse priorities and plans. A SoSE approach would balance the development of the CAIL system with competing system and program objectives and schedules. A SoSE approach would support the integration of the large amounts of data from the many diverse sources.

Finding #8: CAIL will require development and sustainment costs

Team Time Zone performed a cost analysis to estimate the development and sustainment costs of implementing the CAIL system. The team’s projected cost for the development of the CAIL system had a duration between four years and six years with a cost that ranged between $\leq$ \$29.8M to \$35.3M . The team’s estimated cost for CAIL sustainment was a recurring cost of \$4.4M per year.

A. RECOMMENDATIONS AND FUTURE AREAS OF RESEARCH

Team Time Zone explored the data needs of Navy AI/ML developers in depth and found that without an integrated and comprehensive approach, the process of data management will continue to be very challenging, costly, and time-consuming. In order to support digital readiness and encourage the adoption of AI/ML innovations, Team Time Zone recommends that the Navy implement the CAIL system as a solution for streamlining the process of data management throughout mission domains. This section contains the team’s recommendations to support the Navy’s implementation of the CAIL system.

Recommendation #1: Understand data management requirements at the warfighter operational level

The DON must define and develop warfighter operational mission models that capture decision processes and operations, to support the gathering of data on these decision processes and operations. This data can be useful for supporting the training and development of AI/ML algorithms. This will support the process of identifying naval data across diverse mission domains.

Recommendation #2: Understand data management needs at the system level

The DON needs to identify and develop system models for each of their program's systems and subsystems in order to support the identification and gathering of naval data at the system level.

Recommendation #3: Understand data management needs at the SoS level

The DON needs to identify and develop SoS models to represent comprehensive architectures and to understand system interactions and linkages. These SoS models will help the Navy discover datasets at the SoS-level that could be useful to AI/ML developers. This will foster the development of an SoS community of support to the CAIL system for data contributions at all levels and across mission domains.

Recommendation #4: Research and develop new AI/ML methods and applications

The DON needs to continue to research and develop new AI/ML methods and applications and develop data requirements to evolve alongside this advancement.

Recommendation #5: Develop cross-domain information gateways

The DON needs to continue to develop more capable cross-domain solutions that provide information gateways to allow data to flow between the various naval mission, security, and network domains. The DON needs to implement the enterprise-wide CAIL solution to allow these information gateways to screen data content and provide validated and secure data access.

Recommendation #6: Research human machine interactions

The DON needs to continue to research effective human machine interactions to support effective human-machine teaming as more AI/ML methods are implemented in naval operations. Human machine interactions need to develop improved feedback to build trust and safety during operations. The Navy needs to identify and develop datasets that represent effective human-machine interactions to support this research.

Recommendation #7: Establish the CAIL System

The DON needs to provide persistent and dynamic digital data to naval AI/ML developers through the implementation of the CAIL system. The CAIL needs to be established to govern, develop and define data standards to integrate data from the diverse naval mission domains along with metadata to offer a single source integrated data service architecture.

B. SUMMARY OF TEAM'S FINDINGS AND RECOMMENDATIONS

Team Time Zone's analysis of the data needs of the Navy to support AI/ML brought to light a larger and broader capability gap not being addressed: the DON needs persistent and dynamic digital data management across the entire enterprise. The DON could streamline data management by following industry (Google, Amazon, and Microsoft) approaches to understand data from the bottom-up. The team recommends that the DON develop and implement a CAIL SoSE approach to govern, develop and define data standards to integrate and interoperate data from all the data sources into a library catalog for data and metadata stored in various databases and authoritative data sources offering a single source integrated data fabric service for the Navy.

Team Time Zone developed a prioritized summary of findings and recommendations, as illustrated in Table 13. The "red" priority is the DON's need to identify and understand what data exists. Findings #2 and #5 map into this category and the team recommendations #1 and #2 stem from this need. The "yellow" priority is the DON's need to develop the CAIL system and SoS governance. This category stems from the team's findings #7, #8, and #1 and the team recommends that the Navy follow recommendations #1-3, #5, and #7. The "green" priority is the DON's need to continue to pursue areas of future research. This category stems from the team's finding #6 and the team recommends #4 and #6 for the Navy.

Table 13. Time Zone Prioritized Summary

Time Zone Prioritized Summary			
Priority	Category	Problems	Actions
1	Identify & understand what exists	Finding #2: Navy programs/ systems need to identify data and develop interfaces to access the data	Recommendation #2: Understand data management needs at the system level
		Finding #5: Navy needs to identify data sources throughout naval mission domains	Recommendation #1: Understand data management requirements at the warfighter operational level, #2 Understand data management needs at the system level
		Finding #4: Navy data needs to be catalogued and organized	Recommendation #1: Understand data management requirements at the warfighter operational level, #2 Understand data management needs at the system level
		Finding #3: Navy needs persistent and dynamic digital data	Recommendation #7: CAIL needs to be established
2	Develop CAIL SoS architecture & SoS governance	Finding #7: CAIL will require a system of systems approach	Recommendation #3: Understand data management needs at the SoS level from Recommendations #1 and #2 into a comprehensive architecture
		Finding #8: CAIL will require development and sustainment costs	Recommendation #7: CAIL needs to be established
		Finding #1: Navy must follow industry's bottom-up approach to data	Recommendation #1: Understand data management requirements at the warfighter operational level, #2 Understand data management needs at the system level, #3: Develop SoS models to link all of the systems, #5 Develop cross-domain / information gateways, #7 CAIL needs to be established
3	Areas of future research	Finding #6: Limited understanding of AI/ML applications to future naval mission domains	Recommendation #4: Research and develop new AI/ML methods and applications , #6 Research human machine interactions.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. INTERVIEW QUESTIONS

1. QUESTIONS FOR WARFIGHTER (END USER)

- Is there a process and/or procedure that you use to perform your job?
- Is there a system or systems you need to perform your job?
- Are you aware of the data and/or interfaces for these systems?
- Do you know the program sponsors or have any POCs for these system(s)?
- How long does it take to perform these tasks?
- Are there any issues and/or gaps in capability that would help to perform you job better?
- In your opinion are there any tasks that you that think would be automated?
- What type of data is collected in the process of your work?
- Where do we store the data collected during normal operations?

2. QUESTIONS FOR DATA PROVIDERS

- Would you briefly describe the AI/ML strategy and/or capabilities you are working to provide for the Navy? Or is there a website/document we could reference to get a better understanding on the strategy/capabilities?
- Our understanding of AI/ML systems are data intensive requiring large amounts of data to train ML algorithms. Wanted to get your thoughts/ideas on how the Navy should start to tackle this complex problem?

- Are there any issues and/or gaps in capability that would help improve the system you are developing or supporting?
- Is there a process and/or procedure that you are aware of that the end users use to guide them on understanding the system/capabilities you are providing?
- Do AI/ML engineers typically look for Algorithms first and then data set or vice versa?
- There are many different image files and video files types, are certain files types preferred over others? Is preference based on ML algorithms chosen?
- Is there a preference between open source versus proprietary data types?
- What was the longest amount of time spent to get data? Shortest amount of time to get data?
- Given the data that is collected during normal operations, in your opinion do you think AI/ML would be used to improve the process?

3. QUESTIONS FOR DATA CONSUMERS

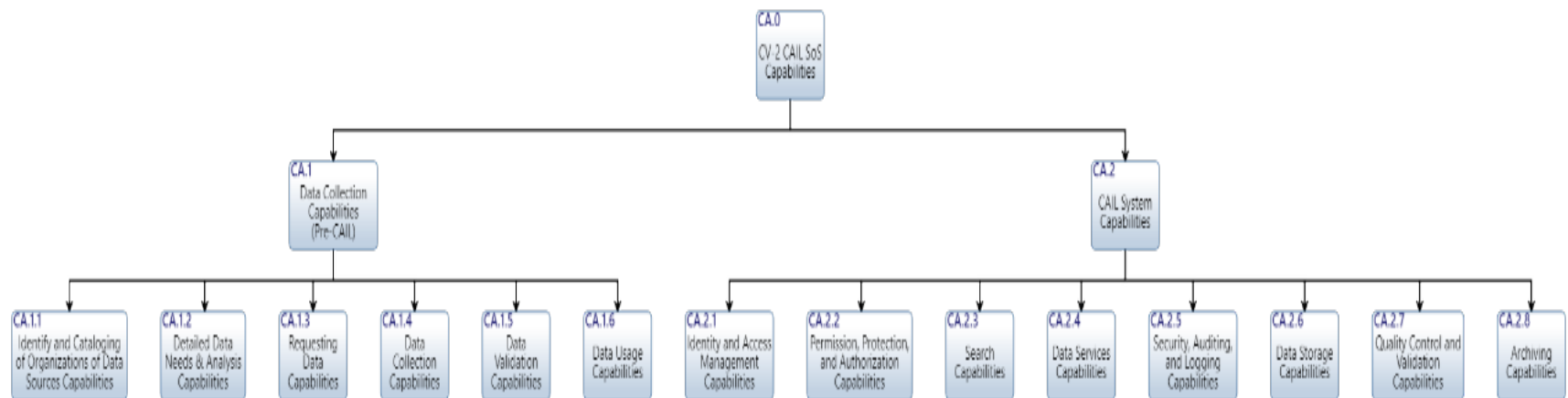
- Are there processes and/or procedures to help you in designing/developing/supporting the system you are working on?
- Are there data and/or interfaces that would help your system to use AI/ML?
- Any authoritative data sources that you need access to?
- Do you know the process and/or procedures to access these authoritative data sources?

- How long does it take get access to these data sources?
- Are there any issues and/or gaps in capability that would help improve the way you are designing the system

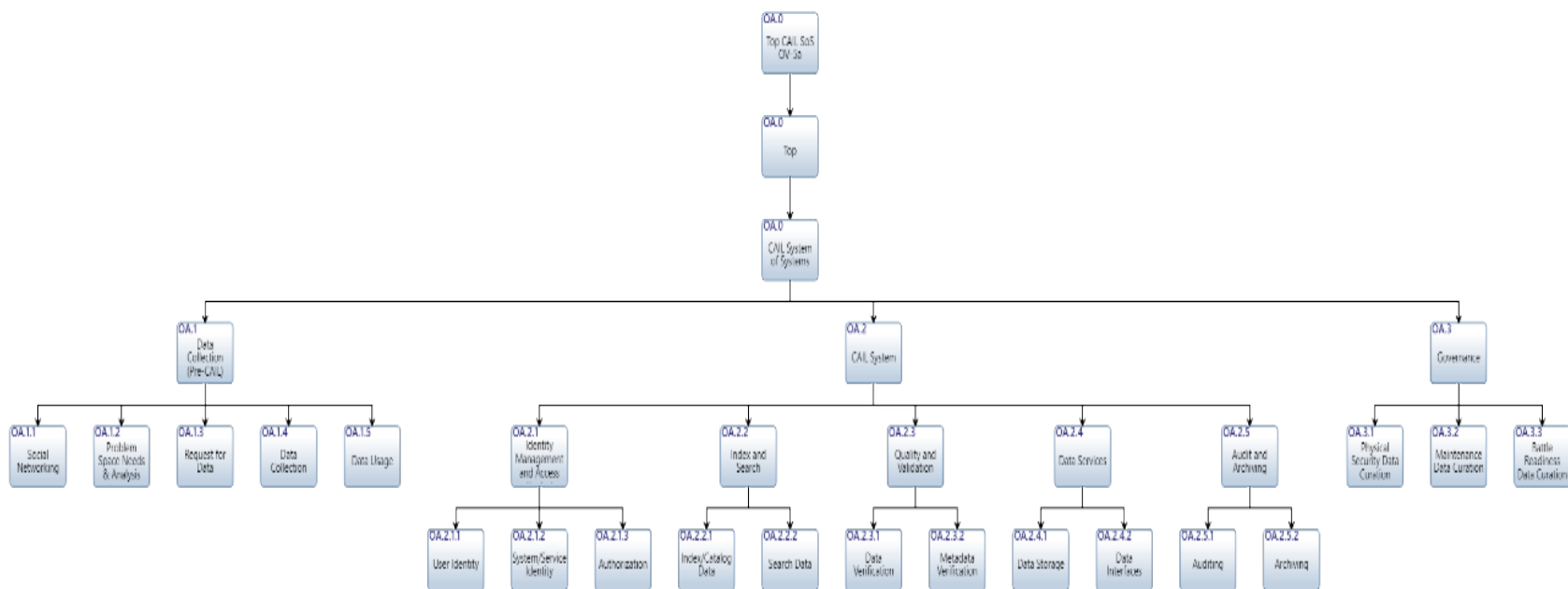
THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DIAGRAMS

1. CAIL CV-2



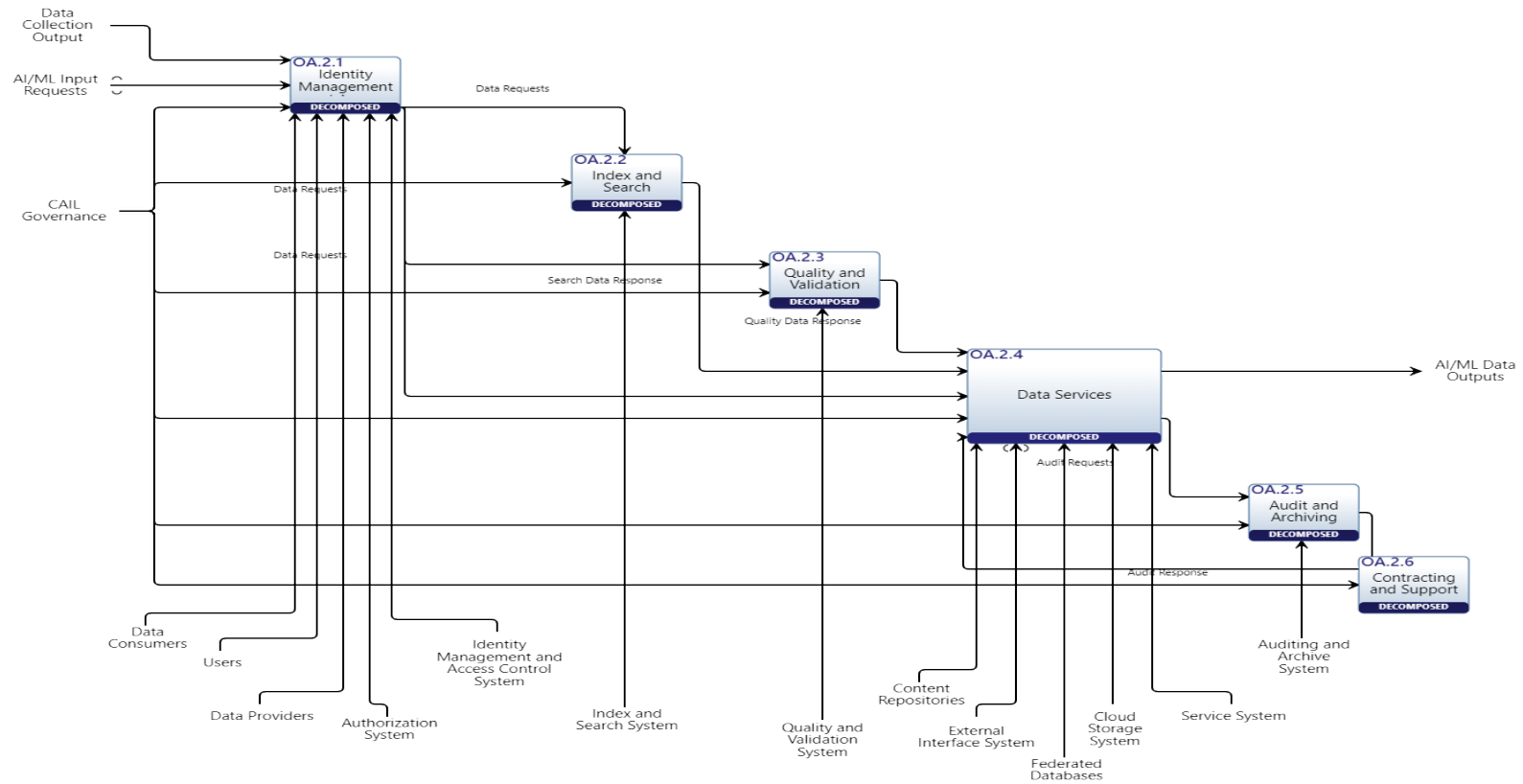
2. CAIL OV-5a



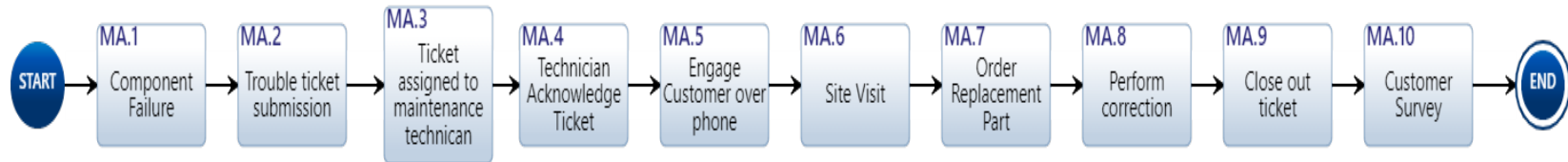
3. Capabilities to Operational Actions Mapping

	OA.0 CAIL System of Systems	OA.0 Top	OA.0 Top CAIL SoS OV-5a	OA.1 Data Collection (Pre-CAIL)	OA.1.1 Social Networking	OA.1.2 Problem Space Needs & A...	OA.1.3 Request for Data	OA.1.4 Data Collection	OA.1.5 Data Usage	OA.2 CAIL System	OA.2.1 Identity Management and ...	OA.2.1.1 User Identity	OA.2.1.2 System/Service Identity	OA.2.2 Index and Search	OA.2.2.1 Index/Catalog Data	OA.2.2.2 Search Data	OA.2.3 Quality and Validation	OA.2.3.1 Data Verification	OA.2.4 Metadata Verification	OA.2.4.1 Data Services	OA.2.4.2 Data S...
CA.0 CV-2 CAIL SoS Capabilities	X	X	X																		
CA.1 Data Collection Capabilities (Pre-CAIL)				X																	
CA.1.1 Identify and Cataloging of Organiz...				X	X	X															
CA.1.2 Detailed Data Needs & Analysis Ca...					X	X															
CA.1.3 Requesting Data Capabilities							X														
CA.1.4 Data Collection Capabilities								X													
CA.1.5 Data Validation Capabilities							X	X													
CA.1.6 Data Usage Capabilities								X													
CA.2 CAIL System Capabilities									X												
CA.2.1 Identity and Access Management C...										X	X	X	X								
CA.2.2 Permission, Protection, and Author...											X	X	X								
CA.2.3 Search Capabilities														X	X	X					
CA.2.4 Data Services Capabilities																		X			
CA.2.5 Security, Auditing, and Logging Ca...																					X

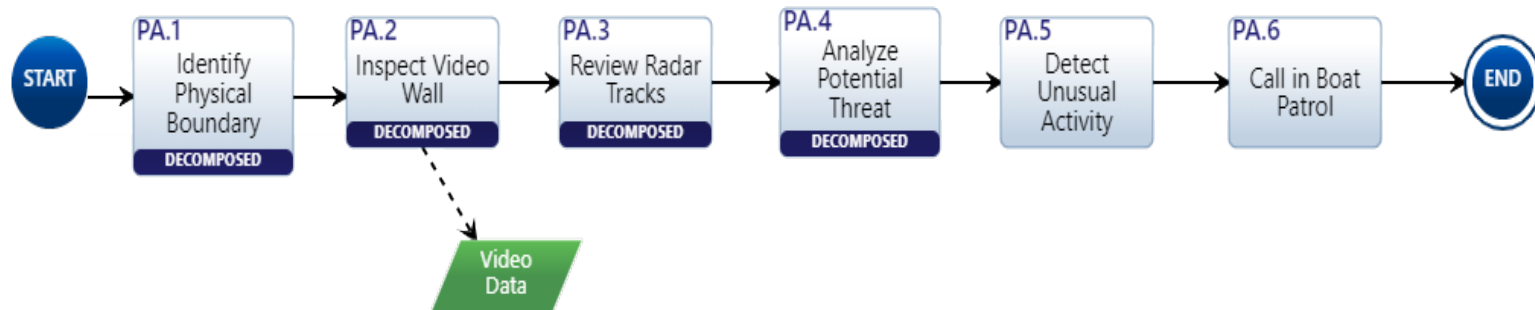
4. CAIL System – OV-5b or IDEF0



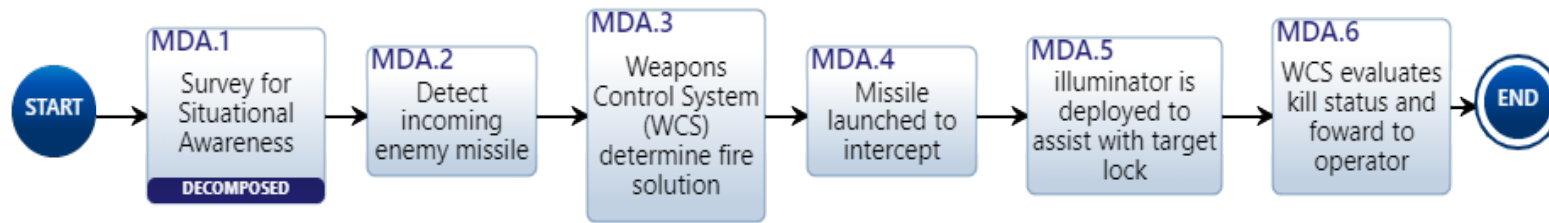
5. Action Diagram System Maintenance



6. Action Diagram Physical Security



7. Action Diagram Battlegroup readiness



LIST OF REFERENCES

- Atherton, Kelsey. 2020. "Navy Turns To A.I. To Save Billions In Fight Against Rust." *Breaking Defense* online, August 27, 2020. Accessed April 18, 2021. <https://breakingdefense.com/2020/08/navy-turns-to-ai-to-save-billions-in-fight-against-rust/>.
- Bird, Michael. 2020. "What AI means for you and your business—Now and in the future." Jul 22. Accessed 11 21, 2020. <https://www.hpe.com/us/en/insights/articles/what-ai-means-for-you-and-your-businessnow-and-in-the-future-2007.html>.
- Bodenmüller, Albert. 2013. "Application of Bayesian Reasoning for Military Identification and Classification." *13th International Conference on Intelligent Systems Design and Applications IEEE Xplore* 13–19.
- Boehm, Matthias, Arun Kumar, and Jun Yang. 2019. "Data Management in Machine Learning Systems." Morgan and Claypool Publishers. February 25.
- Eckert, C., Neris Nieves-Robbins, Elena Spieker, Tom Louwers, David Hazel, James Marquardt, Keith Solveson, A. Zahid, Muhammad Ahmad, Richard Barnhill, T. McKelvey, Robert C. Marshall, E. Shry, and A. Teredesai. 2019. "Development and Prospective Validation of a Machine Learning-Based Risk of Readmission Model in a Large Military Hospital." *Applied Clinical Informatics* 316–325.
- Chollet, Francois. 2019. "On the Measuer of Intelligence." <https://roberttlange.github.io/posts/2020/02/on-the-measure-of-intelligence/>. Nov 5. Accessed Apr 18, 2021. <https://arxiv.org/pdf/1911.01547.pdf>.
- Coraddu, Andrea, Luca Oneto, Alessandro Ghio, Stefano Savio, Massimo Figari, and Davide Anguita. 2015. "Machine Learning for wear forecasting of naval assets for condtion-based maintenance applications." *IEEE Xplore* 1–5.
- Dam, Steven H. 2019. *Real MBSE*. Coppel, TX: SPEC Innovations.
- DeMers, Dan. 2021. *What is Data Fabric? Exploring an Emerging Technology*. Jan 15. Accessed Mar 28, 2021. <https://learn.g2.com/data-fabric>.
- Dietrich, Manzey, Juliane Reichenbach, and Linda Onnasch. 2012. "Human Performance Consequences of Automated Decision Aids." *Journal of Cognitive Engineering and Decision Making* 6, no. 1, January 13: 57–87.
- Department of Defense. 2020. *DOD Data Strategy 2020*. Washington, DC: U.S Dept of Defense. Accessed May 4, 2021. <https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-Data-Strategy.pdf>.

- . 2019. “Summary of the 2018 Department of Defense Artificial Intelligence Strategy.” Washington, DC: U.S Department of Defense. Accessed Apr 24, 2021. <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/Summary-of-DOD-AI-Strategy.pdf>.
- Eleanor Bird, Jasmin Fox-Skelly, Nicola Jenner, Ruth Larbey, Emma Weitkamp, and Alan Winfield. 2020. *The ethics of artificial intelligence: Issues and initiatives*. Brussels, European Union, Mar.
- Éloi Bossé, Jean Roy, and Steve Wark. 2007. *Concepts, Models, and Tools For Information Fusion*. Norwood: Artech House, Inc.
- Fabrycky, Benjamin S., and Wolter J. Blanchard. 2011. *Systems Engineering and Analysis*. Fifth Edition. Upper Saddle River: Prentice Hall.
- . 2011. *Systems Engineering and Analysis*. Fifth Edition. Upper Saddle River: Prentice Hall.
- Faisandier, Alan, Garry Roedler, and Rick Adcock. 2020. *System Architecture - SEBoK*. Oct 30. Accessed Mar 28, 2021. https://www.sebokwiki.org/wiki/System_Architecture.
- Feldman, Philip, Aaron Dant, and Aaron Massey. 2019. *Integrating Artificial Intelligence into Weapon Systems*. May 10. Accessed January 15, 2021. <https://arxiv.org/abs/1905.03899>.
- Ganzfried, Sam, Conner Laughlin, and Charles Morefield. 2019. “Parallel Algorithm for Approximating Nash Equilibrium in Multiplayer Stochastic Games with Application to Naval Strategic Planning.” *ArXiv abs/1910.00193*.
- Gidlay, ADM Mike. 2021. “Chief of Naval Operations (CNO).” *Jan*. Washington, DC: U.S. Navy. Surface Navy Association Symposium.
- Godbole, Amrut. 2020. *AI & Machine Learning for the Indian Navy*. Mumbai, India, April 23.
- Guide to the Systems Engineering Body of Knowledge. 2020. *Stakeholder Needs and Requirements*. Oct 30. Accessed Apr 11, 2021. https://www.sebokwiki.org/wiki/Stakeholder_Needs_and_Requirements.
- Gutierrez, Daniel. 2018. “insideBIGDATA Special Report: Reinventing the Retail Industry through Machine and Deep Learning (Part 2).” *Inside Big Data*. February 20. Accessed April 10, 2021. <https://insidebigdata.com/2018/02/20/insidebigdata-special-report-reinventing-retail-industry-machine-deep-learning-part-2/>.

- Harper, John. 2021. *Federal A.I. Spending to Top \$6 Billion*. February 10. Accessed April 18, 2021. [https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-\\$6-billion](https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-$6-billion).
- Heinze, Clinton, Simon Goss, and Adrian Pearce. 1999. "Plan Recognition in Military Simulation: Incorporating Machine Learning with Intelligent Agents." *Proc of IJCAI-99 Workshop on Team Behaviour and Plan Recognition* 53--63.
- INCOSE - International Council on Systems Engineering. 2021. *Systems Engineering*. Accessed Mar 28, 2021. <https://www.incose.org/about-systems-engineering/system-and-se-definition/systems-engineering-definition>.
- INCOSE. 2021. "A World in Motion Systems Engineering Vision 2025." *INCOSE*. 2014. Accessed Apr 23, 2021. <https://www.incose.org/docs/default-source/aboutse/se-vision-2025.pdf>.
- Institute, Identity Management. 2021. *Access Control Types and Models*. Apr 18. Accessed Apr 18, 2021. <https://www.identitymanagementinstitute.org/access-control-types-and-models/>.
- JAIC. 2020. "Medical Artificial Intelligence." *Health.Mil*. 05. Accessed 05 02, 2021. <https://www.health.mil/Reference-Center/Presentations/2020/05/18/JAIC-Medical-Artificial-Intelligence>.
- Jamsdhidi, Mohammad. 2009. *Systems of Systems Engineering - Innovations for the 21st Century*. Hoboken, NJ: Wiley.
- Johnson, Bonnie , and William A Treadway. 2019. "Artificial Intelligence — An Enabler of Naval Tactical Decision Superiority." *AI Magazine*, March 28: 63–78.
- Johnson, Bonnie. 2021 "Artificial Intelligence Systems: Unique Challenges for Defense Applications." *18th Annual Acquisition Research Symposium*. Monterey: Monterey: Acquisition Research Program.
- . 2020. "Predictive Analytics in the Naval Maritime Domain." *Deep Models and Artificial Intelligence for Defense Applications: Potentials, Theories, Practices, Tools, and Risks 2020*. Virtual: AAAI. 69–77.
- Johnson, Bonnie, and John M Green. 2019. *Advanced Concepts and Applications for Predictive Analytics in the Maritime Domain*. Poster, Monterey, California. Naval Postgraduate School: Calhoun Home.
- Lee, Connie. 2020. *National Defense*. 10 16. Accessed 05 03, 2021. <https://www.nationaldefensemagazine.org/articles/2020/10/16/navy-coast-guard-onboarding-artificial-intelligence-tech>.

- Lei, Bao. 2020. "The Data Visualization of Large Scale AIS Trajectories Data on Hadoop." *IEEE Xplore* 1–4.
- Maier, Mark W. 2009. *The Art of Systems Architecting*. Third Edition. Boca Raton, FL: CRC Press.
- Marcus, Gary. 2020. "The Next Decade in AI: Four Steps Toward Robust Artificial Intelligence." Feb 17. Accessed Apr 18, 2021. <https://arxiv.org/ftp/arxiv/papers/2002/2002.06177.pdf>.
- Merriam-Webster Dictionary. 2021. *metadata*. Apr 30. Accessed May 4, 2021. <https://www.merriam-webster.com/dictionary/metadata>.
- Mitchell, Melanie . 2019. *Artificial Intelligence: A Guide for Thinking Humans*. New York: Farrar, Straus and Giroux.
- Norvig, Peter, and Stuart Russell. 2021. *Artificial Intelligence*. Hoboken: Pearson Education Inc.
- Office of Naval Research. 2021. *Artificial Intelligence/Machine Learning for Photonics, Power & Energy, Atmospheric, and Quantum Science*. Accessed 05 01, 2021. <https://www.onr.navy.mil/en/Science-Technology/Departments/Code-33/All-Programs/333-weapons-and-payloads/artificial-intelligence-machine-learning>.
- Operations, Chief of Naval. 2020. "Memorandum Project Overmatch." Project Overmatch. Washington, DC: Department of Navy Chief of Naval Operations, Oct 1.
- Oxstrand, Johanna, and Katya Blanc. 2014. *Effects of Levels of Automation for Advanced Small Modular Reactors: Impacts on Performance, Workload, and Situation Awareness*. July 1. Accessed February 11, 2021. <https://doi.org/10.2172/1164865>.
- Paul, Celeste Lyn, Leslie M Blaha, Corey K Fallon, Cleotilde Gonzalez, and Robert S Gutzwiller. 2019. "Opportunities and Challenges for Human-Machine Teaming in Cybersecurity Operations." *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 442–46.
- Ping Xue, Stephen Poteet, and Anne Kao. 2012. *Information Extraction Using Controlled English to Support Knowledge-Sharing*. Fairfax, VA: Presented at the 17th International Command and Control Research and Technology Symposium (ICCRTS), 1–17.
- Pomerantz, Jeffrey. 2015. *Metadata*. Cambridge, MA: MIT Press.

- Porche III, Isaac R., Shawn McKay, Megan McKernan, Robert W. Button, Bob Murphy, Kate Giglio, and Elliot Axelband. 2012. *Rapid Acquisition and Fielding for Information Assurance and Cyber Security in the Navy*. Santa Monica: RAND Corporation.
- Raz, Ali K, Barclay Brown, Tom McDermott, Bonnie Johnson, Ramakrishnan Raman, Tom Shortell, Rael Kopace, Erika Palmer, Laura Freeman, and Kevin Robinson. 2021. “Artificial Intelligence – Systems Engineering Primer Workshop.” *INCOSE IW 2021*. January 31.
- Rowley, Jennifer. 2007. *The wisdom hierarchy: representations of the DIKW hierarchy*. University of Wales, Bangor, UK: Journal of Information Science 33 (2) 2007, 163–180.
- Sayler, Kelley M. 2020. *Artificial Intelligence and National Security*. Congressional Research Service.
- Shen, Stephanie. 2019. *7 Steps to Ensure and Sustain Data Quality*. Jul 28. Accessed Apr 18, 2021. <https://towardsdatascience.com/7-steps-to-ensure-and-sustain-data-quality-3c0040591366>.
- Targowski, Andrew. 2013. *Harnessing the Power of Wisdom, From Data to Wisdom*. New York: Nova Science Publishers, Inc.
- The United States Naval Research Laboratory. 2021. *Navy Center for Applied Research in Artificial Intelligence (NCARAI)*. Accessed 05 01, 2021. <https://www.nrl.navy.mil/itd/aic/>.
- Weibel, Stuart L. 2009. “A Personal History of the Dublin Core Metadata.” *The Dublin Core™ Metadata Initiative*. Accessed Apr 24, 2021. <https://www.oclc.org/content/dam/research/publications/library/2009/weibel-elis.pdf>.
- . 2021. *Systems Engineering*. Feb 13. Accessed Mar 28, 2021. https://en.wikipedia.org/wiki/Systems_engineering.
- Zhao, Ying, and Gabe E Mata. 2020. “Leverage Artificial Intelligence to Learn, Optimize, and Win (LAILOW) for the Marine Maintenance and Supply Complex System.” *International Conference on Advances in Social Network Analysis and Mining, ASONAM*. The Hague, Netherlands: IEEE. 678–684.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California