



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**ARTIFICIAL INTELLIGENCE (AI) STRATEGY AND
DESIGN FOR MARINE CORPS INTELLIGENCE**

by

Christopher A. Rodney and Yusef Akbarut

June 2019

Thesis Advisor:
Co-Advisor:
Second Reader:

Dan C. Boger
Scot A. Miller
Glenn R. Cook

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 2019	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE ARTIFICIAL INTELLIGENCE (AI) STRATEGY AND DESIGN FOR MARINE CORPS INTELLIGENCE			5. FUNDING NUMBERS	
6. AUTHOR(S) Christopher A. Rodney and Yusef Akbarut				
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) Within the past 15 years, artificial intelligence (AI) has represented a rapidly expanding field that will intrinsically overhaul analytical processes. Historically human-centric processes and capabilities are quickly being overrun by expanding data collection, creating a gap that AI tools can fill. The use of AI applications that have benefited commercial industry provide similar opportunities to add value within the military domain. The Marine Corps is heavily invested in expanding its collection capabilities across the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE). The MCISRE 2015–2020 plan directs a modernization of intelligence, surveillance, and reconnaissance assets across all intelligence disciplines. As collection capabilities expand, analytical tools that process and exploit information must evolve in a similar fashion. In order to expand its analytical abilities, Marine Corps intelligence must establish a strategy that identifies how to approach integrating AI capabilities. This thesis leverages current AI technological capabilities and proposes a strategy to integrate them across MCISRE. The strategy will provide a holistic outlook across the Doctrine, Organization, Training, Materiel, Leadership/Education, Policy, and Facilities (DOTMLPF) spectrum to provide recommendations for senior leadership on material and non-material solutions to support AI integration within MCISRE.				
14. SUBJECT TERMS intelligence, automation, policy, artificial, machine learning			15. NUMBER OF PAGES 131	
			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.

**ARTIFICIAL INTELLIGENCE (AI) STRATEGY AND DESIGN FOR MARINE
CORPS INTELLIGENCE**

Submitted in partial fulfillment of the
requirements for the degrees of

**MASTER OF SCIENCE IN INFORMATION WARFARE
SYSTEMS ENGINEERING**

Yusef Akbarut
Captain, United States Marine Corps
BS, University of California – Los Angeles, 2012

and

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

Christopher A. Rodney
Major, United States Marine Corps
BS, Virginia Tech, 2006
MBA, Averett University, 2013

from the

**NAVAL POSTGRADUATE SCHOOL
June 2019**

Approved by: Dan C. Boger
Advisor

Scot A. Miller
Co-Advisor

Glenn R. Cook
Second Reader

Dan C. Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Within the past 15 years, artificial intelligence (AI) has represented a rapidly expanding field that will intrinsically overhaul analytical processes. Historically human-centric processes and capabilities are quickly being overrun by expanding data collection, creating a gap that AI tools can fill. The use of AI applications that have benefited commercial industry provide similar opportunities to add value within the military domain. The Marine Corps is heavily invested in expanding its collection capabilities across the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE). The MCISRE 2015–2020 plan directs a modernization of intelligence, surveillance, and reconnaissance assets across all intelligence disciplines. As collection capabilities expand, analytical tools that process and exploit information must evolve in a similar fashion. In order to expand its analytical abilities, Marine Corps intelligence must establish a strategy that identifies how to approach integrating AI capabilities. This thesis leverages current AI technological capabilities and proposes a strategy to integrate them across MCISRE. The strategy will provide a holistic outlook across the Doctrine, Organization, Training, Materiel, Leadership/Education, Policy, and Facilities (DOTMLPF) spectrum to provide recommendations for senior leadership on material and non-material solutions to support AI integration within MCISRE.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION AND OVERVIEW	1
A.	INTRODUCTION.....	1
B.	PROBLEM STATEMENT	1
C.	PURPOSE STATEMENT	2
D.	RESEARCH QUESTIONS.....	3
E.	POTENTIAL BENEFITS, LIMITATION, AND ASSUMPTIONS.....	3
F.	THESIS LAYOUT	4
II.	LITERATURE REVIEW	5
A.	CHAPTER OVERVIEW	5
B.	THE MARINE CORPS INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ENTERPRISE.....	5
	1. The Path to Enterprise	6
	2. Enterprise Design.....	6
	3. Enterprise Execution	9
C.	ENTERPRISE ARCHITECTURE APPROACH TO BIG DATA	11
	1. Defining Big Data	11
	2. The Importance of Enterprise Architecture.....	11
	3. Enterprise Architecture.....	12
D.	CURRENT INTELLIGENCE ANALYTICS TACTICS, TECHNIQUES AND PROCEDURES.....	13
	1. Intelligence Objectives.....	13
	2. Principles of Intelligence Operations	14
	3. Developing Intelligence.....	15
	4. Production and Analysis	17
E.	ACTIVITY BASED INTELLIGENCE	19
F.	CAPABILITIES THAT ENABLE ARTIFICIAL INTELLIGENCE.....	25
	1. Machine Learning and Artificial Intelligence Overview.....	25
	2. Data Ingest.....	29
	3. Data Storage	33
	4. Data Discoverability.....	37
	5. Data Processing and Exploitation.....	37
	6. Data Dissemination	39
G.	CHAPTER SUMMARY.....	41

III.	METHODOLOGY	43
A.	CHAPTER OVERVIEW	43
B.	RESEARCH PURPOSE.....	43
C.	METHODOLOGY	43
D.	DOTMPLF-P APPROACH	45
E.	CHAPTER SUMMARY.....	46
IV.	RESULTS OF ANALYSIS.....	49
A.	CHAPTER OVERVIEW	49
B.	DOCTRINE	49
	1. Update MCWP 2-10, Intelligence Operations.....	50
	2. Update MCTP 2-10A, MAGTF Intelligence Collection	52
	3. Update MCTP 2-10B, MAGTF Intelligence Production and Analysis.....	53
C.	ORGANIZATION	53
	1. Update the MCISRE Enterprise Architecture to Better Address AI Standards.....	53
	2. Establish an AI Community of Practice	55
D.	TRAINING	57
	1. Establish Training to Support Human-Machine Teaming	57
	2. Develop Training to Better Support Data Annotation	58
E.	MATERIEL	60
	1. Establish an Artificial Intelligence Program of Record	60
	2. Employ an Agile Development Process for AI Capabilities.....	61
	3. Develop an AI Information Systems Initial Capabilities Document	63
	4. Establish Open Architecture to Expedite AI Integration	64
	5. Shift Processing, Exploitation, and Dissemination to Point of Collection	67
	6. Develop and Employ Systems that Provide Explainable AI	69
	7. Develop Cross Domain Solutions.....	71
F.	LEADERSHIP AND EDUCATION	72
	1. Joint Approach to AI Integration.....	72
G.	PERSONNEL	73
	1. Evaluate the Task Organization of Intelligence Units across MCISRE	74
	2. Create Structure to Support Data Management across the Marine Corps	75
H.	FACILITIES	78
I.	POLICY	78

1.	Develop a Cloud Strategy in Coordination with JAIC.....	79
2.	Employ Edge Computing in Concert with Cloud Computing	82
3.	Develop a Data Storage Plan.....	83
4.	Develop Policy to Implement Enterprise Wide Cross Domain Solutions	85
J.	CHAPTER SUMMARY.....	86
V.	CONCLUSIONS AND RECOMMENDATIONS.....	87
A.	RESEARCH CONCLUSIONS.....	88
1.	Make Data the Central Focus through Development of a Data Strategy	88
2.	Approach AI Integration in a Joint Manner	89
3.	Institutionalize AI across MCISRE.....	89
4.	Requirements and Acquisition must Support the Pace of Emerging Capabilities	90
5.	Plan to Operate AI in Communications Degraded Environments	91
6.	Overcome Friction to Gain Acceptance of New Technology	92
B.	RECOMMENDATIONS FOR FUTURE RESEARCH.....	93
1.	Full DOTMLPF-P Analysis by CD&I.....	93
2.	Reduction of Manpower T/O	93
3.	Further examination of AI human-machine teaming.....	93
4.	Examination of training requirements to support AI integration.....	94
	APPENDIX: CONSOLIDATED DOTMLPF-P RECOMMENDATIONS	95
	LIST OF REFERENCES.....	101
	INITIAL DISTRIBUTION LIST	111

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	The five design elements of MCISRE. Source: MCISRE (2014).	7
Figure 2.	MCISRE governance framework. Source: MCISRE (2014).	10
Figure 3.	EA Approach: The Six Core Elements. Source: Bernard (2012).	12
Figure 4.	USMC Intelligence Cycle. Source: MCWP 2-10 (2016).	16
Figure 5.	The Information Hierarchy. Source: MCWP 2-10 (2016).	16
Figure 6.	Intelligence Development and the Intelligence Cycle. Source: MCWP 2-10 (2016).	17
Figure 7.	Intelligence Collection Growth and Development. Source: Conklin (2010).	20
Figure 8.	Traditional and Current PCPAD Intelligence Process. Source: Atwood (2015).	23
Figure 9.	How ABI Transforms the Traditional Intelligence Process. Source: Atwood (2015).	23
Figure 10.	Next Gen Stats AI. Source: Amazon (2018).	26
Figure 11.	Deep Learning vs. Machine Learning vs. Artificial Intelligence. Source: Dhande (2017).	27
Figure 12.	Four Approaches to Machine Learning. Source: Fumo (2017).	29
Figure 13.	The Five V's of Big Data. Source: Ramadan (2017).	30
Figure 14.	Timeline of Hard Drive Cost (USD) Per Gigabyte. Source: Komorowski (2014).	31
Figure 15.	Ontological Approach to Healthcare Data. Source: Pedersen et al. (2012).	34
Figure 16.	Ontology Construction Methodology. Source: Boury-Brisset (2004).	36
Figure 17.	JDL Model. Source: Llinas et al. (2004).	39
Figure 18.	Edge Computing Overview. Source: Rahmani et al. (2018).	40
Figure 19.	Updated Intelligence Cycle. Adapted from MCWP 2-10 (2016).	51

Figure 20.	Four Waves of Artificial Intelligence. Source: Lee (2018).	62
Figure 21.	Traditional Development Approach. Adapted from Pace (2019).	65
Figure 22.	FACE OA Development Approach. Source: Pace (2019).	65
Figure 23.	MCISRE Concept Graphic. Source: “DCGS-MC Sharing Information to the Tactical Edge” (2015).	66
Figure 24.	Technology Acceptance Model. Source: Lai (2017).	69
Figure 25.	Traditional AI vs. Explainable AI. Source: Gunning (2019).	71
Figure 26.	Data Scientist vs. Data Engineer. Source: Willems (2017).	76
Figure 27.	Cloud Computing Delivery Models. Source: Watts (2017).	80
Figure 28.	MCISRE AI Core Themes	87

LIST OF ACRONYMS AND ABBREVIATIONS

ABI	activity based intelligence
AI	artificial intelligence
ATG	analytical tradecraft group
CBA	capabilities based assessment
CD&I	Combat Development and Integration
CDD	capabilities development document
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COA	course of action
CONUS	continental United States
CoP	communities of practice
CPD	capabilities production document
DARPA	Defense Advanced Research Projects Agency
DC CD&I	Deputy Commandant for Combat Development and Integration
DC I	Deputy Commandant for Information
DCGS	Distributed Common Ground System
DCGS-MC	distributed common ground system Marine Corps
DCR	DOTMLPF-P change request
DDoS	Distributed Denial of Service
DIB	DCGS Integrated Backbone
DISA	Defense Information Systems Agency
DL	deep learning
DoD	Department of Defense
DODIN	Department of Defense information network
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
EA	enterprise architecture
ESC	executive steering committee
FYDP	future years defense program
G-2	division/regiment level intelligence section

GEOINT	geospatial intelligence
HQMC	Headquarters Marine Corps
HQMC-I	Headquarters Marine Corps Intelligence Department
HUMINT	human intelligence
I&W	indications and warnings
IaaS	infrastructure as a service
IAS	intelligence analysis system
IC	intelligence community
ICD	initial capabilities document
IEEE	Institute of Electrical and Electronics Engineers
IID	Intelligence Integration Division
IMINT	imagery intelligence
INT	intelligence discipline
IOC	initial operational capability
IoT	internet of things
IPB	intelligence preparation of the Battlespace
IR	intelligence requirements
ISR	intelligence, surveillance, and reconnaissance
JAIC	joint artificial intelligence center
JCIDS	Joint Capabilities Integration and Development System
JROC	Joint Requirements Oversight Council
KB	knowledge base
M&RA	Marine and Reserve Affairs
MAGTF	Marine Air-Ground Task Force
MCDP	Marine Corps doctrinal publication
MCIA	Marine Corps Intelligence Activity
MCIS	Marine Corps Intelligence Schools
MCISRE	Marine Corps intelligence, surveillance, and reconnaissance enterprise
MCTP	Marine Corps tactical publication
MCWP	Marine Corps warfighting publication

MEF	Marine Expeditionary Force
MET	mission essential task
MEU	Marine Expeditionary Unit
MIC	Marine Air-Ground Task Force Intelligence Center
ML	machine learning
MOS	military occupational specialty
NLP	natural language processing
NTC	Naval Tactical Cloud
OA	open architecture
OAG	operational advisory group
P&A	production and analysis
PaaS	platform as a service
PED	processing, exploitation, and dissemination
PIR	priority intelligence requirement
PoR	program of record
RDT&E	research, development, test, and evaluation
S-2	battalion level intelligence section
SA	situational awareness
SaaS	software as a service
SCI	sensitive compartmentalized information
SIGINT	signals intelligence
SPOTR	surveillance, persistent observation, and target recognition
SYSCOM	systems command
T/O	task organization
TOECR	table of organization and equipment change request
TTPs	tactics, techniques, and procedures
USMC	United States Marine Corps
XAI	explainable artificial intelligence

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express our deepest appreciation for the guidance, encouragement, and support from our thesis advisors, Dr. Dan Boger and CAPT Scot Miller (Ret). Without your mentorship, this thesis would not have been possible.

We are highly indebted to Cheryldee Huddleston and Kate Egerton for their devoted support and patience in coaching us while providing tireless review and editing of our thesis. You both made a lasting impact on our writing abilities, and for that we are forever grateful.

Last but not least, we would like to thank our families. To our parents who always placed a heavy emphasis on the importance of education and pushed us to excel in all that we do. And to our beloved wives, Jess and Noha, for your steadfast support and encouragement during this thesis journey. Your constant love and devotion make all things possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND OVERVIEW

A. INTRODUCTION

Artificial Intelligence (AI) is a rapidly expanding field which will intrinsically overhaul analytical processes. Historical human centric processes and capabilities are quickly being overrun by data collection expansion, creating a gap which AI tools provide the capability to fill. To date, much of AI's application has been focused on the commercial industry. Information technology, marketing, accounting, and customer service industries have all benefited from the algorithmic and systems development expansion in AI (Ramaswamy, 2017). The military domain, including the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE), can benefit equally from the commercial industry applications of AI.

The Marine Corps is heavily invested in expanding its intelligence, surveillance, and reconnaissance (ISR) capabilities across the MCISRE. The MCISRE 2015–2020 plan directs a modernization of collection capabilities across all intelligence disciplines (HQMC-I, 2014). As collection capabilities expand, analytical capabilities must co-evolve in a similar fashion to prevent a gap between collection and exploitation. In order to expand its analytical abilities, Marine Corps intelligence must establish a strategy which identifies how to approach integration of AI capabilities.

This thesis will explore current AI technological capabilities and propose a strategy to leverage them for application to MCISRE. The strategy will provide a holistic outlook across the Doctrine, Organization, Training, Materiel, Leadership/Education, Personnel, Facilities, and Policy (DOTMLPF-P) spectrum to provide recommendations for senior leadership on material and non-material solutions to support AI integration within the intelligence enterprise.

B. PROBLEM STATEMENT

On September 14, 2012, fifteen Taliban insurgents breached the eastern perimeter of Camp Bastion (Garrett, 2013). By the time the threat was eliminated, two U.S. service members were dead, eight were injured, and over a dozen aircraft were either destroyed or

damaged (Garrett 2013). The subsequent investigation provided causal factors which included improper security manning, unobserved terrain, lack of defense in depth, lack of patrolling, and lack of local airfield security (Garrett 2013). All of these factors tie into improper friendly course of action (COA) development. Other contributing factors listed in the report included an underestimation of the enemy through a faulty threat assessment and failing to consider all possible enemy COAs. AI tools exist that can be applied in the military domain to better enable friendly COA decision making and provide better predictive analysis of enemy capabilities and intentions. If military leadership at Camp Bastion were equipped with AI capabilities, they may have been more prepared for the attack and prevented the enormous loss of life and aircraft.

AI capabilities have expanded at a rapid rate over the past 15 years. The growth in capabilities corresponds to a 14 times expansion of AI startup companies during the same period (Shoham et al., 2017). Despite this growth, the Marine Corps has failed to capitalize and fully incorporate AI across the MCISRE. By not incorporating such a critical capability, failure to adapt AI techniques is negatively impacting the Marine Corps' intelligence warfighting function by degrading analytical capabilities. Data collection is expanding at an exponential rate, with 90% of the current global data ever produced in the history of mankind collected over the past two years (Savitz, 2013). As data collection continues to expand, the analytical degradation in the Marine Corps will grow immense, creating a gap between collection and analysts' ability to process and exploit it. A lack of formalized strategy to integrate AI across the MCISRE contributes to this problem. A qualitative study, investigating DOTMLPF-P considerations for AI integration, can assist in the development of a cohesive strategy, which will assist in solving this issue.

C. PURPOSE STATEMENT

The purpose of this research is to evaluate and juxtapose commercial and Department of Defense (DoD) AI capabilities and software against the Marine Corps analytical toolset in order to identify potential capabilities and methods for integration. This identification and subsequent recommendations are aimed at expanding the analytical tradecraft of intelligence analysts to close an expanding capability gap between collection

and exploitation of big data in the Marine Corps. DOTMLPF-P recommendations integrated into an AI strategy for the MCISRE represents the end result. The research will identify and consider:

- Marine Corps analytical tools and tactics, techniques, and procedures (TTPs)
- AI enabling capabilities
- Commercially available AI capabilities
- Differences in analytical requirements for military application of AI
- DOTMLPF-P analysis to determine requirements for integration of AI

D. RESEARCH QUESTIONS

1. How can the Marine Corps Intelligence Surveillance, and Reconnaissance Enterprise (MCISRE) incorporate already developed commercial AI software and hardware capabilities into its systems architecture to increase analytical abilities across the Enterprise?

2. Given emerging capabilities in commercial AI, what adjustments to software and/or concepts of employment are required to ensure they support military analytical requirements?

3. What are the DOTMLPF-P considerations and implications of incorporating AI into Marine Corps intelligence?

4. What technical options should the Marine Corps pursue based on this strategy?

E. POTENTIAL BENEFITS, LIMITATION, AND ASSUMPTIONS

The research conducted provides an opportunity for the Marine Corps to identify advantages and risks of AI application into its military intelligence toolset. The deliverable will be an AI strategy which will inform future programs of record at Deputy Commandant for Combat Development and Integration (DC CD&I) and policies from Headquarters Marine Corps Intelligence Department (HQMC-I). Since emerging commercial AI capabilities do not currently exist as programs of record, the study will be limited to

literature and commercial AI field research and utilize deductive reasoning to reach recommendations for the strategy. An assumption for this strategy is that the MCISRE will not solve any challenges with additional manpower, and all proposed AI solutions must account for that constraint. This assumption is based upon recent trends in Marine Corps force structure.

F. THESIS LAYOUT

Chapter II is the literature review which examines scholarly work in the field of AI and contextualizes key knowledge concepts required for AI implementation across MCISRE. Chapter II will be split with the first half focusing on how intelligence is currently conducted by examining tactics, techniques, and procedures (TTPs). The second half will focus on AI enabling capabilities across each phase of the intelligence cycle. Chapter III explains the methodology used to extrapolate the identified AI enabling capabilities in conjunction with field research to develop recommendations that form the basis of the AI integration strategy. Chapter IV is the presentation of key DOTMLPF-P considerations. Chapter V presents conclusions and recommendations for future research.

II. LITERATURE REVIEW

A. CHAPTER OVERVIEW

This chapter provides a comprehensive review of the scholarly literature relevant to the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE) and the Artificial Intelligence (AI) field. The first half of this chapter outlines the key components and structure of MCISRE. It also reviews relevant literature on tactics, techniques, and procedures for how the Marine Corps currently conducts its intelligence warfighting function within the enterprise. The second half of this chapter investigates literature on required capabilities to enable AI integration and execution. The capabilities investigated will be synthesized and applied to MCISRE in Chapter IV. A foundational principle of MCISRE is adapting and implementing new technologies that will provide greater efficiencies and effectiveness. The goal of this thesis is to improve MCISRE through strategic implementation and integration of AI capabilities – a natural progression for MCISRE to take.

B. THE MARINE CORPS INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ENTERPRISE

After over ten years of combat operations in Iraq and Afghanistan, the Department of Defense (DoD), as a whole, was seeking to continue to evolve its military function in order to meet the needs of the ever-changing battlespace in the future fight. Operations Enduring Freedom (OEF) and Iraqi Freedom (OIF) demonstrated the nation's adversaries' ability to overcome, adapt, and align their capabilities against the United States. This evolution sought to undermine and compete with battlespace dominance the U.S. had become accustomed to. With the rapid development and implementation of technology into armed conflict, and the consistent and ever growing nature of the information age, the battlefield evolved into a significantly more complex environment than previously experienced. The concept of MCISRE was created in order to ensure the Marine Corps' intelligence warfighting function continued to develop and transform into an Enterprise that constantly reinforces itself and excels in all future and dynamic conflicts:

The Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE) Plan articulates and implements the Director of Intelligence's vision for designing and developing MCISRE. As the Annex B to the Marine Corps Service Campaign Plan (MCSCP), it describes how MCISRE plans and executes the intelligence warfighting function across all echelons of the Service, the Intelligence Community, and the Joint Force. It provides the framework and Service-level direction for continued development of an all-source Intelligence, Surveillance, and Reconnaissance Enterprise to meet the specified and implied tasks identified in the Marine Corps Service Campaign Plan and the subordinate Campaign Support Plan. Together with associated appendices, MCISRE Plan implements the principles of Expeditionary Force 21, the Marine Corps' capstone concept for America's Force-in-Readiness, providing the right intelligence at the right place and the right time. (MCISRE, 2014)

1. The Path to Enterprise

At the core of MCISRE is what it consists of and what it can provide. MCISRE, first and foremost, is made up of Marines. Composed of professional intelligence Marines, the Enterprise serves to perform Intelligence, Surveillance, and Reconnaissance (ISR): "conducting reconnaissance to discover threats or opportunities in the battlespace, conducting surveillance to monitor activities that impact its missions, and turning information into intelligence that helps leaders make timely and accurate decisions" (MCISRE, 2014). A core component in providing a high level of support to the vital ISR functions is the Enterprise's ability to connect every facet of the intelligence community, both internally and externally, to create synergy and better perform its warfighting function. This synergy is created through an Enterprise design.

2. Enterprise Design

From a macro view, MCISRE is designed to integrate intelligence with all other warfighting functions: Command and Control, Maneuver, Fires, Logistics, and Force Protection. Effective and valuable intelligence is the backbone for a Commander's decision making and his ability to decisively win in combat. Integrating intelligence with all other warfighting functions and continually pushing to improve the Enterprise is crucial to not only MCISRE, but success for the entire Marine Corps. From a micro view, the Enterprise is designed to link all of the Marine Corps' disparate ISR nodes into a mutually supporting

whole: “it links these capabilities through professionalism, operational integration, carefully engineered processes, and data interoperability” (MCISRE, 2014). The Enterprise also links intelligence Marines to external resources including joint services, DoD, the broader intelligence community (IC), and select foreign partners. To support the macro and micro viewpoints, MCISRE design is broken down into five elements as shown in Figure 1: Operational Design, Functional Design, Process Design, Partnership Design, and Professional Design.

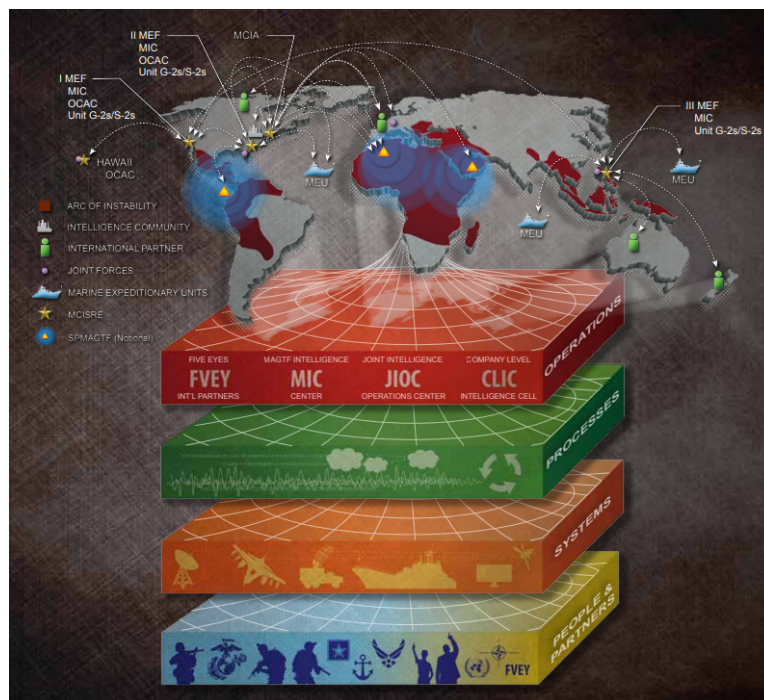


Figure 1. The five design elements of MCISRE. Source: MCISRE (2014).

Operational Design – Through its operational design, MCISRE presents how the Marine Corps’ intelligence apparatus functions and serves its warfighting purpose. This begins with the tactical level intelligence sections of unit S-2s and G-2s from Battalions and Squadrons and feeds up to the three Marine Expeditionary Forces (MEFs) located in Okinawa, Japan, Camp Lejeune, NC, and Camp Pendleton, CA. How these sections both receive support and conduct the requisite intelligence needed for Commanders to make

decisions are the foundation for the Enterprise. The Marine Corps has a Marine Air-Ground Task Force (MAGTF) Intelligence Center (MIC) at each MEF. By staying connected to the broader IC, these MICs provide all-source global intelligence analysis to provide situational awareness and reach back support for their deploying units. Additionally, the Marine Corps Intelligence Activity (MCIA), based in Quantico, Virginia, functions “as the Enterprise ‘fixed site’ to support enterprise operations, specialized skills, functional capacity, collections, analysis, and production support across the Marine Corps” (MCISRE, 2014). These dedicated and persistent intelligence organizations allow the Enterprise to ensure the Marine Corps’ tactical units are fully supported with the most innovative and cutting-edge intelligence needed to be successful in any mission set.

Functional Design – The functional design of the Enterprise aims to renovate and integrate its tools, systems, organizations, and interfaces. After a decade-plus of combat operations, the Marine Corps has compiled various systems and equipment sets that have been useful for their individual purpose, but have lacked an integrated capability across the board. The Enterprise seeks to address this by reevaluating current systems and bolstering “bottom-up operating force innovation that will drive an architecture to meet both garrison requirements and wartime demands” (MCISRE, 2014). Continuous development in its collections and data architectures will provide the Enterprise with modernized infrastructure and systems that will allow Marines to generate intelligence faster, better supporting deploying MAGTFs, the Joint Force, and the IC.

Process Design – Process design within MCISRE is the refinement of how information is accessed and conveyed to Marines across the MAGTF, as well as the renovation and codification of intelligence procedures to improve efficiency. Similar to how disjointed systems are addressed in functional design, historical data and stored information across the Marine Corps is vastly disconnected and there is no singular housing of all information that can be easily accessed. “MCISRE plan seeks a broadly open architecture that enables universal data visibility, smart searching, and ready display” (MCISRE, 2014). The MCISRE Plan (2014) states that the open architecture is a critical component to the development of solutions that support data fusion, analytics and analysis in support of real time decision making. Within process design of the MCISRE plan, there

is significant opportunity for AI and machine learning (ML) to advance Marine Corps intelligence processes. Adding AI capabilities will not only considerably improve the Enterprise and its effectiveness but will also be a requirement for the intelligence warfighting organization to maintain a decisive edge needed to win in future combat operations.

Partnership Design – “MCISRE partnership design expands relationships with foreign and domestic partners, increases linkages to the Joint Force, and expands access to the broader IC” (MCISRE, 2014). Always leveraging the support of adjacent units and giving support at every opportunity is the backbone for partnership design in MCISRE. Continually developing relationships and partnerships with sister services and the IC community is crucial to expanding reach and breadth of knowledge as intelligence professionals. This development consists of actively seeking key billets in both the Joint Force and the IC in order to provide them with the technical and tactical expertise of Marine Corps intelligence. Once Marines return from those key billets, they have an expanded knowledge base from which they can strengthen the Enterprise.

Professional Design – Professional Design in MCISRE goes back to its fundamental component: people. Developing Marines and institutionally professionalizing their tradecraft as intelligence professionals is paramount for the Enterprise’s success: “People are the Enterprise. Investments in human capital are the most important investments we make. Through professional design, we guide those human capital investments to the most effective places” (MCISRE, 2014). Recruiting, developing, and retaining highly qualified Marines within the Enterprise and refining their career development to continually push them to progress will be the catalyst for an enduring and innovative Enterprise.

3. Enterprise Execution

The execution of the Enterprise will be supported by governance, as shown in Figure 2, in order to ensure restructure, refinement, and development are always occurring as dictated by the Enterprise design. The foundational tenet of MCISRE governance is the empowerment of its Marines and their continuous efforts to drive change and innovation.

This can be seen through their direct involvement in Communities of Practice (CoP), Analytic Tradecraft Groups (ATGs), and Working Groups (WGs) specifically established to pursue advancement. These groups directly feed into the Operational Advisory Group (OAG) and Executive Steering Committee (ESC) that create policy and approve plans (MCISRE, 2014).

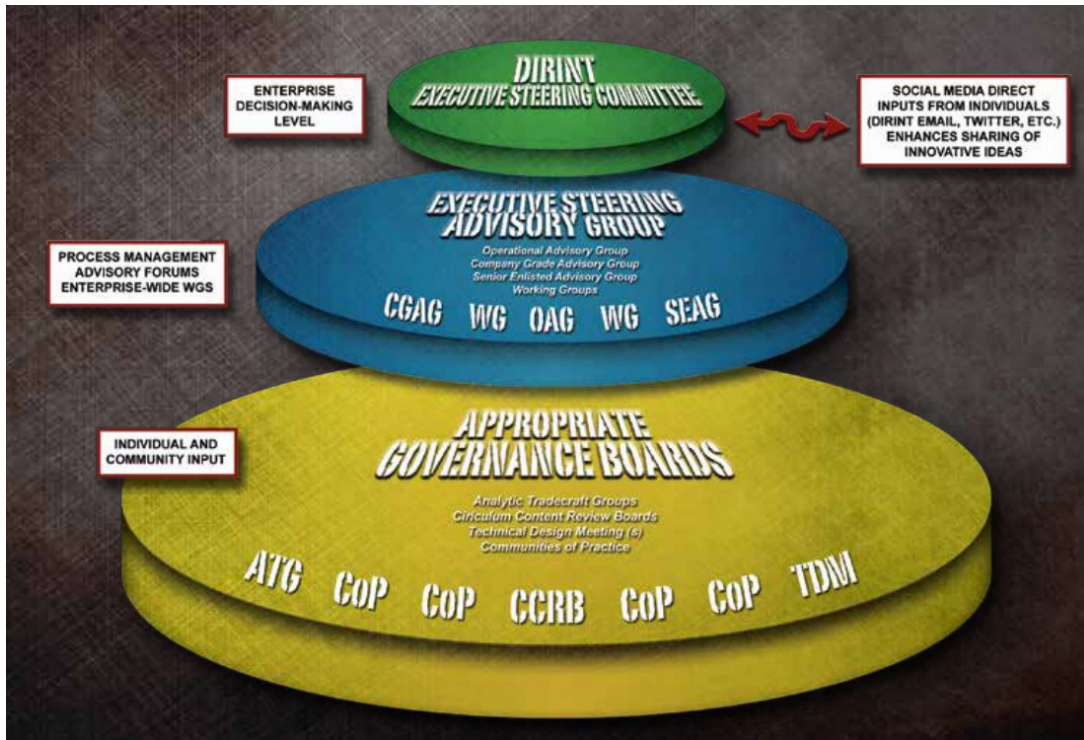


Figure 2. MCISRE governance framework. Source: MCISRE (2014).

At its current stage, ample room exists for AI to make a significant impact on the Enterprise. Adding AI capabilities will lead the Enterprise into the future and make considerable enhancements in its intelligence warfighting effectiveness. Although MCISRE has an established strategy, there are opportunities for improvement in its Enterprise Architecture (EA) to better address the growing issue of big data and enable AI integration. In order to identify the opportunities, it is first important to gain a better understanding of what EA is and how it can support big data and AI integration.

C. ENTERPRISE ARCHITECTURE APPROACH TO BIG DATA

There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system...

– George Orwell, 1984, 1949

George Orwell's fictional 1984, written 70 years ago, is more relevant than ever. With cameras on every corner and in every cell phone, social media capturing real time posts, and intelligence gathering tools and techniques expanding, it seems any expectation of privacy is gone. This explosion of big data collection, while a concern for some, creates a plethora of exploitation opportunities in the IC. Big data will continue to grow exponentially. How the U.S. IC, and more specifically MCISRE, utilizes the data through enterprise architecture, a supporting data strategy, and integration of computer automation with human-in-the-loop will determine whether big data turns into big intelligence.

1. Defining Big Data

The history of the evolution of big data provides a baseline for this study and is important to frame as part of the literature review. In the article "Big Data: The next frontier for innovation, competition, and productivity," big data is defined as "datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze" (McKinsey Global Institute, 2011). The article's definition of big data is open ended and not constrained by size, since volume of data is a moving target that will expand over time. Data collection is growing at an exponential rate with 90 percent of the world's global data ever collected produced within the past two years (Wu, Zhu and Wu, 2014). Therefore, what is considered big data today may not be considered big data in ten years.

2. The Importance of Enterprise Architecture

Exponential growth in big data directly correlates to exponential intelligence collection, processing, and exploitation opportunity, but not necessarily its capability. The biggest challenge for MCISRE is to develop solutions which are capable of supporting decision-making by ingesting large volumes of data and extracting relevant information

(Wu, Zhu and Wu, 2014). MCISRE must grow its capability to store and make data discoverable in order to produce relevant and useful products to assist decision makers. In order to accomplish this, MCISRE must adopt an enterprise architecture (EA) approach.

3. Enterprise Architecture

Enterprise architecture (EA) is the documented analysis of an Enterprise from three perspectives: Strategy, business, and technology (Bernard, 2012). Successful implementation of EA requires continuous engagement at all levels and across all decisions affecting the Enterprise. A shift in strategic guidance has a direct effect on business processes and often times technological decisions. Thus, complete EA approaches have six core elements outlined in Figure 3.

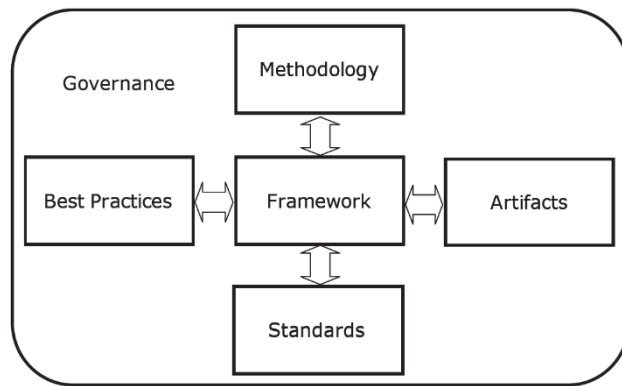


Figure 3. EA Approach: The Six Core Elements. Source: Bernard (2012).

Governance identifies processes for planning and decision making, determining how the EA will be developed and maintained. Methodology indicates how the EA will be implemented. Framework describes the scope of the Architecture and how the sub elements relate to one another. Artifacts are the documentation, including the business plans, workflows, and databases. Standards include technological and business aspects that the Enterprise must capitalize on to successfully implement its architecture. Finally, best practices are proven methods for implementing the chosen EA.

Architecture is often viewed and developed in a siloed nature, resulting in a lack of integration and mutual support which can be detrimental to an organization (Hoogervorst, 2004). Although EA is of vital importance, establishing a successful EA is a difficult task which requires senior leadership sponsorship from beginning to end. EA is not a new concept, and many business executive decision makers dictate a desire for EA to streamline their framework and processes to increase company agility, but few properly approach the problem and dedicate the appropriate resources towards achieving the goal.

D. CURRENT INTELLIGENCE ANALYTICS TACTICS, TECHNIQUES AND PROCEDURES

And therefore I say: Know the enemy, know yourself, your victory will never be endangered. Know the ground, know the weather; your victory will then be total.

– Sun Tzu

The intelligence warfighting function is critical for success in any military operation. Efficient and effective intelligence TTPs are instrumental in creating the decisive edge in maneuver warfare, the heart of Marine Corps warfighting doctrine. This section provides an overview of how the Marine Corps views the intelligence warfighting function, as well as how intelligence processes and operations are conducted in support of it. It will provide a specific focus on the ways the Marine Corps conducts analytics and processes data into relevant intelligence. This focus on analytics and information processing is an area where introduction of AI and Machine Learning (ML) capabilities can deliver a significant impact on effectiveness, efficiency, and innovation.

1. Intelligence Objectives

Intelligence exists to serve two primary objectives. The first objective is reduction of uncertainty by providing situational awareness to commanders through accurate, timely, and relevant intelligence in support of decision making (MCWP 2-10, 2016). MCWP 2-10 (2016) focuses the use of counterintelligence (CI) in support of protecting friendly forces. In the confusion and chaos of war, the commander relies on his intelligence section to provide a cohesive picture of the threat and environment that includes all relevant

information and data in order to reduce uncertainty to a sufficient level. The commander then makes decisions on the basis of the intelligence provided. In order to achieve this, *MCDP 2 Intelligence* identifies four related tasks. The first task is identification and evaluation of enemy capabilities. Using the identified enemy capabilities, the next task estimates possible enemy courses of action (COA). Following estimation of enemy COAs, the third task is to evaluate the friendly side through identification of friendly force vulnerabilities. Lastly, utilizing the output of the first three tasks, intelligence supports the development and wargaming of friendly COAs (MCDP 2, 1997).

2. Principles of Intelligence Operations

In order to achieve the primary intelligence objective and give commanders the decisive edge in combat by enabling maneuver warfare, there are several key principles to conducting intelligence operations. First, the focus is on tactical intelligence: generating intelligence and applying intelligence TTPs to be employed and used at the tactical level. Intelligence is focused downward, meaning that intelligence is always geared towards supporting the commander's decision-making at all levels. Any relevant intelligence is pushed down to the lowest levels in order to ensure maximum understanding of the battlespace and to allow for Marines at all levels to make decisions within the Commander's intent at the decisive edge of combat, a fundamental necessity of maneuver warfare. In short, intelligence drives operations. At the genesis of any operation is a source of intelligence or lack thereof. This concept falls in a continuum from which changes to the battlespace will continue to produce new intelligence, which will then drive future operations.

Furthermore, from an organizational viewpoint, intelligence must be centrally managed through the G-2/S-2 (MCWP 2-10, 2016). These two principles allow for command and control within the intelligence warfighting function. They provide guidance and direction to permit a coordinated and integrated effort amongst all the collection, processing, and analytical resources available, which in turn produces intelligence that can then be disseminated and implemented in the planning and decision-making processes. MCWP 2-10 (2016) directs the necessity for intelligence to be developed in a timely

manner and in a format that meets the requirements of the user. Dissemination of intelligence has to be conducted at the right time and place for it to be beneficial. Finally, “utilization is the final step of the intelligence cycle. Intelligence has no inherent value; its value is derived from its support of decision making. The intelligence cycle is not complete until the intelligence that has been developed is used to plan and/or execute operations” (MCWP 2-10, 2016). These intelligence principles provide the foundation that enables execution of the six fundamental intelligence functions across all levels of the MAGTF.

3. Developing Intelligence

The Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence*, defines intelligence as “knowledge about the enemy or the surrounding environment needed to support decision-making. Since people understand situations best as mental images, intelligence aims to create an accurate or meaningful image of the situation confronting a commander. Good intelligence paints a picture, or more accurately, several pictures, of possible realities” (MCDP 2, 1997). The Marine Corps uses the intelligence cycle, depicted in Figure 4, as a process to support military decision-making by developing intelligence from data and information. There is an abundance of raw data that is available in today’s environment. The first step to deriving intelligence is to process raw data into information that is correlated, formatted and translatable to provide relevance. This information is then analyzed, evaluated and integrated to form a knowledge base from which judgment of the environment and situation will allow an understanding that can be then synthesized and visualized as shown in Figure 5.

This process of transforming raw data into intelligence is used concurrently with the intelligence collection cycle in order to support the commander’s decision-making. The Marine Corps’ intelligence cycle has six steps. First, planning and direction identifies intelligence requirements (IRs) from which intelligence operations and activities are planned. This step supports the formulation of the commander’s estimate and situation. From the initial planning, a collection plan is formed and executed to answer IRs utilizing organic, attached, and supporting intelligence sources. From the collection phase, raw data and information is received that is then processed, exploited and produced into a suitable

form of intelligence. Intelligence is then disseminated in a timely manner to the appropriate levels in order to be utilized and support decision making. The use of intelligence and the subsequent conduct of operations/changes to the battlespace will then lead to further planning and direction within the intelligence cycle (MCWP 2-10, 2016). The combination of the intelligence cycle and information hierarchy support the commander's decision making process as depicted in Figure 6.

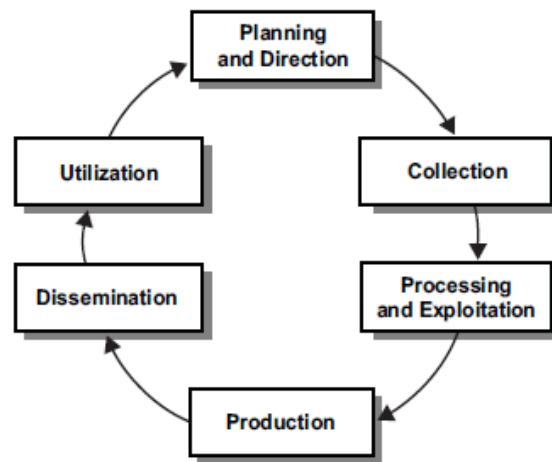


Figure 4. USMC Intelligence Cycle. Source: MCWP 2-10 (2016).

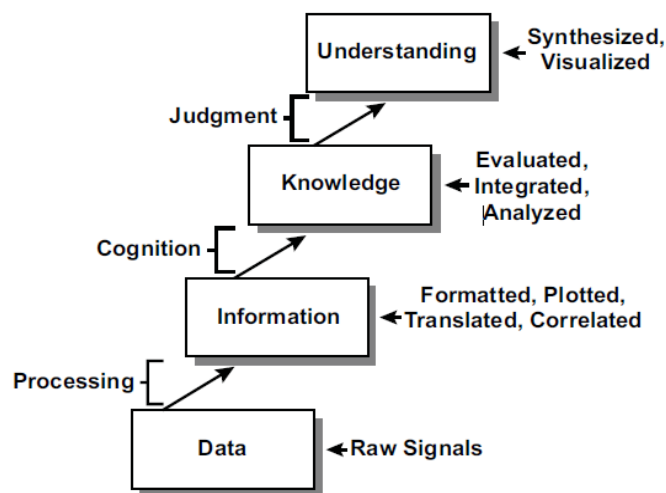


Figure 5. The Information Hierarchy. Source: MCWP 2-10 (2016).

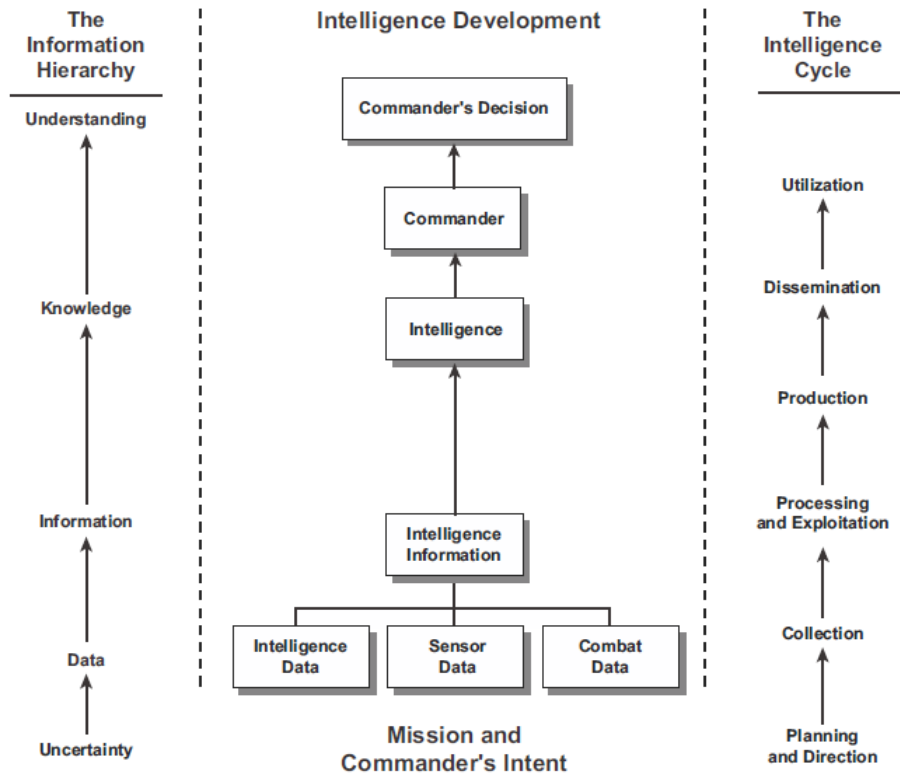


Figure 6. Intelligence Development and the Intelligence Cycle.
Source: MCWP 2-10 (2016).

4. Production and Analysis

At the heart of understanding the threat situation and environment is intelligence production and analysis (P&A). The process of conducting effective intelligence P&A encompasses five steps: filtering, recording, evaluating, analyzing, and product preparation. This section will overview the first four steps and identify potential shortfalls where there are opportunities to adjust current TTPs through the use of AI/ML systems.

Per Marine Corps doctrine, “filtering is the discarding of irrelevant or repetitive information prior to its entering the production process” (MCTP 2-10B, 2016). Filtering out irrelevant and repetitive information is a critical step in preparing information for analysis. The overabundance of data available can overload the intelligence analyst with information if good filtering practices are not observed. Filtering is conducted by the intelligence section leader establishing criteria that allow for an efficient flow of relevant

data/information. This criteria is formed by establishing criteria to discern subject matter that is relevant to the units PIRs/IRs, located within the units Area of Operations (AO) or Area of Influence (AOI), and time of occurrence that is within an appropriate time frame that would provide relevance to making an assessment. All other redundancies of information are discarded to prevent the overflow of information. Continuously updating the established filter criteria is critical to maintaining effective analysis of the threat environment.

The way filtering works in practice is as follows. There is a central node within the intelligence section that receives all data, information, and reports. The analysts at that node filter the data based on the established criteria to pass on relevant information to the intelligence section. However, with the large quantity of data available and being passed through various channels through this node, a single analyst or even a team of analysts can be overloaded and relevant information that may be critical for analysis can easily be overlooked. Currently, intelligence analysts utilize the Intelligence Analysis System (IAS). IAS is a program of record computer that allows analysts to filter through databases of reports (such as HUMINT/SIGINT reporting) based on user-inputted criteria, which provide efficiencies in accessing data. However, these efficiencies are limited due to the fact that analysts manually filter through reports based off their generated queries.

Once filtering has occurred, the next step is recording which is “the reduction of information to writing or graphical representation and then arranging that information into groups of related items” (MCTP 2-10B, 2016). The recording of filtered information allows for an easier evaluation and analysis of that information. Although intelligence journals are typically kept to maintain a log of all incoming information with relevant characteristics, the most common way recording is conducted is a graphical depiction on maps. Effectively recording information allows decision makers to visualize groups of information and better assess the situation holistically. An intelligence analyst will typically use their IAS to create overlays on maps within the computer that provide transparency to the data and permit easy manipulation for evaluation and analysis.

Evaluation of the recorded data is when “the intelligence section determines the relevance, the source reliability, and the accuracy of recorded information. Evaluating

information in this manner also determines whether immediate or deliberate production and dissemination should be performed” (MCTP 2-10B, 2016). Urgent information is disseminated immediately to the appropriate end user, while other relevant information not of an urgent nature is kept for further analysis to help deepen the understanding of the threat picture.

Once data relevance is determined, analysis must occur. Analyzing data is “the process in which information is evaluated and synthesized to predict possible outcomes. Through analysis, information is transformed into knowledge. Understanding is achieved by applying judgment to knowledge, and the future is anticipated by understanding the present” (MCTP 2-10B, 2016). One of the primary examples of how Marine Corps intelligence conducts analysis is through the development of the Intelligence Preparation of the Battlespace (IPB). Given a defined battlespace, established intelligence requirements, understanding of the mission, and commander’s intent, intelligence sections begin to dissect all relevant information available and conduct analysis that yields a reduction of uncertainty and assists the commander with decision-making. This analysis is formulated through the four steps of the IPB: “define the battlespace environment, describe battlespace effects, evaluate the threat, and determine threat courses of action” (MCWP 2-10, 2016). The IPB is typically developed and briefed to the commander and the staff prior to the beginning of major planning. This allows all decision makers to be as cognizant of the threat and environment as possible before devising plans to counter and defeat the threat. The IPB is a living, breathing document that is continuously updated through the conduct of all operations in order to maintain a current complete view of the battlespace and most up-to-date analysis of the situation.

E. ACTIVITY BASED INTELLIGENCE

To effectively implement material AI solutions, Marine Corps intelligence processes must follow suit. As noted above, the intelligence cycle operates in a cyclical, yet linear fashion. Collection occurs at step two, followed by processing and exploitation, then production. In order to better leverage AI, changes to this linear intelligence process may be required. Current methods for intelligence processing, exploitation, and

dissemination (PED) are slow and disjointed and would marginalize the capability provided by the introduction of AI. The intelligence cycle leads to a siloed approach of collection within each discipline, with HUMINT to SIGINT performing a full cycle of collection before synchronization and data integration occurs.

Since the Cold War, intelligence collection has evolved in distinct periods. During the Cold War, the IC collected and exploited stovepipe intelligence. OIF and OEF ushered in a new wave of collection requirements, forcing the IC into the distributed intelligence period. Recently, the IC has entered the most challenging period of integrated intelligence (Conklin 2010). These periods have been dictated by a combination of the nature of the threat and friendly data collection capabilities. Figure 7 shows the growth and development of intelligence collection by period.

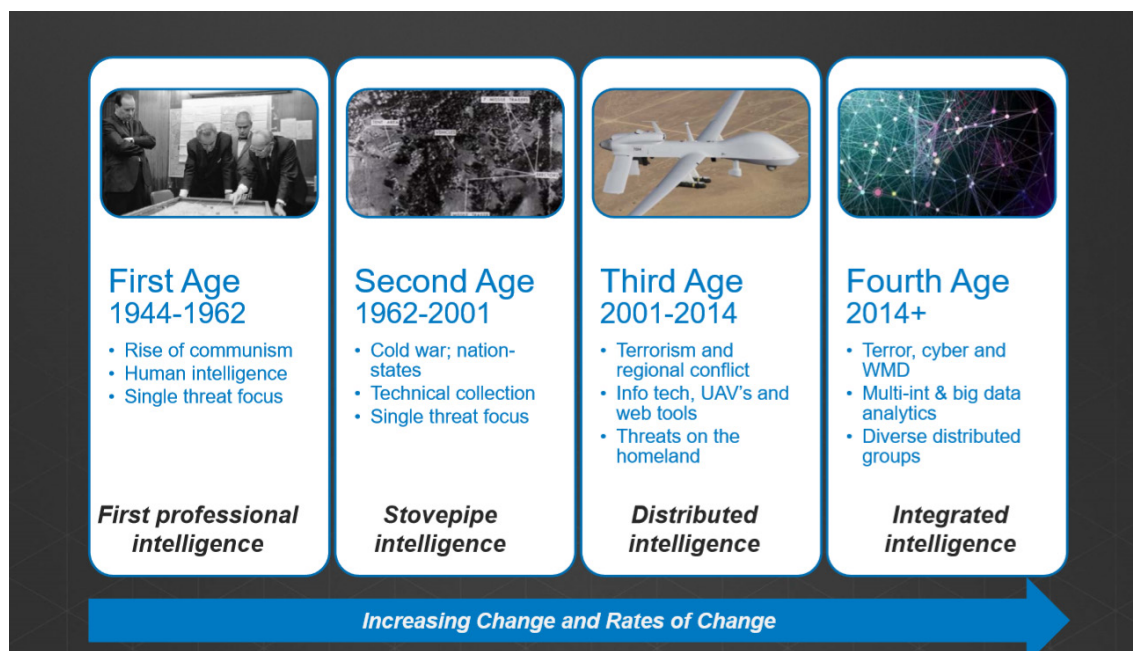


Figure 7. Intelligence Collection Growth and Development. Source: Conklin (2010).

Integrated intelligence is required to combat diverse threat actors with a unique set of collection requirements not encountered with conventional nation-state enemies. Doctrinal collection methodologies, however, were developed to target conventional

adversaries such as Russia or China. During the stovepipe intelligence period of collection, nation-state targets masked their capabilities and made intelligence collection akin to looking for ‘needles in a haystack’ but the haystack was known (Russia and China) and the needles were merely objects – planes, radars, logistical hubs (Long, 2013). OIF and OEF changed the nature of U.S. warfare. Few, if any, nations are now willing to fight the U.S. in a conventional setting. At best, the Nation can expect to fight a hybrid approach to warfare. As the nature of warfare has evolved, so has the level of difficulty in developing and exploiting collection in a timely and relevant manner to enable pre-emptive and decisive action. The needle in the haystack comparison has evolved to a point where neither the needle nor the haystack is immediately discernable. Nation-states have been replaced with individual organizations and even ‘loan wolf’ actors with terms like “irregular” and “asymmetric” warfare becoming the norm (Llinas and Scrofani, 2014). This threat evolution has a corresponding collection requirement challenge. Collection focus has shifted from the physical dimension to the relational. Collecting on the relational is highly dimensional and further exasperating the problem is the fact that individual actors possess significantly reduced collectable signatures (Llinas and Scrofani, 2014). Couple the diverse threat with the exponential increase in big data analysts must sort, and the problem becomes wicked. In the business world, most big data exploitation is handled through analytical tools provided by AI. For intelligence, though, the problem of determining what indicators to seek and what questions to ask remains present. A relatively new intelligence process called Activity Based Intelligence (ABI) provides a supportive approach to resolving these issues and enabling AI.

ABI is “an inherently multi-INT approach to activity and transactional data analysis to resolve unknowns, develop object and network knowledge, and drive collection” (Long, 2013). ABI uses large volumes of data gathered across every intelligence discipline and integrates and identifies correlational attributes instantaneously, replacing traditional intelligence processes where exploitation occurs after the collection phase of the intelligence cycle. One of the core requirements of ABI is the fusion of data across the various disciplines prior to exploitation (Atwood 2015). In other words, integration happens instantaneously while collection is still occurring. This methodology supports

traditional target-centric approaches where the analyst is looking for a specific threat indicator, but it also supports identification of unknowns, or targets the analyst was not originally looking for. Equally as important, fused data from the ABI process provides unknown threat indicators in a timely manner where traditional approaches failed, due to fusion occurring at the conclusion of the multi-INT collection.

Under current collection management and exploitation approaches, collection plans are built with capabilities that queue and provide redundancy. At face value, a collection plan is well constructed with complimentary layers, however, the reality is the exploitation via integration of the multi-source collection is not the norm. While a target may be tasked for collection by HUMINT and IMINT, the synergy achieved by integrating the collection either doesn't come to fruition or happens too late. The 2013 chemical weapons attack in Syria provides a good case study to illustrate this point. In the days leading up to the attack, the Intelligence Community (IC) had multi-INT reporting the Syrian regime was conducting preparations for use of chemical weapons (Atwood, 2015). HUMINT, GEOINT, and SIGINT collection all provided relevant data that, if integrated in a timely manner, would have revealed the intentions of the regime (Atwood, 2015). In this example, the IC properly allocated multi-discipline collection capabilities on the target. Individually, the capabilities performed as expected and produced actionable information. Current stovepipe processes, however, resulted in an inability to fuse the data and provide I&W of the pending attack. Looking at the same problem set from the ABI approach, the collection of HUMINT, GEOINT, and SIGINT would have been fused earlier in the process and what appeared as irrelevant indicators when viewed through the stovepipe lens of a singular discipline would have been flagged as I&W of the attack. Figures 8 and 9 provide a comparison of the traditional approach and the ABI approach.

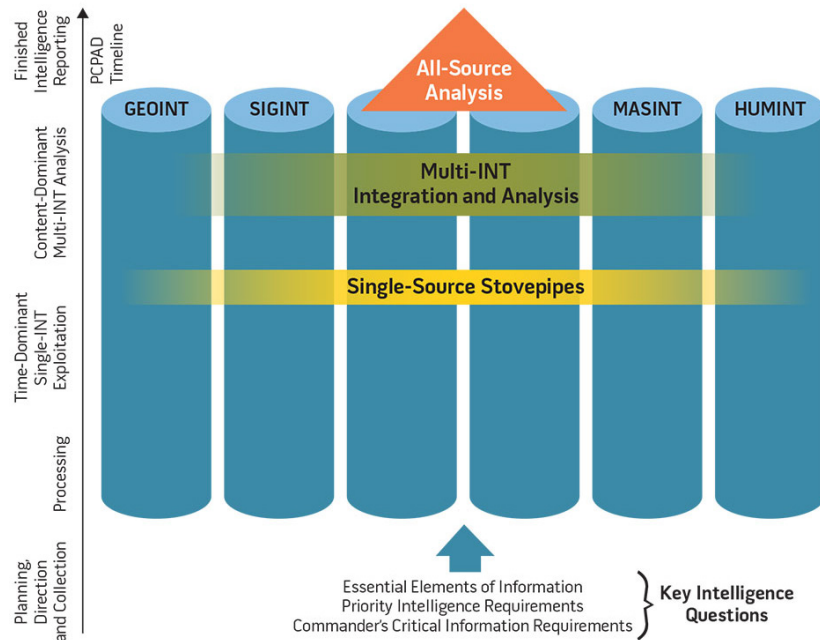


Figure 8. Traditional and Current PCPAD Intelligence Process.
Source: Atwood (2015).

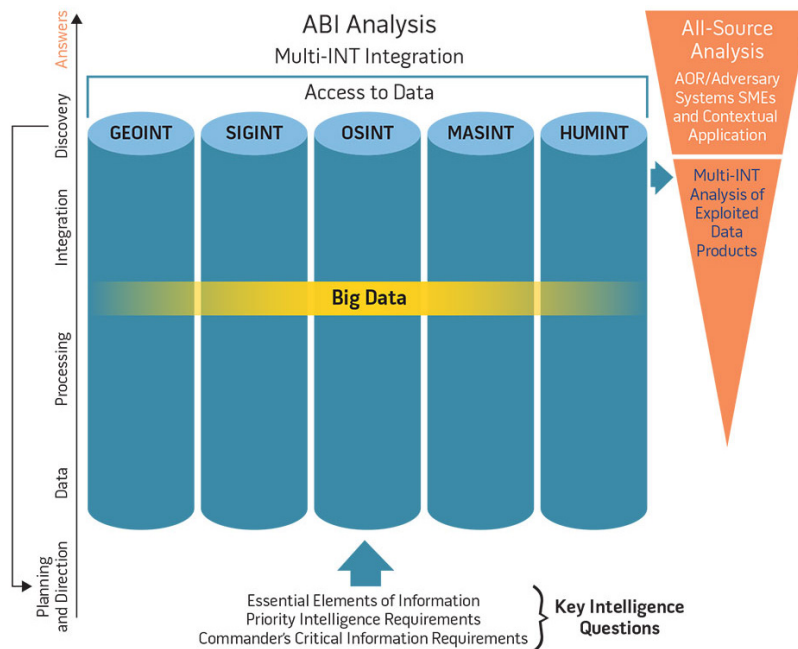


Figure 9. How ABI Transforms the Traditional Intelligence Process.
Source: Atwood (2015).

ABI has four main pillars required for execution: “geo-reference to discover, [integration] before exploitation, data neutrality, and sequence neutrality” (Atwood, 2015). These pillars do not occur in a sequential order and are not listed in order of precedence. All are required to enable discovery of unknown IRs gained through early integration of collected data.

Geo-reference to discover – Data must be tagged, both spatially and temporally, at the point of collection as opposed to historical methods where it occurs at the end of the analytic process (Atwood, 2015). If data is not properly tagged, it will be impossible to retrieve and integrate using AI technological solutions. If the data is not tagged instantaneously, the multi-INT integration which takes place simultaneous to ongoing collection cannot occur.

Integration before exploitation – Integrating data at the earliest point and prior to exploitation and analysis under the traditional intelligence cycle (Atwood, 2015). As Figure 8 exhibits, the current intelligence process integrates data via all source analysis at the end of the stovepipe discipline collection period. ABI seeks to improve on the process by enabling the integration to occur at the spot of collection. This exhibits why the first pillar of geo-reference to discover is vital to the process.

Data neutrality – The concept that all data is relevant and analysts should not bias their collection to focus solely on a specific discipline (Atwood, 2015). Current analytical methods often cause analysts to seek specific information based upon the identified target set. Collection plans are developed with specific assets tasked to collect on the target. If analysts bias their analysis by only taking in data from specific assets, they may miss important correlations that lead to answers of unknown intelligence requirements. More simply stated, the analyst may find the answer they are seeking, but it may be limited in scope and they may not identify other critical answers they didn’t think to ask in the first place.

Sequence neutrality – Traditional intelligence processes focus on a linear methodology. ABI is non-linear and the focus of the analyst should not be solely focused

on the most recent collection. Archived multi-INT collection analyzed forensically can be just as useful (Long, 2013).

ABI is not only a process change, but a technological change as well. To support the four aforementioned pillars, the use of geo-enrichment technology, real-time analytics, big data analytics, and application frameworks should be considered as part of the intelligence enterprise (Conklin, 2010). As MCISRE pushes forward in building its intelligence processing and exploitation capabilities, it must do so in a deliberate manner. The days of acquiring standalone capabilities must come to an end, and the Enterprise must view acquisition through an integrated approach. The future acquisition approach for collection assets must enable data tagging and interoperability from all collection in support of multi-INT integration for modern warfare.

F. CAPABILITIES THAT ENABLE ARTIFICIAL INTELLIGENCE

Integration of AI is not as simple as developing an algorithm and applying it to existing programs of record. There are critical enabling capabilities to support data discoverability using AI tools. These capabilities span across data ingest, storage, discoverability, processing, and dissemination. Failure to plan for and manage data across the various stages renders algorithmic solutions inept. The remainder of this literature review will focus on capabilities that support and enable AI. These capabilities will form the basis for DOTMLPF-P recommendations provided in Chapter IV.

1. Machine Learning and Artificial Intelligence Overview

AI is the modern buzzword thrown around for every emerging predictive capability but is rarely used correctly. For sports fans, a relatable example of this is the National Football League's (NFL) use of Next Gen stats provided by Amazon Web Services (AWS). AWS provides player tracking to capture real time location data, speed and acceleration. AWS uses sensors placed across the entire playing field to track tags on players' uniforms and chart individual movements within inches (Amazon, 2018). As Figure 10 shows, using the data and a self-described AI capability, passes are dissected with probability of completion at different points during the route.



Figure 10. Next Gen Stats AI. Source: Amazon (2018).

The use of thousands of data points from multiple actors involved in the play combined with ball velocity, trajectory and historical player statistics is impressive and takes the evaluation of the play to a new level, but it is not AI. AWS would more appropriately be labeled ML.

AI is defined as, “the capability of a machine to imitate intelligent human behavior” (Merriam-Webster, 2018). Simply taking data and running a statistical probability like Next Gen stats is not drawing intuitions or imitating human behavior. AI is able to use rules-based reasoning, natural language processing, and knowledge representation techniques to simulate human decision making (MC.AI, 2018). Succinctly stated, AI can use temporal reasoning to gain inferences from data to aid in decision making.

ML is a subcategory of AI that uses data mining and predictive analysis (Domingos, 2012). In ML, the algorithm uses numerical and statistical approaches to reduce large amounts of data to a logical predictive conclusion (MC.AI, 2018). A key component of ML is the algorithm’s ability to improve itself over time, known in ML as learning. Another way of stating this is the algorithm can teach itself based upon past results and positive or negative user feedback on its accuracy.

A third subset known as deep learning (DL) also exists, but is not referenced as interchangeably as AI and ML. DL is explained as “a form of machine learning where computers develop and learn from experience to understand the world in terms of a

hierarchy of concepts” (Goodfellow, Bengio and Courville, 2016). There is no need for a human to specify all knowledge to the computer, but rather provide initial input via simple hierarchy concepts from which the computer can build upon and teach itself (Goodfellow, Bengio and Courville, 2016). In DL, the computer develops a hierarchy of neural networks to build upon the foundational input. The use of the neural network approach enables DL which then enables ML and AI as depicted in Figure 11.

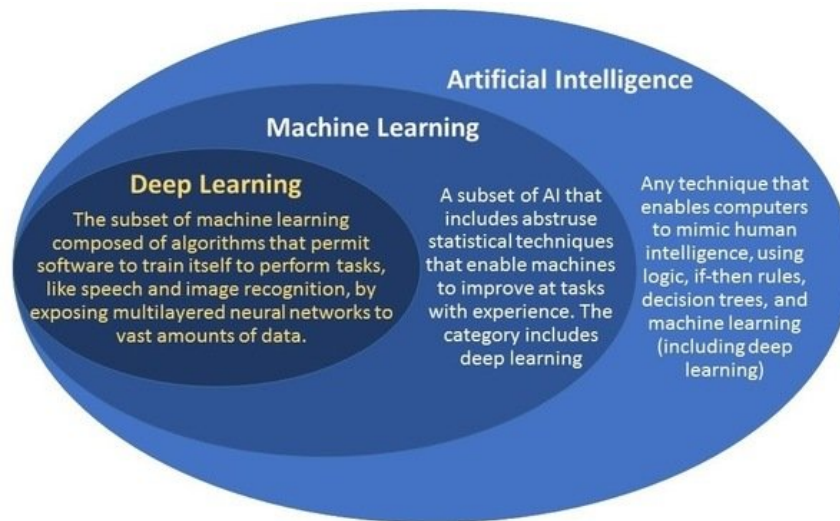


Figure 11. Deep Learning vs. Machine Learning vs. Artificial Intelligence. Source: Dhande (2017).

There are four main types of algorithmic approaches to enable DL, ML, and AI: supervised, unsupervised, semi-supervised, and reinforcement learning (Fumo, 2017). Supervised learning can be viewed as function approximation. With supervised learning, the human acts as a teacher for the computer. The human feeds the computer with labeled input data and identifies correct answers (Fumo, 2017). This training phase ultimately enables the algorithm to learn patterns and improve itself autonomously over time. When future data sets are introduced, the computer can then reference back to what it learned from previous data sets. Looking at a military application, supervised learning may be useful when an analyst is attempting to identify specific indicators for identified intelligence requirements. The supervised approach, however, can be limiting in that the

output is driven strictly by the input and the rules applied. If the analyst is biased in the output they are looking for, an unsupervised approach may be more useful and identify unknown unknowns which were not previously identified as intelligence requirements.

With unsupervised learning, the computer is trained with unlabeled data (Fumo, 2017). In this case, the human does not act as a teacher. The computer learns patterns independently and produces outputs. This type of approach is especially useful if the human is not sure what to look for in the data (Fumo, 2017).

Semi-supervised learning combines the use of labeled data with unlabeled data (Fumo, 2017). Analysts may find this useful if there are specific priority intelligence requirements and indicators they are seeking but do not want to limit their output to a strict set of rules. This approach gives analysts more control over the outcomes without limiting them with a direct supervision approach.

The last approach is reinforcement learning. Reinforcement learning uses data gathered from the outputs it produces and modifies its algorithm to either maximize reward or minimize risk. This is a combination of supervised and unsupervised learning. Reinforcement uses supervised learning to identify what a risk and reward are for a given scenario. The algorithmic approach utilizes unsupervised learning because it is not reliant upon a labeled data set, but rather the responses from decisions made (Fumo, 2017). Reinforcement learning is able to continuously learn from the environment in an iterative process until the full range of possible states are evaluated. A synopsis of the four approaches is provided in Figure 12.

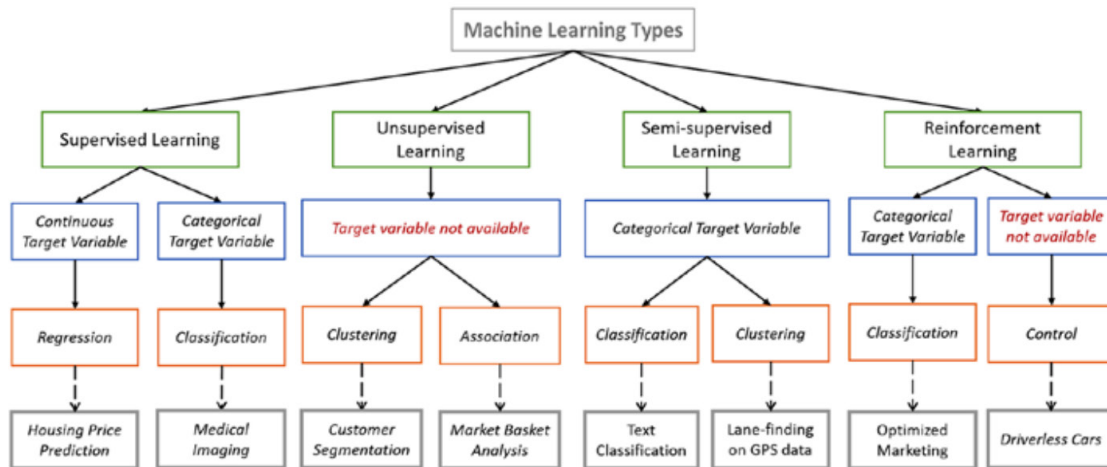


Figure 12. Four Approaches to Machine Learning. Source: Fumo (2017).

2. Data Ingest

MCISRE faces challenges across the five Vs of big data depicted in Figure 13 (Ramadan, 2017). MCISRE's current processing, exploitation, and dissemination (PED) capabilities cannot keep pace with the five Vs or continue to mitigate issues from poor interoperability resulting from stovepipe system development. Big data challenges have historically centered around volume and velocity; however, recent growth in variety and issues with veracity expound the complexity across the information environment (Atwood, 2015).

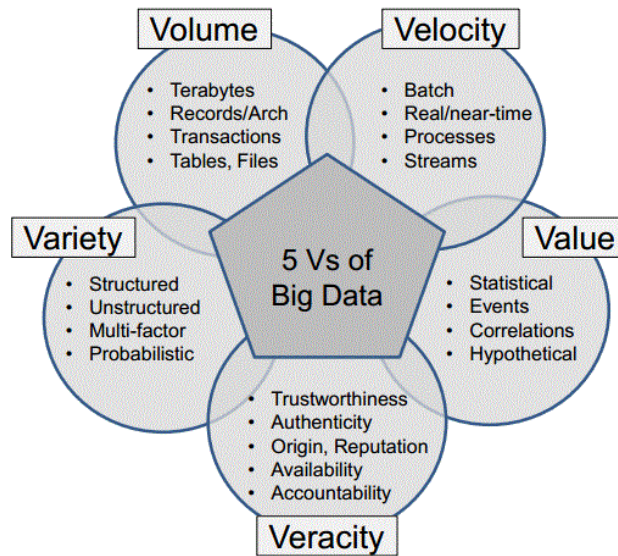


Figure 13. The Five V's of Big Data. Source: Ramadan (2017).

Volume – Volume refers to the exponential growth in data that is collected. Every day, the IC collects more raw data than the entire workforce could analyze over the course of their entire lifetime (Allen and Chan, 2017). AI requires large volumes of data to train algorithms using supervised and semi-supervised techniques. Aside from training algorithms, the volume of data required to support AI must span all classification domains. Current methods of storing data across disparate classification domains reduces the volume of critical data required to enable AI. MCISRE must overcome cross domain issues in order to implement AI.

Aside from training, the volume of data is important because although certain information may seem insignificant, it may actually be the key to algorithmic deduction and cross-cueing with other information. The IC must continue to invest in technological advancements to automate data compilation, processing, and exploitation through artificial intelligence.

The continual growth in collected data and the ability to store it is a significant consideration for an enterprise dealing with requirements associated with AI. On the positive side, data storage continues to rapidly decrease with cost per unit of space being

cut in half every 14 months (Komorowski, 2014). Data storage today costs around \$0.03 per gigabyte compared to \$2.58 per gigabyte fifteen years ago (Komorowski, 2014). Figure 14 demonstrates the logarithmic decrease in cost over the past 38 years.

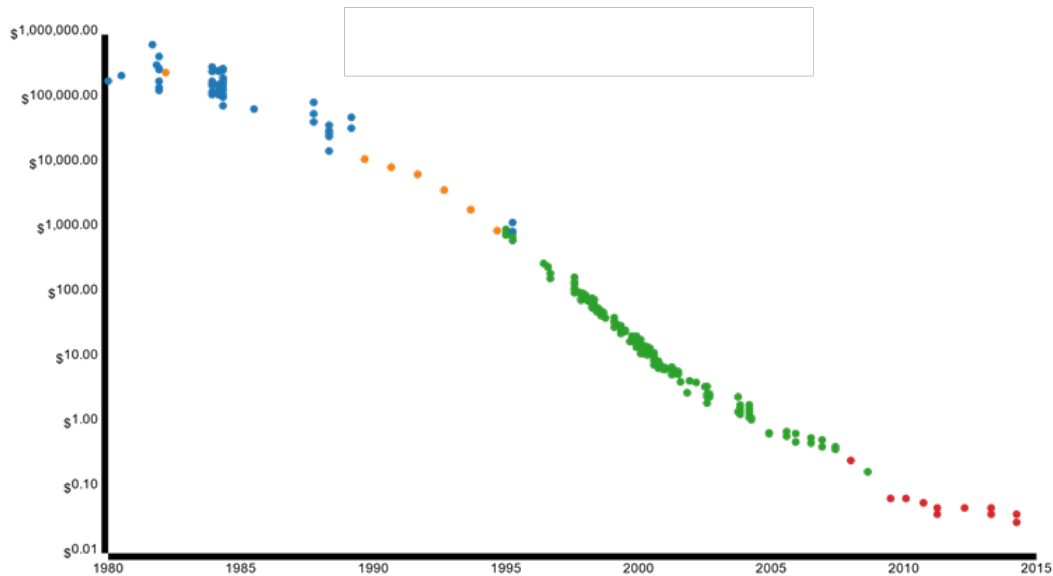


Figure 14. Timeline of Hard Drive Cost (USD) Per Gigabyte. Source: Komorowski (2014).

While it may be cheap to purchase data storage capacity, simply deciding to keep all data for an undetermined amount of time has other considerations. On the financial side, the space to store data servers requires data storage building construction and maintenance, which drive up the cost figure. Cost can also be viewed in time. As the data knowledge base increases exponentially in size, a cost of velocity, or time to process and disseminate, increases as well. Issues of velocity can be minimized through edge computing where processing takes place at the point of data storage and decreases the volume of data being transmitted.

Velocity –Velocity is the speed that data can be processed and disseminated. MCISRE must identify requirements for processing times of data based upon concept of operations and employment of intelligence systems. For example, processing speed for big data to develop an Intelligence Preparation of the Battlespace (IPB) product prior to

deploying is not the same as the velocity required to support indications and warnings (I&W) of pending attack on coalition forces.

Variety – Variety refers to data existing in different forms. These forms are generally labelled as structured or semi-structured data. Structured data is easily sortable by AI algorithms. An example of a structured format is an excel document or a finished intelligence product which is tagged with a geo-location and time to enable Distributed Common Ground System – Marine Corps (DCGS-MC) to easily sort. Semi-structured data is everything else. Emails, social media postings, and satellite imagery are examples of semi-structured data. Some academics refer to semi-structured data as being unstructured. All data, however, has some structure or it would simply be a signal. Therefore, this thesis will employ the semi-structured viewpoint. There are ways to convert semi-structured data to structured data using an ontological approach which will be covered in more detail later. Semi-structured data is inherently more difficult to work with and unfortunately comprises the majority of intelligence collection.

Veracity – This represents confidence in the collected data (Lee, 2016). The confidence in collected data is affected by data inconsistency and incompleteness (Tamhane and Sayyad, 2015). Big data's quality and accuracy can be difficult to control when not organically collected and managed. When leveraging AI solutions, MCISRE will require large volumes of data from organic as well as outside sources. Data across the internet of things (IoT) will include varying degrees of veracity which MCISRE must find a way to sort and assess. Relying solely upon organic collection is not a supportable course of action in the age of AI.

Value – A mountain of data does not necessarily result in a mountain of intelligence. Employment of data mining and analytics can cull important pieces of information from the massive amount of collected data and produce value. Without a means to produce the “so what,” big data provides little value to the customer. The value of information provided by AI will be directly proportional to the ability of the algorithm to explain its output. This is referred to as explainable AI (XAI). XAI enables humans to understand, trust, and manage their machine counterparts by providing rationale (Gunning, 2019). In the intelligence field, decisions must be supported with an explanation. The value

of intelligence produced by AI information systems will be significantly higher with the application of context and rationale.

3. Data Storage

The abundance of disparate software and hardware tools serving the intelligence community portfolio presents significant challenges to enabling AI capabilities. Knowledge-based software solutions developed in isolation without an enterprise architecture approach have diverse hardware platforms, programming languages, and network protocols (Gruber, 1995). The lack of commonality leads to issues in communication, interoperability, and systems engineering functions (Fensel, 2001). The challenges are further exasperated by the fact AI algorithms should not simply rely upon DoD developed collection capabilities but must be able to ingest and make discoverable data collected across the entire web of information. In other words, even if a true enterprise architecture approach was adopted by the DoD to synchronize development of hardware and software under established architectural guidelines, issues with data ingest and sharing across the entire web of information would still pose significant issues. One way to overcome the challenges is through an ontological approach, which “captures knowledge in related fields, provides a common understanding of domain knowledge, identifies common recognition vocabularies, and gives a clear definition of the relationship between these vocabularies from different levels of formal patterns” (Wang et al., 2009). Another way of explaining the definition is information that is collected forms a knowledge base (KB) and the ontology is the structured representation of the data to make it storable, searchable, and retrievable. The development of a common ontology reduces the engineering work load by enabling individual knowledge base systems to develop platform specific knowledge applications which are able to tie into the larger pre-established ontology.

In AI, knowledge that exists is only that which can be represented (Gruber, 1995). An ontology takes the data ingest and breaks it into objects, categories, relations, and attributes. Figure 15 provides a simple example of a healthcare ontology to illustrate the definition. In the ontology, the object would be “healthcare provider” and the “physician”

or “pharmacist” as well as the sub levels identifying types of physicians or pharmacists would be categories. The relation would be the binary connection between the categories. In the example, the relation delineation would be “is a” to represent being a subset category. If one were to expound upon the example and include information such as salary amount that would form the attribute portion.

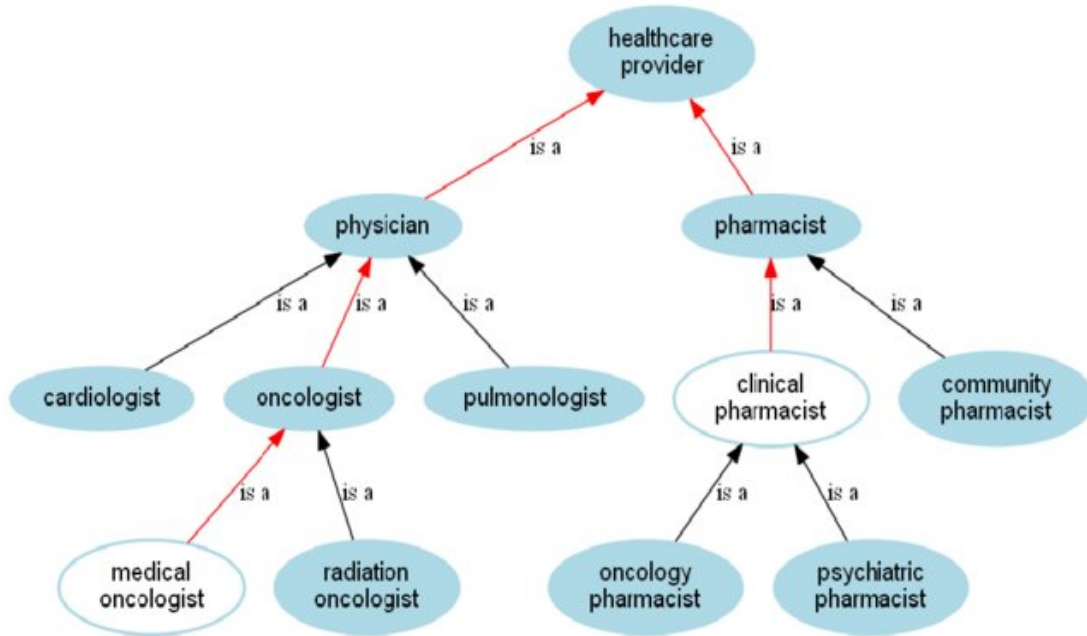


Figure 15. Ontological Approach to Healthcare Data. Source: Pedersen et al. (2012).

Considerations for Designing Ontologies – Ontologies are designed by data engineers. Determining how to represent a given set of data and its interdependent relationships is done through design decisions. In his article, “Toward Principles for The Design of Ontologies Use for Knowledge Sharing,” Thomas Gruber outlines a few key considerations for ontology design.

(1) Clarity – The design process should follow an engineering approach using objective criteria. Data engineers involved in the design process are humans and possess a natural bias. Building an ontological framework should seek to avoid bias gained from a person’s mental schema. Using a formalism approach where the engineers state definitions

in logical axioms vice personal interpretation is a means to reduce bias and increase clarity (Gruber, 1995).

(2) Coherence – Ontologies must be coherent with inferences consistent with established definitions. Formal and informal axiom inferences must match the established definitions. If a natural language sentence can be inferred as contradictory to established definitions, that axiom is not coherent with the model (Gruber, 1995).

(3) Extendibility – Ontologies should be designed to enable expansion from their original design through the use of shared vocabulary (Gruber, 1995). One of the key concepts of ontological design is the ability to continually add to the framework and grow capability to meet a range of tasks and cases – both anticipated and unanticipated. In other words, the design must be able to incorporate new terms for special use cases without having to revisit and redefine the original terms.

(4) Minimal ontological commitment – An ontology should only provide the level of detailed representations which is required to support the knowledge sharing activities (Gruber, 1995). Making as few claims about the subject being modeled allows end users of the ontology to maintain freedom to specialize it to their specific needs. This can be accomplished by defining only terms which are essential to the communication of the knowledge consistent with the theory and letting the use of common vocabulary to allow user specialization to meet their specific needs (Gruber, 1995).

Ontology Construction Methodology – Development of ontologies is not a new concept. In the book, *Ontological Approach to Military Knowledge Modeling and Management*, Anne-Claire Boury-Brisset articulates generalized steps to support the process of ontological development as depicted in Figure 16:

- Definition of the requirements for the ontology (purpose and scope)
- Building informal specification of concepts (taxonomy)
- Formally represent the concepts and axioms in a language (ontology)
- Evaluation of the ontology (Boury-Brisset, 2004)

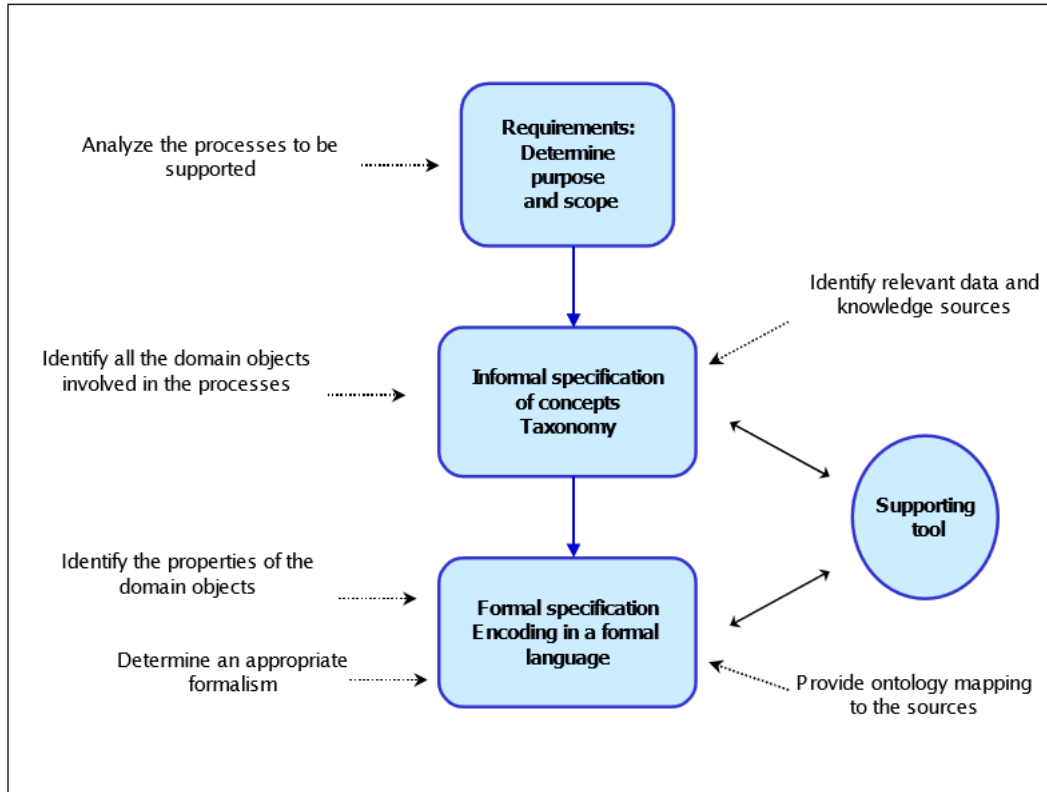


Figure 16. Ontology Construction Methodology. Source: Boury-Brisset (2004).

While data engineers are typically the personnel who design the ontological structure, the process requires an equal contribution from data scientists as well as the end user. A delineation of the differences between data engineer and data scientist will be explored in greater detail later. For now, a simple way of viewing the difference is the data engineer develops the architecture of the ontology and the data scientist provides the insights to the development. The ontological approach is an iterative process requiring constant adjustment and management to support changing events and data streams. The intelligence analyst is the end user and recipient of products produced using the ontology. In the ontology development process, the end user plays a critical role, providing feedback to inform and guide data engineers and scientists.

4. Data Discoverability

Storing data in an ontology makes it sortable and discoverable through the use of text mining. Text mining is the extraction of non-trivial knowledge from structured, semi-structured, and unstructured text (Tan, n.d.). Text mining is accomplished through a variety of approaches and techniques. Two of the most common techniques are clustering and natural language processing (NLP).

Data Clustering – Clustering is a technique that involves the grouping of unstructured data points (Seif, 2017). Clustering is different than data classification. Classification is a supervised learning technique which uses structured data to classify new data based upon previous input. Clustering, however, employs an unsupervised approach to organize unstructured data into groups (Stefanowski, 2009). In theory, data points which are clustered in the same group have similar properties. Clustering analysis can be used to gain insights from data by seeing what groups the data points fall into when a clustering algorithm is applied (Seif, 2017).

Natural Language Processing – While the use of supervised and unsupervised learning are effective for data classification and clustering techniques, semantic language understanding is required to support data discoverability not provided by machine learning (SAS, 2018). NLP is significant because it transforms unstructured language data into a structured searchable and discoverable format. The commonly used Alexa application is an easy way to illustrate NLP. When a user tells Alexa “I like this song,” the application uses NLP to interpret context and meaning and convert it to a rating scale for that music. The application then adjusts its algorithm to add that song and other similar songs to your desired playlist (SAS, 2018). Much like ontologies, NLP breaks down language statements into smaller pieces to better organize and understand the relationships between noun, verb, adjective, etc. This structuring approach ultimately enables the algorithm to provide semantic meaning in a computer algorithmic format.

5. Data Processing and Exploitation

Data ontologies not only support the storage of big data, they directly feed into the data processing and exploitation phase of the intelligence cycle. The ability to store data in

a discoverable manner is not equivalent to operationalizing it. The Joint Directors of Laboratories (JDL) Data Fusion Working Group has developed a model for an ontological approach to support military operational planning (Boury-Brisset, 2004). The JDL model utilizes a five-level approach to data ontology in the military domain.

- Level 0 – Signal assessment
- Level 1 – Object assessment
- Level 2 – Situation assessment
- Level 3 – Impact assessment
- Level 4 – Process Refinement (Llinas et al., 2004)

Level 0 provides data preparation, association, and estimation of entity signals and features. The signal and feature estimation feeds into Level 1, providing an estimation of the entity state using concrete entity information. This estimation details identity, location, and activity of a given entity such as classification of a person, vehicle track, or weapon system (Llinas et al., 2004). Levels 2 and 3, however, operate in a more abstract domain seeking to answer questions about the current situation. In level 2, the output from level 1 is fused with other elements to identify its relationship with other entities within a larger structure. Level 3 then applies output from level 2 juxtaposed with user goals and stated objectives to provide and impact assessment (Llinas et al., 2004). The impact assessment directly supports military planning and course of action development. Level 4, process refinement, is outside of the operationalized parsing of ontology levels, focusing on resource management and process refinement. An overview of the JDL approach is provided in Figure 17.

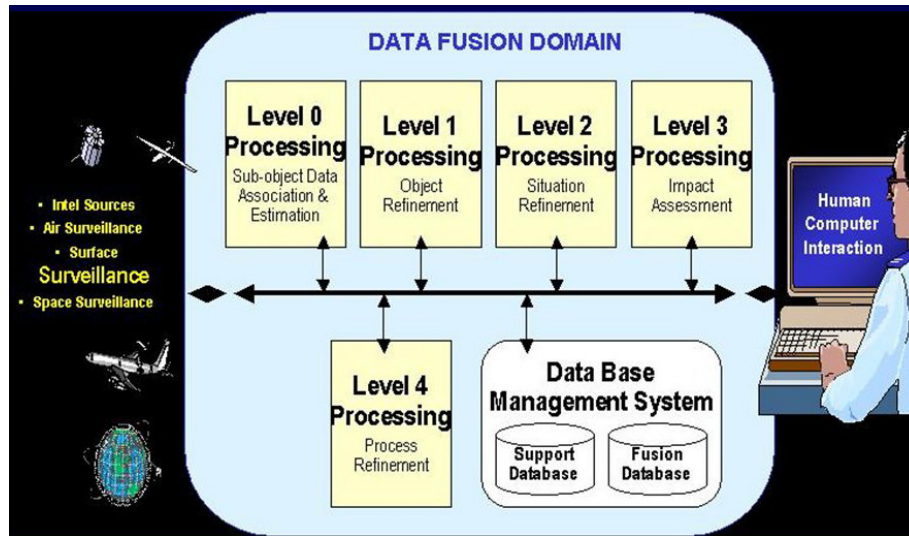


Figure 17. JDL Model. Source: Llinas et al. (2004).

6. Data Dissemination

Once data is processed and exploited, it is only useful if it can be disseminated to the decision maker in a timely manner. Data dissemination using AI applications involves moving large amounts of data from a cloud or land based service not located at the point of data generation or consumption. Thus, industry AI applications rely upon a high level of connectivity and large bandwidth support. This presents a problem for MCISRE. Whether deployed on a MEU or ground based in a foreign nation, the bandwidth requirements to support traditional cloud storage and data mining techniques doesn't mesh well with communication capabilities related to bandwidth usage. One way to overcome this issue is through the use of edge, or fog, computing to enable AI in remote locations where bandwidth is limited. Edge computing moves computing and storage resources away from a geographically separated cloud to the edge of the network close to end devices (PremSankar, Di Francesco and Taleb, 2018). A visual representation of edge computing is provided in Figure 18.

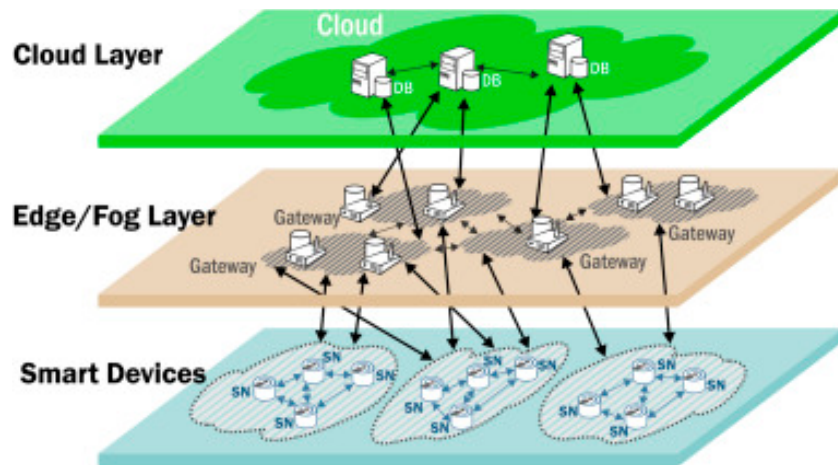


Figure 18. Edge Computing Overview. Source: Rahmani et al. (2018).

The major advantages of edge computing are speed, security, scalability, and reliability (Gyarmathy, 2018).

Speed – The most important benefit provided by edge computing is a reduction in data latency. While data latency may not be as big of an issue for a CONUS based unit, the same cannot be said of a deployed one. Bandwidth limitations experienced on a ship or in a communications contested environment are only further exasperated if the data has to be requested and then disseminated from a geographically dispersed location. Aside from the distance traveled, the dissemination from a centralized location requires the use of several router hops in route to its final destination. Housing and processing data closer to the end user reduces the transmittal distance, expediting the dissemination of time critical information (Gyarmathy, 2018).

Security – In addition to reducing latency, the use of edge computing can also serve to reduce risk from enemy denial of communications. Traditional centralized cloud computing tied to a single node presents an opportune target for an enemy Distributed Denial of Service (DDoS) attack (Gyarmathy, 2018). Any denial or disruption of that node affects the entire Enterprise. Edge computing's employment of multiple clouds, however, protects the network by prohibiting a single targeted DDoS attack from disrupting the entire Enterprise.

Scalability – Housing data at a centralized storage center such as MCIA is expensive and can limit future expansion requirements. Limiting data storage facilities to confined structures restricts an organization’s ability to support future expansion requirements (Gyarmathy, 2018). Edge computing provides a more fiscally advantageous model that allows for additive capability using a combination of data repositories (Gyarmathy, 2018).

Reliability – The security benefits provided by edge computing also produce an increase in reliability. With a single cloud concept, system failure of the node results in catastrophic effects across the organization. Edge computing overcomes this issue by providing a capability for alternative nodes to subsume the workload of a failed node(s) (Gyarmathy, 2018).

G. CHAPTER SUMMARY

This literature review summarized the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise and how its current intelligence tactics, techniques and procedures operate in today’s fight while always keeping an ever persistent eye on bettering itself for future fights. While MCISRE’s design allows for Marine Corps intelligence professionals to be effective today, there are several gaps and opportunities for AI to drastically improve processes and create efficiencies that will allow us to excel in the future. The importance of Enterprise Architecture and how the Marine Corps approaches Big Data using AI will have great impact on MCISRE. The literature review also examined requirements to enable AI capabilities. AI is not a simple acquisition and integration. There are many secondary and tertiary interdependent considerations to leverage. These considerations will be further examined and expounded upon in the context of the DOTMLPF-P spectrum in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. CHAPTER OVERVIEW

The first part of the previous chapter presented a literature review to provide contextual background on how the Marine Corps currently executes its intelligence functions. The review supports analysis to understand how current processes must adapt to enable the integration of AI toolsets, which will be addressed in the data analysis chapter. The second half of the literature review outlined capabilities required to enable AI solutions. Whether purchasing or developing AI solutions, there are many baseline enabling capabilities and considerations that must be planned for and developed. More simply stated, integration of AI capabilities is not as simple as buying a commercial capability and considering the process complete.

This chapter outlines the approach utilized to develop an AI integration strategy for the MCISRE. This chapter enables the research to be recreated in future research efforts which may expound upon the current subject material. The chapter begins with an overview on the methodology used then further details how the DOTMLPF-P and technology acceptance model approaches are applied to present final recommendations.

B. RESEARCH PURPOSE

The purpose of this research is to evaluate and juxtapose commercial and Department of Defense (DoD) AI capabilities and software against the Marine Corps analytical toolset in order to identify methods for integration. This identification and the subsequent recommendations are aimed at expanding the analytical tradecraft of intelligence analysts to close an expanding capability gap between collection and exploitation of big data in the Marine Corps. DOTMLPF-P recommendations integrated into an AI strategy for the MCISRE is the end result.

C. METHODOLOGY

The authors began by reviewing scholarly research pertaining to commercial AI enabling capabilities. The topics for this research were informed by the authors' thesis

advisor and industry experts which included data ontologies, multiple data source storage and processing, in memory processing, knowledge representation, edge processing, and current prominent AI algorithms used by commercial industry. This review was presented in Chapter II and provided background knowledge required to understand the complexities involved in enabling and implementing AI solutions.

In conjunction with scholarly research, the authors conducted field research by meeting with Marine Corps intelligence professionals as well as commercial industry experts to grow their knowledge base. The authors attended the annual Intelligence Operational Advisory Group (OAG) where they met with representatives from Deputy Commandant for Combat Development and Integration (DC, CD&I) and the Intelligence Integration Division (IID). IID is tasked with developing the final AI integration strategy for the MCISRE. The purpose of the meeting was to ensure the efforts from this thesis aligned with efforts being worked from IID. The OAG also provided an opportunity to sit in the MCISRE Capabilities Based Assessment Working Group. The working group identified required capabilities and gaps to execute the intelligence warfighting function over the next 10–20 years.

The authors also met with the Office of Naval Research to discuss current AI related projects being funded by the Marine Corps. The meeting provided the authors with a further understanding of the current path and focus the Marine Corps is taking towards its development of AI material solutions.

Lastly, the authors met with industry experts from Progeny Systems Corporation and Forge.AI. Progeny Systems Corporation provided an overview on the DoD machine learning product called Surveillance, Persistent Observation, and Target Recognition (SPOTR). SPOTR provides automated detection, tracking, and identification of targets using deployed sensors operating on existing hardware without human interaction (Faltiemier and Middendorff, 2018). Forge.AI is a technology-based company which focuses on processing unstructured information and developing fully automated AI-driven solutions (Forge.AI, 2019).

Using information gathered from scholarly and field research, the authors employed knowledge gained from their curriculum at the Naval Postgraduate School to apply systems engineering processes to conduct a functional analysis of the information collected.

D. DOTMLPF-P APPROACH

As noted in Chapter I, this strategy aims at providing a holistic outlook across the DOTMLPF-P spectrum to provide tangible recommendations to senior leaders across the MCISRE. DOTMLPF-P defines “the eight possible non-materiel elements involved in solving warfighting capability gaps” (DAU, 2018). Nestled within the Joint Capabilities Integration and Development System (JCIDS), DOTMLPF-P analysis is the standard approach utilized across the DoD for defining requirements and enacting non-material changes. Aside from being a standard defined under JCIDS, this strategy is also utilizing a DOTMLPF-P approach to provide an enduring set of recommendations that will transcend specific material capabilities which continue to evolve at a rapid rate. This is because the answer to an emerging requirement is not always more technology.

At the onset of the JCIDS process, a capabilities-based assessment (CBA) is conducted. The CBA establishes required warfighting capabilities, identifies gaps, and transforms them into requirements (DAU, 2018). Following the identification of gaps, a determination of potential solutions is evaluated. Solutions can either be material or non-material in nature. Material solutions go through the full JCIDS process, producing an Initial Capabilities Document (ICD), Capabilities Development Document (CDD), and sometimes a Capabilities Production Document (CPD) prior to material acquisition. Non-material solutions are evaluated through a formal DOTMLPF-P analysis. The results of the DOTMLPF-P analysis lead to a DOTMLPF-P Change Request (DCR). The DCR process establishes non-materiel solutions to mitigate capability gaps (DAU, 2018). The eight specific elements evaluated during the DOTMLPF-P analysis are defined below.

Doctrine: the way we fight (e.g., emphasizing maneuver warfare, combined air-ground campaigns)

Organization: how we organize to fight (e.g., divisions, air wings, Marine-Air Ground Task Forces)

Training: how we prepare to fight tactically (basic training to advanced individual training, unit training, joint exercises, etc.).

Materiel: all the “stuff” necessary to equip our forces that DOES NOT require a new development effort (weapons, spares, test sets, etc., that are “off the shelf” both commercially and within the government)

Leadership and education: how we prepare our leaders to lead the fight (squad leader to 4-star general/admiral - professional development)

Personnel: availability of qualified people for peacetime, wartime, and various contingency operations

Facilities: real property, installations, and industrial facilities (e.g., government owned ammunition production facilities)

Policy: DoD, interagency, or international policy that impacts the other seven non-materiel elements. (DAU, 2018)

E. CHAPTER SUMMARY

This chapter outlined the approach the authors utilized to gather information and synthesize it into an AI integration strategy for the MCISRE. It detailed the research approach which entailed a review of previously published material and field research. The chapter also detailed the DOTMLPF-P approach and why it is being used as the basis for recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS OF ANALYSIS

AI might be a powerful technology, but things won't get better simply by adding AI

– Vivienne Ming

A. CHAPTER OVERVIEW

Chapter I established the imperative and urgent need for MCISRE to develop an AI strategy. Chapter II examined MCISRE in the context of its organizational design and methods for evolutionary improvement. The literature review also detailed the host of enabling capabilities required to support AI across an organization. This chapter synthesizes information from the literature review and field research through a functional analysis of identified AI requirements juxtaposed with MCISRE design. This chapter employs an end-to-end systems analysis of enabling AI capability recommendations across the DOTMLPF-P spectrum. As noted in Chapter III, the DOTMLPF-P approach is being employed in this research to use standard terminology common across the Enterprise, as well as provide an enduring set of recommendations that will transcend evolving material capabilities.

B. DOCTRINE

The doctrine pillar of DOTMLPF-P provides a review of existing military doctrine to determine where updates are required. From Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting*, the Marine Corps defines doctrine as

a teaching of the fundamental beliefs of the Marine Corps on the subject of war, from its nature and theory to its preparation and conduct. Doctrine establishes a particular way of thinking about war and a way of fighting. It also provides a philosophy for leading Marines in combat, a mandate for professionalism, and a common language. In short, it establishes the way we practice our profession. (MCDP 1, 1997)

The fundamental principles that built MCISRE and how the Enterprise conducts its business are based on the writings and teachings of MCDP 1 and other Marine Corps

intelligence publications. This section addresses recommendations for MCISRE to update specific Marine Corps publications that support the employment of AI systems, as well as support implementation of an Activity Based Intelligence (ABI) approach to the intelligence discipline.

1. Update MCWP 2-10, Intelligence Operations

Current methods outlined in Marine Corps intelligence publications prescribe the intelligence cycle as six steps, conducted in a linear process. MCISRE historically and currently produces intelligence to inform commanders' decision making by executing the intelligence cycle in sequential order. With the employment of AI systems and implementation of ABI techniques, the cycle requires a new approach.

ABI calls for a non-linear and continuous process—a stark contrast to the current intelligence cycle. ABI uses large volumes of data across every intelligence discipline, integrating and identifying correlational attributes instantaneously (Long, 2013). This approach replaces traditional intelligence processes where exploitation occurs after the collection phase of the intelligence cycle. Processing, integrating, and exploiting data must occur immediately upon collection and be a persistent procedure through every step of the intelligence cycle. Historical processes of stove-piping storage of collected data by intelligence disciplines (INTs) do not support ABI. In today's information-dominant environment, conducting all-source data exploitation post-collection is disjointed and inefficient. Through the use of analytical toolsets that employ AI techniques, MCISRE will be able to autonomously correlate data, spatially and temporally, across all the INTs and allow processing and exploitation to occur immediately upon collection. This automated correlation assumes a host of other enabling factors that will be discussed as separate recommendations later in this chapter.

Following the sequence neutrality pillar of ABI, MCISRE must develop a non-linear intelligence process. Although collection efforts will be planned and directed to accomplish specific intelligence objectives, the exploitation and analysis of those intelligence requirements will no longer serve only that purpose, but will also be tied into the greater multi-INT collection of data that is continuously exploited. The data collected

not only answers specific intelligence requirements, but will also play a role in feeding a larger picture to uncover unknown requirements. Utilization of intelligence and future analysis of information will play a critical role in providing feedback to the continuous processing and exploitation. The understanding of a threat environment or situation can play into future analysis of the same or similar problem set and will be updated with new multi-INT collection. Therefore, the Enterprise must embrace persisting all data when possible.

It is recommended that the current intelligence cycle detailed in MCWP 2-10 be updated to reflect the adaptation of ABI techniques through the employment of AI systems. A graphic of an updated intelligence cycle that reflects these changes is highlighted in Figure 19.

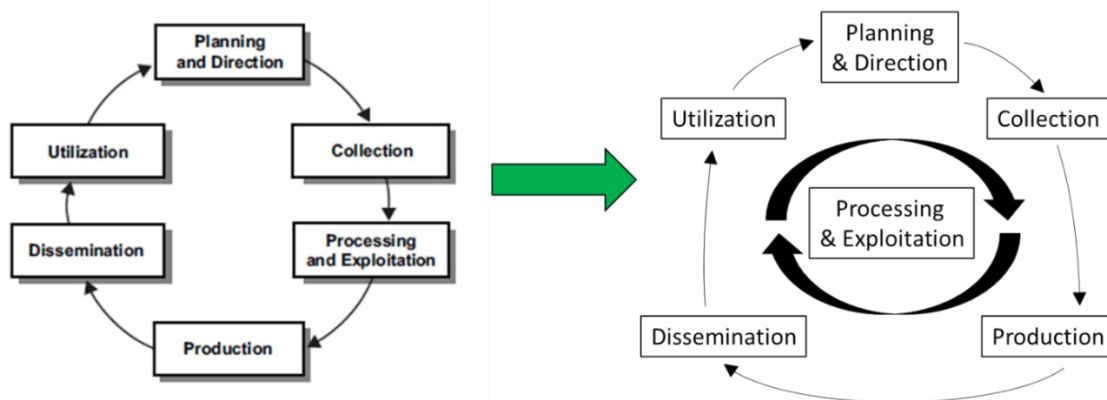


Figure 19. Updated Intelligence Cycle. Adapted from MCWP 2-10 (2016).

Along with updating the intelligence cycle, MCISRE should update Chapter Three, “Developing Intelligence,” to dismiss the claim that too much data overloads capacity to conduct PED, becoming a detriment as opposed to an asset. There are specific times, in limited and denied environments, where only necessary data is required and prioritized to be collected, processed, exploited, and disseminated. However, Marine Corps intelligence doctrine must dispel the notion that having too much data can lead to confusion simply because the means to analyze and put immediate meaning or value to an immense amount

of data was not present. AI systems have the ability to correlate and interpret vast amounts of data that, if not readily useable, can be discoverable for future use. The data neutrality pillar of ABI dictates that all data is relevant, and MCISRE should update MCWP 2-10 to reflect this point. Continuing with Chapter Three of MCWP 2-10, the description of processing and exploitation requires updating to include tagging and geo-referencing data spatially and temporally so it is discoverable and correlated to data across all INTs. As long as data is tagged for geo-reference to discover, all data is important and could provide correlations and insights that did not exist beforehand. AI systems can make use of data that was previously thought to be unimportant or irrelevant. Due to the vast amount of data and reduced signatures of relatable threat information in today's environment, ABI will allow MCISRE to correlate disparate data and provide greater insights for developed intelligence. ABI allows for target-specific information to be discovered, as well as the unknown unknowns about the target environment.

Chapter Four, "Concept of MAGTF Intelligence Support," needs to be updated to reflect changes in personnel and staff sections. This will be discussed in more detail in recommendations found under the organization section of this chapter. MCWP 2-10 must account for and delineate the added structure and support of data engineers, data scientists, and the potential establishment of a new intelligence discipline, Data Intelligence (DATINT), within MCISRE.

2. Update MCTP 2-10A, MAGTF Intelligence Collection

MCTP 2-10A requires updates to reflect changes in the collection and exploitation management process, including the immediate and continuous integration and exploitation of all multi-INT data. This includes updating the previously-discussed intelligence cycle also found in this publication. In Chapter Two of this publication, "Collection Requirements Management," an in-depth review and evaluation of the requirements analysis criteria (pertinence, feasibility, completeness, validation, priority) should be conducted in order to determine a need for new requirements or updates to the existing ones. With the implementation of AI systems and the continuous processing and

exploitation of the intelligence database, the collection criteria of validation may be unnecessary as this will occur automatically.

3. Update MCTP 2-10B, MAGTF Intelligence Production and Analysis

As previously discussed, it is recommended that Chapter One, “Fundamentals,” of MCTP 2-10B be similarly updated to reflect the changes to the intelligence cycle. Also, in Chapters One and Two of MCTP 2-10B, a revaluation of the production steps – filtering, recording, evaluating, analyzing, and product preparation – and their relation to the implementation of AI and Machine Learning systems needs to be conducted. The concepts of synthesis and analysis of information will become more automated with AI/ML systems, and with the housing of big data and the use of ABI methodologies, irrelevant information may take on a whole new meaning in the filtering process.

While automation of the analytical process will continue to increase, feedback loop, as well as analyst input into the accuracy and reliability of the AI analysis, will become increasingly more important. Ultimately, MCISRE must ensure this publication addresses and emphasizes the importance of feedback loop while employing AI systems.

C. ORGANIZATION

Analysis of organization examines how MCISRE is organized to fight. This analysis seeks to identify if a better organizational structure or capability exists that can be developed to support AI integration (DAU, 2018). Organizational recommendations that follow are derived from the baseline MCISRE organizational design to enable a fluid evolutionary transition of AI vice a revolutionary approach, requiring a complete overhaul of the existing structure.

1. Update the MCISRE Enterprise Architecture to Better Address AI Standards

The literature review provided in Chapter II examined Enterprise Architecture and its importance to an organization’s success. As mentioned, an effective EA encompasses six core elements: framework, governance, best practices, artifacts, methodology, and standards. Each element must be considered when enacting organizational change.

The MCISRE 2015–2020 Plan outlines the need for an enterprise approach to intelligence production and provides the framework the enterprise is built. MCISRE governance is clearly identified within the roadmap as stemming from the DIRINT to the Executive Steering Committee down to the advisory groups and governance boards. At every level, the Enterprise is structured around the same foundational concepts working in unison toward a common end state. Best practices are shared across the Enterprise through communities of practice and online dissemination of lessons learned. Artifacts are well defined through requirements documents and programs of record. Methodologies, although they may differ slightly from one unit to the next, largely operate in a harmonious manner, based upon common Mission Essential Tasks (METs) and training and readiness metrics. To effectively implement AI, however, MCISRE must adjust its standards. From the point of collection through to data dissemination, if MCISRE is going to maximize its return on investment in the field of AI, the storage, discoverability, production, and dissemination of data must adhere to an enterprise architecture standard.

The Institute of Electrical and Electronics Engineers (IEEE) defines standards as “published documents that establish specifications and procedures designed to ensure the reliability of the materials, products, methods, and/or services people use every day” (IEEE Standards Association, 2011). Established specifications and procedures are vital to enabling data compatibility and interoperability required to execute AI. Standards come in many forms, but some of the key standards MCISRE must address are analytic, interpretability, technical, and data standards.

Analytic standards address the quality of the algorithmic analysis (Public-Private Analytic Exchange Program, 2018). As AI solutions are implemented, MCISRE must ensure it develops standards to support the identification of algorithmic biases and uses its governance structure to mitigate them. That is, AI systems rely upon the data to learn and produce outputs, and MCISRE must develop standards to ensure the input data are not skewed, limited or biased, any of which would alter the optimal output.

Interpretability standards concentrate on the insight into how algorithms derive outputs. Oftentimes, AI algorithms provide little insight into how outcomes are reached (Lai, 2018). The inability for an algorithm to demonstrate how it reached a conclusion

makes it far less likely to be trusted and utilized to make operational decisions. This is especially important in the early stages of AI integration when trust in the human-machine teaming process is at its lowest point. MCISRE must explore creating AI systems which are explainable to build human user trust in AI. Some experts call this “explainable” AI.

Technical standards provide a means to measure the performance of an algorithm (Public-Private Analytic Exchange Program, 2018). Integration of AI must be approached with an ability to monitor effectiveness. To evaluate technical standards, controlled scenarios can be employed with known outcomes to assess if the algorithm produces results that meet technical standards required of a given scenario. An example of this is the number of false positives or negatives. If the system is given data and the evaluator knows it should identify a certain number of threats, he or she can use the algorithm’s output to determine how many items were identified incorrectly as threats (false positives) and how many threats were not identified at all (false negatives). Depending on the scenario and user input criteria, these standards can shift, but MCISRE must have a way to identify and evaluate standards before employing an AI system.

Data standards are critical to data discoverability. Quantity and quality of data are the backbone for most AI systems (Public-Private Analytic Exchange Program, 2018). Much of the data and software used across MCISRE are developed in a proprietary nature which doesn’t support interoperability. To address this issue, MCISRE should seek to build an open data ecosystem with established standards for structuring and labelling data (Public-Private Analytic Exchange Program, 2018). The standards must also implement the use of cloud computing to support discoverability across currently siloed databases. The Joint Artificial Intelligence Center (JAIC) is leading the effort to consolidate databases from within the DoD as well as outside organizations into a common cloud environment while also tackling the issues of data compatibility (Freedberg, 2018). MCISRE would benefit from leveraging the JAIC efforts and resources in this area.

2. Establish an AI Community of Practice

The MCISRE 2015–2020 Plan outlines a vision for continued forward advancement within the Enterprise through utilization of communities of practice (CoP)

(MCISRE, 2014). The MCISRE Plan states, “The Enterprise will be achieved through continuous incremental improvements, most of which will be recommended by innovative Marines and Communities of Practice” (MCISRE, 2014). The alignment of CoPs feeding into higher level steering groups and advisory committees ensures knowledge is harnessed across the Enterprise, feeding directly into executive level decision making.

A CoP is “an informal network of people engaged in a particular profession, occupation, or job function who actively seek to work more effectively and to understand their work more fully” (Gurteen, 2019). CoPs have three critical characteristics: domain, community, and practice (Wenger, 1999). The domain of interest is what defines the CoP. In the case of MCISRE, CoPs exist across domains of interest defined by intelligence disciplines. The community aspect encompasses the members who comprise the CoP. These members communicate with each other, build relationships, and share knowledge on the domain of interest. The practice aspect is the building of a repertoire of resources through the community engagement. It is the product of the domain and the community coming together over a sustained period. From a MCISRE viewpoint, the practice is the tangible recommendations that come out of the CoP to feed across the Enterprise.

Within MCISRE, CoPs are designed according to functional processes to optimize respective contributions to the MAGTF (MCISRE, 2014). The MCISRE Plan aims for communities to ensure specific intelligence disciplines operate in a unified manner toward process and technological improvements. This same principle must be applied to AI integration and sustainment. AI is a cross-cutting functional capability that touches all intelligence disciplines. As such, the CoP community should be built differently than that of a SIGINT or HUMINT CoP. The AI CoP community must have membership across all disciplines and all levels of MCISRE.

The complexity of the domain of interest for the AI CoP is growing at an exponential rate. What is perceived as ground breaking technology today may be antiquated five years from now. Understanding the rapid evolutionary nature of AI makes the relevancy and need for a CoP even more prominent. AI also stands to overhaul current processes within the intelligence warfighting discipline. As processes change, a CoP ensures lessons learned are captured and shared across the Enterprise. Lessons learned

through trial and error become value added to the organization instead of repeated mistakes. Establishment of an AI CoP will provide MCISRE a bottom up and top down integrated approach to tackle issues, share best practices, and most importantly support a unified approach to future AI developments across the Enterprise. If MCISRE fails to establish a control mechanism to reel in the dozens of active AI funded projects currently being worked in isolation, it will have a disjointed solution without a clear vision. Establishment of a CoP early through a formal charter represents an essential first step.

D. TRAINING

Training analysis examines how MCISRE prepares its forces to execute the intelligence warfighting function from basic training, advanced individual training, and unit training (DAU, 2018). Introduction of AI capabilities will provide significant process improvements, causing considerable gains in efficiency for analysts and their ability to make sense of big data to support decision makers. While the technology adoption will provide opportunity for improvement, its effectiveness will largely be determined by the directly-correlated training required on how to employ, understand, and manage AI.

1. Establish Training to Support Human-Machine Teaming

Human-machine teaming through integration of AI provides an opportunity to significantly bolster intelligence production capability. In warfighting, the interaction of humans and machines is characterized by huge benefits and grave consequences (Hendrickson, 2018). The nature of warfare increases the strain between humans and machines more so than that experienced in commercial industries worried about predicting the next quarter's sales revenue. In a military context, the most critical aspect of automation is not the engineered algorithmic code, but rather the human and machine relationship (Hendrickson, 2018). Specific to the relationship, the key consideration is trust. Trust between a human-machine team can be built in the same manner as a human only team – through training and repetition.

Everett Rogers' Diffusion of Innovation Theory states the "rate of adoption of innovations is impacted by relative advantage, compatibility, trialability, observability, and complexity" (Rogers, 2003). With the plethora of AI related capabilities on full display

across society, the relative advantage is an easy point to achieve. To gain acceptance of AI once implemented, MCISRE must focus on increasing trialability and decreasing complexity. These two points can be achieved through a detailed training plan for any AI toolset introduced to the Enterprise.

Every developed or procured AI product must be accompanied by a robust fleet training plan during fielding as well as an institutional plan at intelligence schoolhouses. This is a critical aspect which, if overlooked, puts the entire effort at risk of failure. No matter how great a technology is, if it lacks acceptance and becomes ignored, it becomes another weight in the corner of the room. MCISRE must anticipate and posture against the resistance to change which comes inherent with the introduction of new technologies. Working with Marine Corps Systems Command on a fielding plan which includes adequate training as well as Marine Corps Intelligence Schools (MCIS) on adjusting training plans is critical to ensuring technology acceptance and success of AI. Training and repetition will not only produce efficiency, but more importantly it will build trust in the human-machine team.

2. Develop Training to Better Support Data Annotation

As detailed in the literature review, AI tools operate within the 5 V's of big data: volume, velocity, value, veracity, and variety (Ramadan, 2017). AI provides the ability to take on large volumes of data, use it to train algorithms, and deduce results previously unattainable using human centric processes. The veracity, or data validity, and ability to handle the variety of data are critical to the process. A human training example is a good way to illustrate these three aspects of big data. Becoming an expert in a field is a strenuous process which takes a minimum of 10,000 hours, or ten years (Prietula, Cokely and Ericsson, 2007). Over the course of ten years, the human is exposed to large volumes of information and scenarios which build their repertoire of knowledge. The same fundamental requirement holds true for AI solutions. In the case of AI, the time period is condensed, but the need for large volumes of data to train remains a critical component. If the human is not studying information with high veracity, training for ten years actually produces negative results resulting in the human producing incorrect assessments. The

same is true for AI. Lastly, the human must be able to access training material from all available resources from printed book to online professional blogs. If the human is unable to discover and access relevant material to study, they are unable to train. AI systems must overcome this through conversion of data variety into a structure data storage lake which is sortable and discoverable for use by many algorithms.

Recommendations to deal with volume issues can be addressed with a cloud computing strategy. This subject will be examined further under policy recommendations. One consideration to deal with veracity and structuring variety of data is through human data annotation. Analysts employing proper data annotation techniques enable a supervised learning approach to teach algorithms. In supervised learning, the human acts as a teacher for the computer by feeding the computer labeled input data and identifying correct answers (Fumo, 2017). This training phase ultimately enables the algorithm to learn patterns and improve itself autonomously over time. When future data sets are introduced, the computer references learning that occurred during the training phase and generates output without human guidance. The key part of supervised learning is the ability of the human to properly label data feeding into the system. This is accomplished through tagging data with all pertinent information including geo-location, timestamp, and classification of activity.

Surveillance, Persistent Observation, and Target Recognition (SPOTR) is a capability being developed by the Navy and Marine Corps which provides automated detection, tracking, and identification of targets using deployed sensors operating on existing hardware without human interaction (Faltmier and Middendorff, 2018). In order for SPOTR to autonomously identify targets such as an enemy combatant, proper data annotation must feed into the training phase. The SPOTR algorithm is not built knowing what a weapon is, it learns it through repetition gained from analyst data annotation input. The success or failure of SPOTR and any other AI systems, relies upon proper data tagging up front. Analysts across the intelligence community are not adequately trained and do not invest enough time into employing data annotation techniques. For AI to be successful across MCISRE, a renewed focus on training analysts to properly tag and annotate data feeding into the system is required.

E. MATERIEL

The traditional Joint Capabilities Integration and Development System (JCIDS) definition of materiel analysis is an examination of all the necessary equipment and systems required to fight and operate effectively (DAU, 2018). As stated in the introduction of this chapter, this thesis is not focused on recommending specific algorithmic solutions. The long-term approach is focused on recommendations that enable and transcend all materiel solutions. Recommendations in this section focus on approaches to developing materiel solutions that can assist the Enterprise moving forward in pursuit of material capabilities.

1. Establish an Artificial Intelligence Program of Record

During the 2018 Fall Operational Advisory Group (OAG), six MCISRE programs presented future programmatic plans to incorporate AI capabilities into their baselines. A few months later, the Marine Corps Warfighting Lab (MCWL) hosted an AI cross-leveling summit in response to the host of disjointed Artificial Intelligence (AI) efforts being funded across the service. The common theme across the OAG and MCWL summit is that the Marine Corps is aggressively pushing AI integration, but it is doing so in a disjointed manner without a cohesive long-term vision and plan. The development of a formal MCISRE AI strategy, which this thesis supports, will remedy the problem. A strategy, however, is just a plan to achieve implementation. AI integration into MCISRE will only happen with proper funding. In order to approach AI in a holistic manner across all programs of record, establishment of an AI Program of Record (PoR) is recommended. Establishing a formal PoR for AI will force development of formal requirement documents detailing specific AI capabilities required by MCISRE to close gaps in its intelligence capabilities. These formal documents force a long-term outlook, providing an opportunity to consolidate current efforts. AI will ultimately touch every intelligence PoR whether it's an analysis capability or collection system. Establishing a PoR which focuses on a spiraled implementation plan will allow MCISRE to prioritize efforts starting with emphasis on processing, exploitation, and dissemination (PED) per the DIRINT's POM 21 guidance.

Another advantage of establishing an AI PoR is funding justification and defensibility. Funding requests under a consolidated AI PoR produce life cycle cost

estimates which present total cost of ownership, bolstering justification for financial resources. Procurement of AI tools is not a one-time cost. Data management, algorithmic manipulation, and software sustainment across the life cycle of AI solutions are relatively unknown across many current efforts which are funded with a short-term view on development, disregarding long term sustainment costs.

Funding defensibility is also increased through a consolidated PoR. At the time of this writing, AI is one of the most heavily discussed topics across the DoD and is viewed as the future of warfighting. Current practices placing AI efforts across multiple PoRs puts funding at risk. Having an established Future Years Defense Program (FYDP) funding line dedicated to AI which supports all MCISRE PoRs makes it more defensible against uncertain future economic environments. MCISRE has been able to shield its DCGS-MC PoR from massive funding cuts due to an ability to demonstrate the vitality of the program which serves as the backbone of MCISRE PED. An AI PoR would serve the same purpose by increasing ability to obtain funding and survive budget cuts in unknown fiscal environments.

2. Employ an Agile Development Process for AI Capabilities

Across the DoD, the average cycle time from program initiation to fielding of an initial operational capability (IOC) is eight years (Tate, 2016). The lengthy process to field critical warfighting capabilities is often the result of seeking the perfect solution in one delivery. An example of this is the F-35 which was took over 20 years to reach IOC (Jones, 2019). While the deliberate approach may support major acquisition programs, such as fielding the next generation fighter jet, it will not work for AI. In a short 20 years, AI has undergone four transformational waves: Internet AI, Business AI, Perception AI, and Autonomous AI (Lee, 2018). Each wave of development experienced shorter cycle time than the one prior as demonstrated by Figure 20. In order to keep pace with the rapid development of AI, MCISRE must steer away from traditional methods of acquisition and adopt an agile development approach.

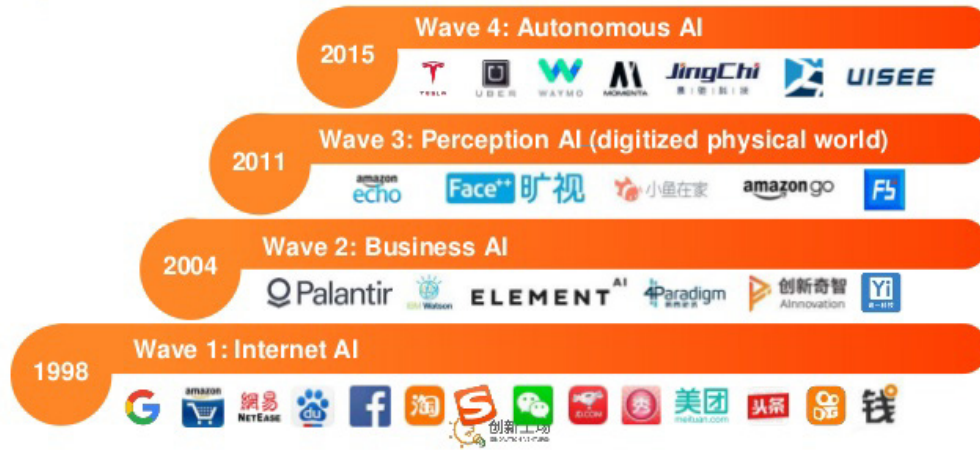


Figure 20. Four Waves of Artificial Intelligence. Source: Lee (2018).

Agile software development is a series of “sprints” to support evolving visions and requirements (Jones, 2019). These sprints can be viewed as incremental and iterative processes placing a heavy emphasis on feedback loop. Agile methodologies are an alternative to waterfall, or traditional sequential development (Jones, 2019). Adopting agile development provides two critical considerations for MCISRE. First, it reduces programmatic risk by enabling cutting edge technology development to fail early and often in the RDT&E phase without incurring significant programmatic delay or increase in funding requirements. More simply stated, since the development of a capability will focus on one iteration across many iterations in the total life cycle of development, the risk is reduced. Secondly, the agile process enables a more expedited fielding of capabilities since they are produced in more manageable pieces vice the traditional approach delivering one final capability.

One cautionary point for agile development is software security. Agile development focuses on functionally working software and iterative delivery, often at the expense of security (Adelyar and Norta, 2016). While rapid development of capability is essential to keep pace with AI technological advancements, it can never come at the cost of compromised security. To overcome the obstacle, some basic tenets must be applied. First, screen software developers and limit their privileges to only that which is required. This principal applies whether using agile or traditional development methods. Second,

maintain software simplicity (Adelyar and Norta, 2016). This principal is supported by agile development which focuses on short sprint efforts. Lower amounts of coding support easier vulnerability assessment. Lastly, increase security testing throughout the development process. Depending on the project, integrate security testing into a daily or weekly routine. If the intent of agile development is to speed delivery of capability, waiting until the product design is complete is too late to begin security analysis. The key point is security must be at the forefront of system design, with testing at every phase of the project's life cycle.

3. Develop an AI Information Systems Initial Capabilities Document

Delay in the delivery of warfighting capabilities is not just an acquisition issue, it is a requirements one as well. The traditional JCIDS process requires development of an Initial Capabilities Document (ICD), Capability Development Document (CDD), and Capability Production Document (CPD) to field a capability (Jones, 2019). The simple development and approval of these documents can take several years. The Joint Requirements Oversight Council (JROC) recognized the problem facing the DoD and in 2008 instituted the Information Systems (IS) construct via JROC Memorandum 008-08 (DAU, 2016). The JROC wanted to provide IT programs with flexibility to “plan for and incorporate evolving technology” by providing an agile and responsive requirements process (DAU, 2016).

The Marine Corps' requirements organization is Combat Development and Integration (CD&I), Capabilities Development Directorate (CDD). Within CDD, Intelligence Integration Division (IID) is responsible for all intelligence programs of record (PoR) that support MCISRE. IID has already taken advantage of the IS construct through development and JROC approval of a Persistent Intelligence, Surveillance, and Reconnaissance (PISR) IS ICD as well as a Distributed Common Ground System (DCGS) IS CDD. PISR and DCGS encompass multiple MCISRE PoRs for collection and data analysis. The approval of the PISR IS ICD and DCGS IS CDD enable MCISRE to approve software requirements internally at a level lower than the MROC and/or JROC. The CG CDD, CG SYSCOM, and DIRINT comprise the triad of stakeholders who are voting

members to approve software acquisition under the validated IS requirements documents (JROC, 2013).

In order to rapidly field capabilities in an agile manner, MCISRE should seek to adapt iterative and rapid approach to requirements. To achieve a rapid requirements process, IID should produce an AI IS ICD. Approval of an AI IS ICD by the JROC would enable MCISRE to execute the aforementioned spiral development approach in rapid sequence by approving AI software requirements internally, avoiding bureaucratic delays associated with traditional JCIDS requirements approaches.

4. Establish Open Architecture to Expedite AI Integration

The MCISRE 2015–2020 plan identified a need to utilize open architecture (OA) across its portfolio of programs (MCISRE, 2014). The first step in achieving this stated goal is the development of an OA strategy. A comprehensive OA strategy enables the commoditization of capabilities across multiple systems by developing established government managed product lines (Pace, 2019). These product lines identify common requirements and establish reuse of common capabilities across various programs (Pace, 2019). In other words, product lines get away from developing capabilities from scratch and instead use an open architecture approach to build out from a common set of shared functional capabilities. This approach increases affordability and decreases development time.

A good example to illustrate OA is the Army's Future Airborne Capability Environment (FACE). Regardless of type, military aircraft share numerous capabilities. They all have to navigate, communicate, and provide situational awareness (Taylor, 2017). Under the traditional approach, capabilities were developed in isolation for each platform as shown in Figure 21.

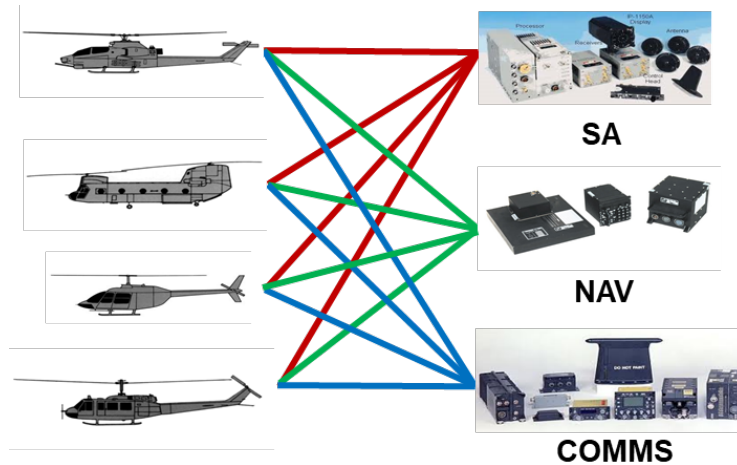


Figure 21. Traditional Development Approach. Adapted from Pace (2019).

The process to develop these similar functional capabilities was redundant, costly, and time consuming. Each new software block required 18–33 months to develop, test, and integrate (Pace, 2019). In order to improve the development method, the Army teamed up with The Open Group to develop an OA approach using FACE. With FACE, the Army was able to perform a functional decomposition of common airframe requirements and adopt a set of OA standards shown in Figure 22. The approach produced an unprecedented reuse of software components across multiple platforms which enabled faster integration and delivery of capability (Pace, 2019).



Figure 22. FACE OA Development Approach. Source: Pace (2019).

Currently, MCISRE manages its data discoverability through its DCGS-MC Program of Record (PoR). An operational view of the DCGS-MC PoR is provided in Figure 23. DCGS-MC is MCISRE's entry point to the greater DODDCGS enterprise (Concepts and Programs, 2018). It provides a DCGS Integrated Backbone (DIB) framework which is a set of standards for sharing and managing data, to which all intelligence systems must comply. The DIB framework enables interoperability by establishing meta-data tagging standards. These standards allow data to be discoverable and usable by all military services, interagency, and coalition partners (Concepts and Programs, 2018).

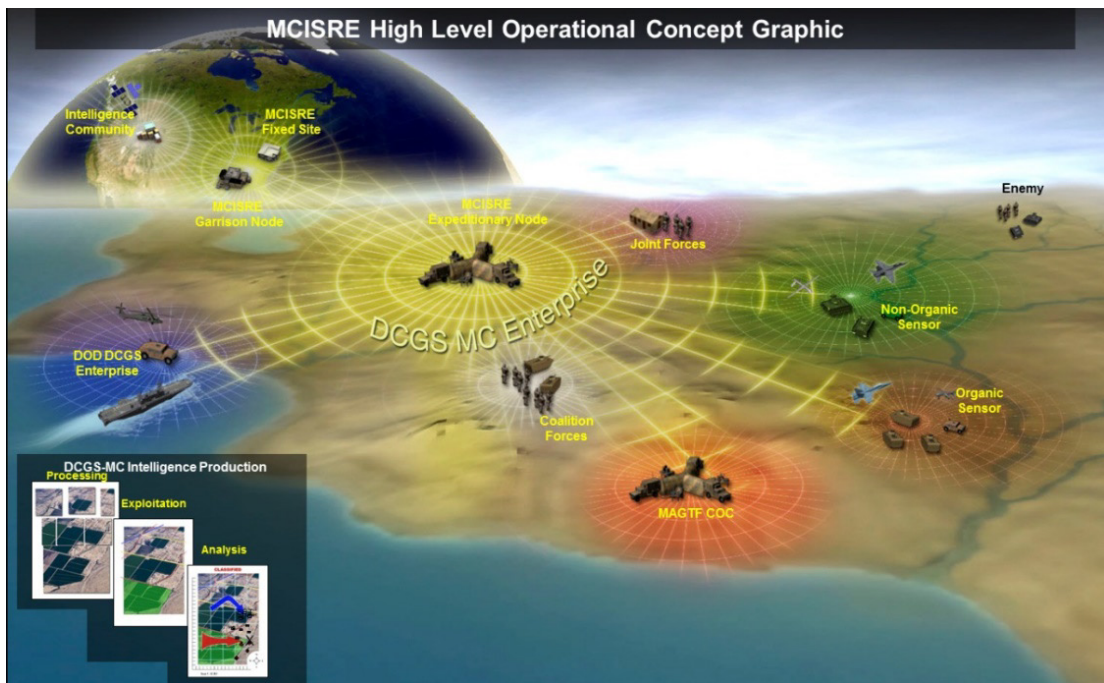


Figure 23. MCISRE Concept Graphic. Source: "DCGS-MC Sharing Information to the Tactical Edge" (2015).

While DCGS-MC provides a foundation to open the data aperture across the DoD, it requires further development to truly support OA. Jerry Mamrol, director of ISR systems at Lockheed Martin, stated

The DIB took an important step toward an open architecture by providing a standardized method to query and access finished intel product data. This

provided some degree of openness by enabling interoperability and sharing of finished products between the services via the DDF. For the architecture to be fully open, it also needs a standardized, common infrastructure that allows applications to be developed and ‘plugged in’ by different providers. (Alderton, 2017)

Vice President of Booz Allen Hamilton’s Strategic Innovation Group, Ralph Wade, believes what is missing is a common Information Technology (IT) platform. This common platform would serve as a common ISR IT platform that the Marine Corps could build out with applications and services similarly to Apple’s iOS (Alderton, 2017).

DCGS-MC is MCISRE’s iOS. As such, MCISRE should approach AI integration just as Apple does with apps or the Army did with FACE. Apple does not develop a completely new IT platform to enable integration of an app. It has a standard interface which apps build and link into. The Army moved away from developing unique platform capabilities when it determined it could build out from common hardware and software approaches. MCISRE’s approach to AI should not be any different. DCGS-MC should serve as the launch point for a MCISRE OA product line and AI should be built in as a functional component to enable other programs to tie in.

5. Shift Processing, Exploitation, and Dissemination to Point of Collection

The National Defense Strategy highlights the need to advance technological capabilities to maintain the decisive edge in an increasingly contested and denied combat environment. As stated by former Secretary of Defense Mattis, “for decades the United States has enjoyed uncontested or dominant superiority in every operating domain...Today, every domain is contested—air, land, sea, space, and cyberspace” (Mattis, 2018). State actors such as China and Russia continue to pose a threat, as their technological advances diminish the gap in dominance the U.S. has historically kept. To address this concern and excel in the likely environment where communications are denied or degraded, MCISRE must focus on obtaining material solutions that implement Processing, Exploitation, and Dissemination (PED) as close to the point of collection as possible.

The Defense Systems Information Analysis Center defines PED as “the transformation of raw collected data into usable information distributed for further analysis and/or use as combat information by commanders and staff” (DSIAC, 2015). In the vast majority of current intelligence processes, PED is conducted post-collection and after transmittal of the raw data or information from a sensor to the intelligence consumer. This transmission of raw data requires significant bandwidth that should not be assumed as readily available either due to friendly force constraints or the variable threat environment. Implementing sensors capable of conducting initial PED will drastically enhance effectiveness in limited bandwidth environments.

MCISRE should focus on sourcing sensors that provide computer vision technologies, specifically in the GEOINT realm of collection. Computer vision uses algorithmic solutions to automate extraction and analysis of relevant information to achieve near-real time visual understanding (BMVA, n.d.). With a provided feedback loop from an analyst and time spent on the front end teaching an algorithm to function in a specific way, computer vision enables autonomous detection, tracking, and alerting. This will allow a collection platform to conduct initial PED on board its system and only transmit immediately relevant data. Post-mission, the remaining data can be offloaded for further exploitation and analysis. Placing PED at the point of collection makes the platform significantly more effective in a communication degraded or denied environment with a near peer threat. It will also play a role in diminishing the effects of the electromagnetic spectrum and bolstering signature management, a critical aspect of maintaining dominance in future fights.

Collection platforms with on-board sensor processing also support the fundamental principles of Activity Based Intelligence (ABI). One of ABI’s main pillars required to effectively execute its methodologies is for all data to be geo-referenced for discoverability. In other words, all data must be spatially and temporally tagged in order to be searchable, findable, and easily usable for analysis. Sourcing collection platforms that employ sensors with capabilities such as computer vision will allow data to be immediately tagged upon collection prior to transmittal to intelligence consumers and further promote ABI methodologies.

PED at the point of collection has tactical implications as well. On board detection, classification, and identification creates real-time operational sensors. Real-time PED supports optimal tasking and re-tasking of sensors, providing increased on-the-ground situational awareness which will save lives. A focus to advance solutions that place PED at the point of collection is imperative for MCISRE to hold its leading edge and protect its forces.

6. Develop and Employ Systems that Provide Explainable AI

Technology is only effective if it is integrated and utilized. One of the biggest hurdles to integrating AI across MCISRE will be acceptance of new technology which produces changes to already adopted analytical processes. The acceptance or rejection of information systems (IS) technology is explained in Fred Davis' Technology Acceptance Model shown in Figure 24.

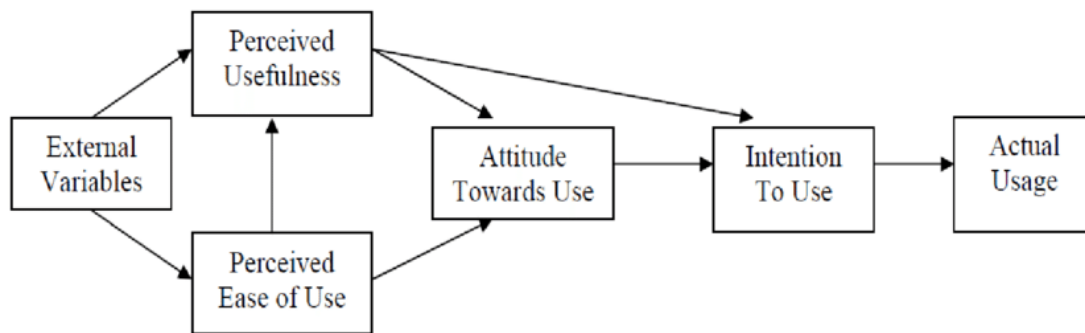


Figure 24. Technology Acceptance Model. Source: Lai (2017).

In simple terms, the model details the perceived usefulness and perceived ease of use as the major factors in determining actual usage of an IS system. The perceived usefulness of AI is an easy objective to achieve. AI is integrated into many aspects of everyday life and its benefits are easily relatable to analysts. The perceived ease of use is something that must be accounted for by lowering the complexity of systems as outlined in recommendations provided under the training pillar of this chapter. The attitudes towards

use and intention to use are areas that MCISRE must also focus on. These factors can be assisted through implementing AI solutions that employ explainable AI (XAI).

Trust in AI to sort large amounts of data and produce outputs better than a human is something that will be built over time as the human-machine team relationship expands. To build upon this trust, the human part of the team must be able to understand how the algorithm(s) work and why they produce given outputs. Furthermore, once trust in the AI system to produce proper output is gained, intelligence professionals will still require justification for a given analysis before presenting findings to decision makers. In the intelligence field, decisions must be supported with an explanation. No intelligence professional would feel comfortable briefing leadership only having the justification of “because the machine said so.”

This issue is currently being addressed through the Defense Advanced Research Projects Agency’s (DARPA) Explainable AI (XAI) initiative. XAI enables humans to understand, trust, and manage their machine counterparts (Gunning, 2019). DARPA’s goal with XAI is to produce more explainable models which provide human users the algorithm’s rationale, enabling understanding and trust in the emerging generation of AI machine partners (Gunning, 2019). The effort employs computer interfaces into the AI process which translate models into understandable and useful explanation dialogues for the end user as shown in Figure 25.

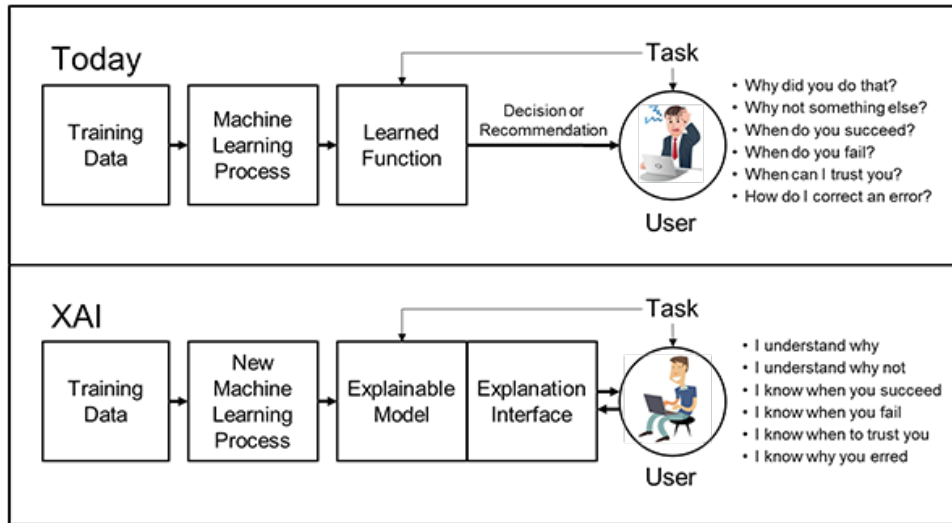


Figure 25. Traditional AI vs. Explainable AI. Source: Gunning (2019).

MCISRE should implement AI tools which provide context and reasoning to the end user. Collaboration with DARPA on the current XAI initiative offers MCISRE an outlet to capitalize on research already being conducted and funded. Failure to employ AI systems that are open and transparent will be met with friction and limit the effectiveness of the technology across the Enterprise.

7. Develop Cross Domain Solutions

One final material area requiring Enterprise attention is that of cross domain data parsing. Many Enterprise sources are received at the SCI classification level, yet to best employ various AI algorithms, SCI data must be combined with GENSER SECRET data. It is possible to easily import SECRET data into an SCI enclave for analysis and AI use, but often the users who need the results are only cleared to SECRET. Devices, such as Radiant Mercury, do allow data to be parsed so that the SECRET data is partitioned out from the AI answers derived from the SCI enclave. However, they are time consuming to use, requiring elaborate approval chains, and frustrate users. If the Enterprise is going to more frequently merge different classifications of data sets to enable better use of AI, then it needs tools to immediately and easily parse out lower classified, but useful findings, to operators cleared only to SECRET.

F. LEADERSHIP AND EDUCATION

Leadership and education analysis is the examination of how MCSIRE prepares its leaders to integrate, support, and execute AI from squad leader to the general officer ranks. The key consideration with AI is determining if leadership understands the scope of the problem and is approaching the solution in the right manner. From field research conducted, senior leadership in the Marine Corps understands the value of AI and is aggressively seeking integration of capabilities to solve complex problem sets. The issue discovered during the course of this research is the lack of a coordinated approach resulting in disparate efforts failing to capitalize on mutually beneficial research.

1. Joint Approach to AI Integration

The 2018 National Defense Strategy (NDS) detailed how capabilities such as AI will fundamentally change the character of war (Mattis, 2018). The NDS outlined an intent to invest in and develop emerging capabilities which support advanced computing, big data analytics, and artificial intelligence to ensure the nation is able to fight and win in modern warfare (Mattis, 2018). In response to the NDS, the Deputy Secretary of Defense (DepSecDef) issued a memorandum in June 2018 directing the DoD Chief Information Officer (CIO) to establish a Joint Artificial Intelligence Center (JAIC) (DepSecDef, 2018). The overarching goal of the JAIC is “accelerating the delivery of AI-enabled capabilities, scaling the Department wide impact of AI and synchronizing DoD AI activities” (DepSecDef, 2018). For MCISRE, a key component of the goal is synchronization of DoD AI activities. As the Enterprise continues to evaluate implementation AI across its PoRs, it should do so through coordination with the JAIC, not only because of the DepSecDef directive, but more importantly, the enormous benefits an integrated approach affords. Benefits from a joint approach include funding for AI developmental efforts, access to academia and research outside the direct purview of MCISRE, and prevention of redundant developmental and integration efforts.

The JAIC has significant financial resources MCISRE can leverage. In FY19, the JAIC received \$89 million with a projected increase to \$208 million in President Trump’s FY20 budget proposal (Mitchell, 2019). The DepSecDef memorandum directed the

services to coordinate with the JAIC on any AI efforts totaling more than \$15 million in order to ensure Department-wide advantages (DepSecDef, 2018). As MCISRE seeks to implement an AI strategy for development and integration, it should tap into the financial resources the JAIC offers. Every dollar saved through the coordinated approach is funding which can be applied elsewhere across MCISRE.

In FY20, the JAIC will possess a dedicated consortium of 58 General Schedule (GS) employees (Kojac, 2019). These employees who are focusing solely on AI across the DoD will have countless other points of contact working various projects. MCISRE faces daily challenges spanning its entire spectrum of capabilities. AI, although hugely important and at the forefront of many efforts, is just one of many issues being worked. Tapping into the JAIC offers the potential to offload some of the workload to resident experts.

Lastly, approaching AI integration through the JAIC will prevent redundant developmental efforts. At the MCWL AI cross levelling summit, eleven organizations presented AI efforts spanning various sectors ranging from manpower to logistics to intelligence. Although eleven presented, dozens of other organizations and efforts were not represented, but are still funding AI development. The key takeaway from the summit was AI is being applied across all warfighting functions and many organizations within the Marine Corps, but not in a synchronized fashion. The efforts presented at the summit contained similar functional capabilities which should be developed in a synchronized approach.

MCISRE must approach AI integration in a joint manner if it wants an enduring and integrated capability with maximized benefits. Aligning efforts with the JAIC enables MCISRE to tap into funding and personnel resources as well as capitalize on current development efforts. It also ensures AI capability implemented across MCISRE is synchronized with broader DoD capabilities to enhance mission effectiveness for intelligence analysts.

G. PERSONNEL

Analysis of personnel involves the evaluation of available people to execute MCISRE functions with AI support. This evaluation looks at how existing task

organizations (T/O) may change as well as identifies what new personnel capabilities must be developed to support AI. AI is not a single purchase fire and forget weapon that can be added to the MCISRE arsenal. The introduction of innovative technology will incur personnel costs to support its management. From a cost savings viewpoint, AI increases efficiency, reducing the number of analysts required to execute mission essential tasks. A key takeaway from this section is the recommendation that any efficiency-based personnel reduction decisions be made following implementation of AI. T/O reductions must be informed with proper and sufficient data and acting prematurely brings unnecessary risk to the Enterprise.

1. Evaluate the Task Organization of Intelligence Units across MCISRE

If AI tools, which possess the ability to outpace human ability to analyze big data, are implemented across MCISRE, is there a need for analysts within the intelligence production loop? This is the same argument made with the future of pilots as capabilities move towards remote based platforms. However, the nation's adversaries are not binary, they are fluid and algorithms should not determine final intelligence analysis. Traditional estimates support an 80% to 20% machine to human in the loop mixture (Schrage, 2017). However, with continual advancements in algorithms, humans are being phased out in many industries with analytically aggressive firms decreasing human interaction to as low as 5% (Schrage, 2017). The machine only mindset works in certain data stagnant industries, but not in intelligence where collection and analysis involve fluidity. A thinking enemy will always require a human-in-the-loop to interpret big data. If the analyst, with their implicit knowledge of the enemy, does not agree with the output of an algorithm, they must present that view along with their reasoning. In cases where there is complete divergence, presenting two assessments, one from AI and one from the analyst will only bolster the information presented to decision makers.

While human in the loop will remain a standing requirement, the potential efficiency gain AI offers presents an opportunity for reduction in the task organization (T/O) of analysts across the Enterprise. Some of this reduction will end up serving as a repurpose of manpower to support the data management requirements for AI. Other

reductions in personnel could result in manpower savings for the Marine Corps. The decision to make any T/O changes to intelligence units is a major determination with significant risk, especially in the early stages of the human-machine teaming process. It is recommended that any evaluation of T/O adjustment be conducted post AI implementation with sufficient data to support the proper course of action recommendation. Following sufficient implementation of AI capabilities, MCISRE should conduct a manpower assessment and work with Manpower and Reserve Affairs (M&RA) to submit a manpower Table of Organization and Equipment Change Request (TOECR) to properly set the T/O required to support analytical tasks in a post AI implementation Enterprise.

2. Create Structure to Support Data Management across the Marine Corps

Successful implementation of AI starts with data and how it is managed. AI solutions are not humans, they are nothing more than code which is developed and trained to empower future autonomous expansion in capability. In order to achieve success in AI, the algorithms must be supported and managed by trained data professionals. These data professionals are referred to as data engineers and data scientists.

Data engineers develop the infrastructure to enable exploitation of big data by data scientists (Aghabozorgi, 2016). They are software engineers who develop, construct, test and maintain the architecture (Willems, 2017). In the case of MCISRE, data engineers would be those responsible for ensuring data ingest across all collection platforms is stored and organized in an ontological format which is discoverable and usable by data scientists.

Data scientists use the architecture developed by data engineers to conduct analysis using ML and AI tools to turn raw data into insightful information (Willems, 2017). In other words, they use AI algorithms to turn big data information into intelligence. This involves developing and managing AI algorithms critical to the process. A comparison of responsibilities between data engineers and scientists is depicted in Figure 26.



Figure 26. Data Scientist vs. Data Engineer. Source: Willems (2017).

As noted in the previous recommendation, adopting and implementing AI tools will increase the efficiency and productivity of the intelligence analyst. As such, it is anticipated that MCISRE will be able to reduce the number of analysts needed to perform required tasks. Rather than looking at this reduction as a savings, MCISRE should view the situation as a transfer from one tradecraft to another. Reduction in required T/O for intelligence analysts should be reinvested in the establishment of data management professionals.

MCISRE is already addressing the data management challenge through establishing a new intelligence discipline, DATINT, which is outlined in the concept Data Intelligence: Marine Corps Concept for “Making Sense” (HQMC, 2018). Although still in draft form at the time of this writing, the concept defines the discipline as

DATINT as tradecraft requires an amalgamation of Data Science skills, such as Data Analytics and Data Engineering, combined with Knowledge and Information Management. It provides the quantitative analysis of collection resources, evaluation of dissemination methods, and introduces a form of automated intelligence production referred to as intelligence on demand services, and again, whose data is geospatially and temporally referenced to the warfighter. Successful DATINT requires a comprehensive

analysis of our systems, networks, and technology. It must also identify how, and in what areas, data refinements can improve the efficiency of the information environment. (HQMC, 2018)

To support implementation of the concept, MCISRE is seeking to establish three new military occupational specialties:

- 2652 Intelligence Data Engineer
- 2653 Intelligence Software/Security Engineer
- 2659 Intelligence Technology and Data Chief

The current MCISRE formula for developing data engineers and scientists is a great first step. Training Marines to a MOS standard without work experience in their tradecraft, however, does not provide the optimal solution. This approach places unnecessary risk on the institution as it builds out an ontological data management structure for its entire repository. Skills taught at entry level data engineering courses are a launching point, but industry experience in the field of data engineering is critical to accomplishing large organizational projects involving big data. As such, MCISRE should evaluate the benefit of outsourcing its initial build of the ontological architecture then transition to sustainment using its newly established MOS skillsets.

MCISRE must also determine the proper business model approach to effective sustainment and continued development of the aforementioned MOS skills. Under the traditional approach, Marines transition to new billets every three years. Sometimes those billets are within their MOS, but sometimes they are not. If MCISRE is going to invest heavily in the development of data engineering and data science skillsets, it should evaluate its talent management approach to ensure those Marines remain within their MOS to continue to gain proficiency. The institution must also identify ways to retain the highly specialized individuals within the institution. Data management skillsets are in high demand in the civilian sector, but MCISRE will rely upon retention to grow its capability. Lastly, as MCISRE seeks to develop the training curriculum for its data scientists and engineers, it should reach out to universities who offer specialized courses in the fields.

Naval Postgraduate School is one opportunity that exists to support the temporary training solution. Ultimately, the Marine Corps needs to provide internal training at MOS producing schoolhouses run by the service, but the utilization of existing programs in other universities provides a gap filler in the interim.

Looking at the data management more holistically, MCISRE's approach demonstrates the Enterprise's understanding of manpower requirements and skillsets required to manage data as the backbone of AI. This approach, however, should not be driven solely by MCISRE. The Marine Corps is implementing AI across all of its warfighting functions and the need to provide a data management capability is a service wide problem, not just an intelligence problem. The Marine Corps should develop a data management capability to replace MCISRE's DATINT proposal. The utilization of data management Marines in the data science and engineering fields should be supported by training and T/O across the service, not pulled from MCISRE.

H. FACILITIES

Facilities examines the military property, installations and industrial facilities required to support AI (DAU, 2018). Throughout the course of this research, no requirements for adjustment to facilities were identified. This is largely due to AI being a software-based capability which doesn't require large storage space. The single issue that may cause an increase in required facilities space is data storage. Implementation of AI should seek to integrate a larger volume of data across the internet of things (IoT). This includes a heavier emphasis on open source intelligence such as that found in social media. Although the volume of data should increase to support AI, employment of cloud storage prevents a corresponding increase in facilities space.

I. POLICY

Policy is the identification of any DoD policy issues that may prevent effective implementation of AI (DAU, 2018). To scope the overarching definition in support of this thesis, policy will be defined as aspects which MCISRE should develop sub-strategies on in support of a larger AI strategy. The recommendations in this section all revolve around and have a specific focus on data.

1. Develop a Cloud Strategy in Coordination with JAIC

MCISRE can improve its data discoverability limitations through the use of cloud computing. Traditional methods of storing data on server stacks is not a sustainable business model to support data availability and discoverability across a globally distributed environment. This point was driven home by the Marine Corps Director of Intelligence's POM 21 Guidance which directed MCISRE to operationalize intelligence cloud services by leveraging naval and DoD clouds.

The National Institute of Standards and Technology defines cloud computing as “a model for enabling on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort” (NIST, 2018). The 2017 Marine Corps Strategy for Assured Command and Control outlines the requirement for the Marine Corps to move to a cloud service concept of employment

Cloud services are needed to move applications and associated data to the point of need. Old “reach-back” models are too slow and are most susceptible to service outages during times of network segregation, especially at the tactical edge. Cloud services also are a crucial component to our mobility strategy both in warfighting and business (e.g., recruiting) operations. Finally, the cloud and our tactical services-oriented architecture enables our budding Ready Data Environment (RDE) by creating secure and accessible repositories to share information. (USMC, 2017)

Cloud computing is comprised of three main delivery models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (DoD ESI, 2018). A snapshot of the services delivered by each model is provided in Figure 27.

SaaS stores and manages applications via a central location and delivers them to end users via the internet. A third-party vendor installs and manages the software, reducing time and money spent by the customer (Watts, 2017). The disadvantage and risk of employing SaaS is the end user has limited ability to oversee software management and accreditation. Another critical consideration when looking at SaaS is operating in an internet denied environment. If the end user is unable to connect to the third-party site, they have no ability to access any of the applications hosted by the third-party vendor.

PaaS operates similar to SaaS in that it provides the customer a platform for software creation. The customer is then able to develop their own customizable applications to operate on the established framework (Watts, 2017). The advantages of PaaS are application development simplicity and cost-effectiveness, automation of business policy, reduction in the amount of coding required by developers, and reduction in time spent maintaining the software. For MCISRE, PaaS would ensure applications developed across the Enterprise adhere to a common framework to enable data discoverability.

IaaS provides automated and scalable computing services in addition to the aforementioned SaaS and PaaS capabilities (Colman, 2013). IaaS customers have direct access to their servers and storage and can build a “virtual data center” in the cloud without having to invest in the maintenance and management (Colman, 2013). For large organization such as MCISRE, two major advantages of IaaS are security and cost effectiveness. IaaS supports security by maintaining full control over the development of applications and infrastructures. Cost-effectiveness is achieved by enabling the consumer to only procure the amount of storage and server capacity that is consumed (Watts, 2017).

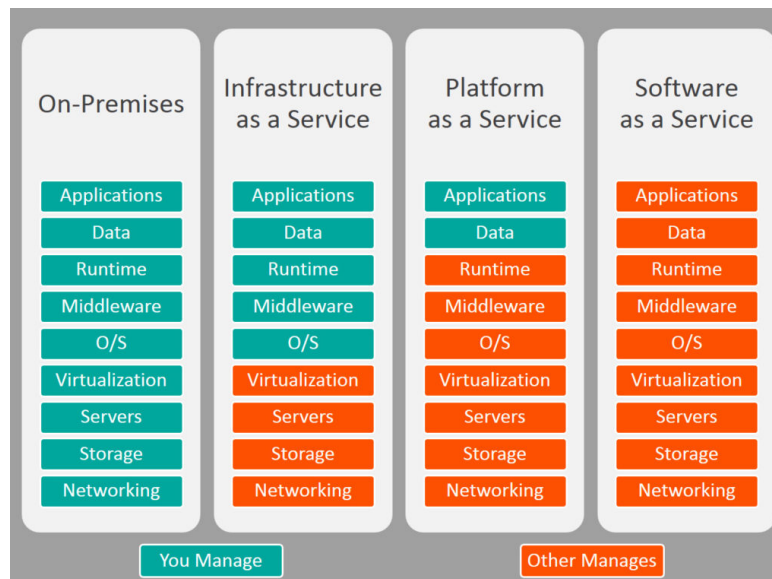


Figure 27. Cloud Computing Delivery Models. Source: Watts (2017).

When looking at cloud computing and its delivery models, there are several important considerations to consider. First, as identified above, reliance on cloud computing puts intelligence functions at risk when operating in a limited or denied communications environment. If MCISRE is solely reliant on internet connection to access its applications, cloud computing poses significant risk. The same issues exist with current business practices and capabilities using DCGS-MC which also requires connection to enable its applications to access data across the Enterprise. Secondly, cloud computing's nature of out-sourcing management of enterprise capabilities raises the risk of cyber security. As capabilities are out-sourced, MCISRE puts at risk its ability to maintain control and oversight of cyber security for its data and applications. Still, there are many monetary, time, and access advantages to moving towards a cloud framework.

MCISRE AI will be reliant upon access to data both within and outside the Enterprise. When developing a MCISRE cloud strategy, the Enterprise should work in conjunction with the existing cloud efforts being funded by the Joint Artificial Intelligence Center (JAIC). The JAIC is working towards a common foundation cloud environment which users across the DoD can access through their respective portals (Kojac, 2019). One of the funded efforts to support the common foundation is the Joint Enterprise Defense Infrastructure (JEDI) program. The program spawned from a 2017 memorandum from the Deputy Secretary of Defense which directed the expedited delivery of a DoD wide cloud computing system (Peters, 2018). It is currently funded at \$10 billion across the next 10 years (Williams, 2018). The key point for MCISRE is not to simply adopt whatever JEDI becomes, but rather to work with the JAIC on developing a MCISRE cloud strategy which leverages efforts and funding across the broader DoD. The JAIC tie in could be viewed as a macro cloud strategy while still enabling MCISRE to develop a micro approach on specific SaaS, PaaS, and IaaS capabilities unique to the Enterprise. This approach will save considerable financial and time resources while still enabling MCISRE flexibility in its Enterprise design for cloud computing.

2. Employ Edge Computing in Concert with Cloud Computing

As noted in Chapter II, commercial industry AI applications rely upon a high level of connectivity and large bandwidth support. MCISRE, however, operates in remote locations with limited bandwidth. One way to overcome this issue is through the use of edge, or fog, computing. Edge computing moves computing and storage resources away from a geographically separated cloud to the edge of the network close to end devices (PremSankar, Di Francesco and Taleb, 2018). In addition to reducing bandwidth requirements, the use of edge computing can also serve to reduce risk from enemy denial of communications. If a cloud computing strategy tied to a single node located within the U.S. is adopted, any denial or disruption of that node affects the entire Enterprise. Employing edge processing with a node approach reduces the risk by creating dispersed local data collection points.

The major advantages of edge computing are speed, security, scalability, and reliability (Gyarmathy, 2018).

- **Speed** – The most important benefit provided by edge computing is a reduction in data latency. While data latency may not be as big an issue for a CONUS based unit, the same cannot be said of a deployed one. Bandwidth limitations experienced on a ship or in a communications contested environment are only further exasperated if the data has to be requested and then disseminated from a geographically dispersed location. Aside from the distance traveled, the dissemination from a centralized location requires the use of several router hops in route to its final destination. Housing and processing data closer to the end user reduces the transmittal distance, expediting the dissemination of time critical information (Gyarmathy, 2018).
- **Security** – In addition to reducing latency, the use of edge computing can also serve to reduce risk from enemy denial of communications. Traditional centralized cloud computing tied to a single node presents an opportune target for an enemy Distributed Denial of Service (DDoS)

attack (Gyarmathy, 2018). Any denial or disruption of that node affects the entire Enterprise. Edge computing's employment of multiple clouds, however, protects the network by prohibiting a single targeted DDoS attack from disrupting the entire Enterprise.

- Scalability – Housing data at a centralized storage center such as MCIA is expensive and can limit future expansion requirements. Limiting data storage facilities to confined structures restricts an organization's ability to support future expansion requirements (Gyarmathy, 2018). Edge computing provides a more fiscally advantageous model that allows for additive capability using a combination of data repositories (Gyarmathy, 2018).
- Reliability – The security benefits provided by edge computing also produce an increase in reliability. With a single cloud concept, system failure of the node results in catastrophic effects across the organization. Edge computing overcomes this issue by providing a capability for alternative nodes to subsume the workload of a failed node(s) (Gyarmathy, 2018).

The concept of edge computing is already being developed by the Navy through its Naval Tactical Cloud (NTC) program. The NTC is an implementation of big data tactical cloud services at the tactical edge (Kamel, 2019). NTC employs IT efficiency clouds at large data centers operating on high bandwidth networks and complements them with IT performance clouds located at the tactical edge operating on tactical RF networks (Kamel, 2019). The aforementioned advantages of speed, security, reliability, and scalability are all by-products of the NTC effort. MCISRE should investigate advantages of implementing the NTC, or similar capability, across its Enterprise.

3. Develop a Data Storage Plan

MCISRE must develop policy for storing data. The policy must address data retention as well as what storage approach MCISRE wants to adopt. All data is not equal

in the intelligence field and AI will require data from across the IoT. This includes structured data from DoD collection systems and unstructured data from open source systems such as social media. Determining what data to house in a cloud repository and for how long is an important determination.

Once data retention is determined, the manner in which it is stored is the next step. There are two main storage approaches which can be adopted to enable data to be searchable and discoverable across the Enterprise. The first approach is keeping the data in its unstructured format and placing it in a “data lake” (Seltser, 2018). With the data lake approach, collected information is stored in its original form, requiring no additional time or financial resources to convert it to a structured format. The data is then pulled from its storage location on an as needed basis (Seltser, 2018). The disadvantage of using the data lake approach is every time the storage database is queried, the algorithm must sort through large amounts of data costing valuable time. The second approach is employing data engineers to develop an ontologically formatted knowledge base. The ontological approach converts data to a structured format up front by breaking it into objects, categories, relations, and attributes. This approach speeds up the process for searching data but it also has inherent upfront costs.

A comparison of data lake versus structured ontological storage can be clearly illustrated using grocery shopping as an example (Seltser, 2018). The data lake approach would be similar to an individual buying only a few required groceries at a time. The structured format storage approach would be equivalent to an individual developing a shopping list to buy all required groceries and then taking them home, unpacking, and storing them where they can be easily found at a later time. The individual who chooses to buy many groceries at once and then unpack them for future use must invest more upfront time and financial resources than the individual who buys items as needed from the store. However, over the long run, the individual saves time compared to the one who buys only a few items and must maneuver the entire grocery store to find items every time they want to make a meal.

As MCISRE evaluates its method for storing data, a combination approach may suit it best. Data collected from sensors should be delivered in a structured approach,

making employment of an ontology knowledge base easy to accomplish. The remaining IoT unstructured data could be prioritized with the most important seeing investment up front in the ontology approach and the lower importance, or least searchable, may be best to leave in an unstructured format. Regardless of the method decided upon, data retention and storage policy are items which must be addressed in a MCISRE data strategy.

4. Develop Policy to Implement Enterprise Wide Cross Domain Solutions

In concert with the recommendation to develop better cross domain solution devices noted in the Materiel section of this chapter, one of the priority actions from the National Security Strategy is reduction of information sharing barriers such as speed and classification levels (Trump, 2017). This priority action comes at a vital time with the aggressive approach to AI integration across the DoD as outlined in the DoD AI Strategy. In support of the broader NSS and DoD AI Strategy as well as a MCISRE AI strategy, implementing autonomous solutions to enable data fusion across all classification levels is vital.

As previously examined, the historical and current process of multi-INT fusion is cumbersome, slow, and challenging. The ability to execute ABI is non-existent under current constructs. Changing the intelligence cycle will shift the approach, but if data remains stagnant within siloed databases, ABI will remain unachievable and AI will be limited in its capability. An example of this is SIGINT. SIGINT operates on the NSA network. Only after it is processed and approved for dissemination at lower levels via tear lines can it be integrated. The same issue arises with CI/HUMINT reporting. Reports are submitted and after considerable time tear line information is released for inclusion in all source analysis.

To fix issues of multi-INT fusion that will be detrimental to AI, MCISRE must integrate cross domain solutions (CDS) into its portfolio of programs. Cross domain solutions manage secure data transfers between DoD's three clearance levels – Top Secret, Secret, and Unclassified (Kamis, 2019). Defense Information Systems Agency (DISA) provides CDS on behalf of the DoD by fielding capabilities under the Chairman Joint

Chiefs of Staff Instruction (CJCSI) 6211.02D (DISA, 2019). This is done by utilizing a net-centric, service-oriented CDS approach to support users across the Defense Information Network (DODIN) (DISA, 2019).

CDS solutions exist and the support to integrate them is established through DISA. It is recommended that MCISRE work with Deputy Commandant for Information (DC I), DISA and the NSA to develop certified CDS capabilities in conjunction with development of policy to support it.

J. CHAPTER SUMMARY

In this chapter, the authors synthesized information from the literature review and field research into an end-to-end analysis of DOTMLPF-P recommendations to assist MCSIRE with AI integration moving forward. As stated in the chapter introduction, the recommendations provided are designed to support long term AI strategy decisions. These recommendations are enabling conditions to support the variety of algorithmic solutions that will inevitably be developed and procured in support of the Marine Corp's intelligence warfighting organization. The complete list of recommendations is provided in a consolidated format in the Appendix. Some recommendations require further in-depth analysis before decisions are able to be made across the Enterprise. These areas, which were introduced broadly as aspects for consideration, could serve the basis of future thesis work and will be addressed in the following chapter.

V. CONCLUSIONS AND RECOMMENDATIONS

This thesis provided AI strategy recommendations across the Doctrine, Organization, Training, Materiel, Leadership/Education, Personnel, Facilities, and Policy (DOTMLPF-F) spectrum. The primary customer was the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE), but the final recommendations are applicable across the entire Department of Defense (DoD). The authors approached this thesis by conducting a thorough review of relevant literature on AI and machine learning (ML) combined with field research, then applied that background to MCISRE to provide final DOTMLPF-P recommendations. This chapter details research conclusions by organizing recommendations from Chapter IV into a composite of six core themes MCISRE must focus on displayed in Figure 28. The chapter concludes with recommendations for future research in support of MCISRE application of AI.

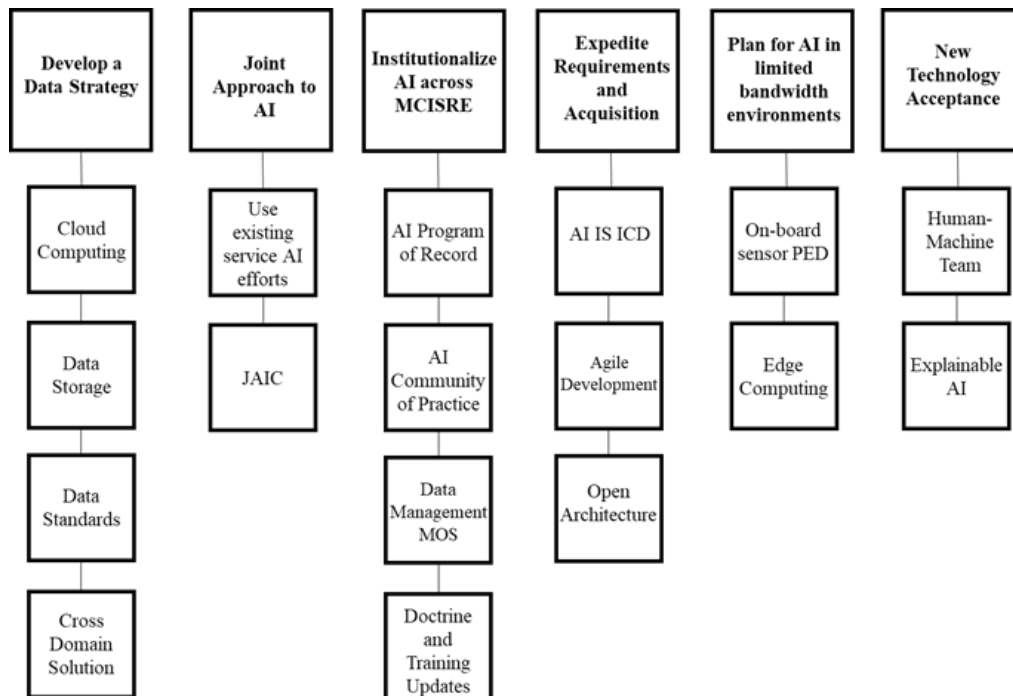


Figure 28. MCISRE AI Core Themes

A. RESEARCH CONCLUSIONS

1. Make Data the Central Focus through Development of a Data Strategy

Application of AI across MCISRE revolves around the data. A lack of volume as well as veracity of data renders algorithms inept. The vitality of data to AI necessitates development of a comprehensive data strategy. One of the central components to the strategy is determining how MCISRE will employ cloud computing to manage data storage, accessibility, and discoverability across the Enterprise. The cloud computing approach can be supported through internal development or outsourcing support using Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). Whatever approach is identified, it should account for management of security risks and life cycle costs.

In addition to cloud computing, the data strategy should identify a data storage plan to address retention and storage. All data is not equal in the intelligence field. AI will require data from across the internet of things, including structured data from DoD collection systems and semi-structured data from open source datasets such as social media. MCISRE's determination of what data to house in a cloud repository and for how long is a critical aspect of its data strategy. For data storage, MCISRE must choose between using an approach that supports structured ontological parsing up front or an unstructured data lake approach. The decision on storage should be informed by cost analysis and operational requirements for accessibility timeliness.

Following determination of data storage, the data strategy must identify common standards to support an open data ecosystem. These standards span analytic, interpretability, technical, and data. Articulation of common standards supports veracity of data to prevent biased outputs, a means for system performance evaluation and explainability, and data discoverability across the Enterprise. MCISRE should work with the Joint Artificial Intelligence Center (JAIC) which is leading the effort to consolidate databases from within the DoD as well as outside organizations into a common cloud environment while also tackling the issues of data compatibility.

Lastly, the volume of data accessible to AI solutions is limited by the access that algorithms have across security classification levels. A MCISRE data strategy must address policy changes required to enable cross domain solutions (CDS). CDS represents both a materiel capability and policy change. Failure to address the gap in ability to conduct cross domain data parsing would marginalize the data strategy.

2. Approach AI Integration in a Joint Manner

Dozens of AI efforts are funded across MCISRE, the Marine Corps, and the DoD. Each effort was initiated from an identified opportunity to develop and apply AI to provide an optimal solution to a given problem set. These individualized efforts share many common characteristics and possess the ability for broader application. As MCISRE seeks AI solutions to integrate across its portfolio of programs, it should first seek to capitalize on existing research and development. The JAIC is a great starting point to identify areas of commonality and prevent redundancy. Aligning efforts with the JAIC enables MCISRE to tap into funding and personnel resources as well as capitalize on current development efforts to expedite timeliness of its AI development and integration. It also ensures AI capability implemented across MCISRE is synchronized with DoD capabilities to enhance mission effectiveness for intelligence analysts. A prudent MCISRE approach necessitates up front due diligence to explore opportunities for joint alignment of efforts.

3. Institutionalize AI across MCISRE

Investment in AI should be viewed as an enduring capability to ensure MCISRE retains its tactical advantage over adversaries in both the near and distant future. To ensure maximum capitalization of both short and long term gains, the Enterprise must codify and institutionalize AI. One way to accomplish this is through establishment of an AI program of record (PoR). A PoR would consolidate disjointed efforts into a single program. This consolidation would force formal approval of requirements documents which would enhance synchronization of efforts and support funding justification and defensibility for the total life cycle of MCISRE AI.

In addition to establishing a PoR, MCISRE should establish an AI community of practice (CoP). A CoP provides means for bottom up and top down integration and

knowledge sharing. Utilization of an AI CoP provides a feedback channel across the entire Enterprise. Since AI is a cross-functional capability, the CoP should be designed with membership representation across all intelligence disciplines.

Data management is a critical requirement for AI. MCISRE already seeks to address the gap in data management capability through establishment of a new intelligence discipline named DATINT. The approach by MCISRE articulates senior leader understanding of the complexity of the data management problem, but the approach should be broadened. Data management will support AI across the entire Marine Corps. MCISRE should coordinate with Deputy Commandant for Information (DC I) to establish a data management MOS that supports all warfighting functions, not just intelligence. MCISRE's requirement for data management is no different than a logistical one. The utilization of data management Marines in the data science and engineering fields should be supported by training and T/O across the service, not pulled from MCISRE.

The final recommendation to institutionalize AI is for MCISRE to update intelligence doctrine and training. AI fundamentally changes certain analytical approaches and processes. These changes must be captured across doctrine and supported by adjustment to training at schoolhouses. Procurement of algorithms without corresponding updates to doctrine and training does not support long term use and sustainment.

4. Requirements and Acquisition must Support the Pace of Emerging Capabilities

The Joint Capabilities Integration and Development System (JCIDS) can hinder rapid software technology development and procurement. Technology moves at a rapid pace and AI is not an exception. What is currently considered ground breaking in the field of AI, will likely be outdated two years from now. MCISRE must overcome challenges posed by traditional JCIDS requirements and acquisition processes. The Enterprise already has two Joint Requirements Oversight Council (JROC) approved information systems capabilities documents. The PISR IS-ICD and DCGS IS-CDD enable software requirements approval at levels lower than the JROC, expediting approval of rapidly evolving technologies. MCISRE should approach AI in the same manner. Development

and approval of an AI IS ICD would enable MCISRE to accelerate its requirements approval process to keep pace with emerging AI capabilities.

The AI IS ICD approach speeds up the requirements aspect of JCIDS, but the acquisition process must adjust as well. MCISRE should adopt an agile development process for AI. Employing an agile development process using an incremental and iterative approach as opposed to traditional sequential waterfall approach produces small gains in a more rapid manner. This approach enables the Enterprise to fail early and often without significant programmatic risk and funding loss. Most important, it speeds up delivery of capabilities by focusing on manageable pieces compared to traditional approaches seeking one ultimate delivery.

Utilization of open architecture (OA) provides another avenue to expedite development and integration of AI. MCISRE should develop a standard common information technology platform that allows developers to plug in AI applications. This approach is similar to Apple's iOS. If DCGS-MC is the MCISRE iOS, it should serve as the launch point for its OA product line.

5. Plan to Operate AI in Communications Degraded Environments

Commercial industries who employ AI have the luxury of a high level of connectivity and large bandwidth support. MCISRE does not have the same luxury. The Enterprise operates in remote locations with limited bandwidth. As MCISRE proceeds with its fusion of AI, it must account for and plan to operate in environments where bandwidth is limited. One consideration which may assist in this matter is conducting on board sensor processing at the point of collection. Processing collection using computer vision technology aboard sensors allows a collection platform to only transmit immediately relevant data, making it significantly more effective in a communication degraded environment. The segregation and dissemination of strictly relevant data also diminishes the electromagnetic signature between the sensor and ground station, bolstering signature management.

Another recommendation to overcome degraded communication environments is through the use of edge computing. Edge computing is a subset of cloud computing. It

moves computing and storage resources away from a single geographically separated cloud to the edge of the network. In other words, traditional cloud computing relies upon a single node, or cloud, whereas edge computing employs multiple nodes closer to the end user. The dispersion of nodes reduces bandwidth requirements since data is stored closer to the end user, requiring less hops to cover the transmittal distance. It also reduces risk from enemy denial of communications by enabling multiple nodes to provide a required service in the event one node fails.

6. Overcome Friction to Gain Acceptance of New Technology

One of the biggest hurdles facing MCISRE's AI implementation remains the actual acceptance of the technology. AI's ability to improve analytical capabilities is easily identifiable and relatable. Empirical data exists across commercial industries to support this assumption. The perceived usefulness, however, is only half of the equation to determine technological use. The perceived ease of use is the other half. Perceived ease of use not only entails the complexity of system design, but also the ability for Marines across the Enterprise to adjust the methods and processes they have been taught and utilized throughout their entire careers. The transition to AI will entail a transition from human centric processes to a human-machine team. This transition will naturally undergo learning and acceptance phases before it can enter full utilization. To expedite the process, MCISRE should establish a detailed training plan to provide guidance and use application to Marines. Demonstrating, teaching, and making the technology available will provide a bridge to establish the human-machine dynamic.

Training the human-machine trust can be supplemented through employing systems which employ explainable AI (XAI). XAI enables Marines to understand how and why a given output was reached. Fielding technology which simply provides outputs without a means to explain how they were arrived at would grow the gap in trust rather than bridge it. Analysts must be able to provide reasoning for conclusions reached. Relying upon a machine algorithm without any context will never be an acceptable solution. XAI provides the reasoning and is critical to gaining acceptance, and ultimately utilization, of AI.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

1. Full DOTMLPF-P Analysis by CD&I

This thesis conducted a DOTMLPF-P evaluation of enabling AI capabilities. The recommendations and conclusions reached fused scholarly and field research with DOTMLPF-P experience gained working in a requirements focused billet at Combat Development and Integration (CD&I). The approach by the authors represents the findings from an informal DOTMLPF-P analysis, but warrants further evaluation. A full and formal DOTMLPF-P analysis conducted by CD&I's Intelligence Integration Division (IID) is recommended. The formal approach with input across MCISRE entities may identify refinements to current findings as well as identification of additional recommendations.

2. Reduction of Manpower T/O

One of the recommendations presented in Chapter IV outlined potential for a reduction in manpower task organization (T/O) across intelligence units. Within the recommendation, the authors cautioned to resist making T/O adjustments without sufficient understanding of the AI human-machine team and corresponding data to support proper determinations. Following implementation of AI across MCISRE, research that provides detailed evaluation of analytical processes and associated manpower requirements across all intelligence units from a battalion S2 shop up to a Marine Expeditionary Force Intelligence Operations Center (MEF IOC) would support determination of proper task organization.

3. Further examination of AI human-machine teaming

Implementation of AI has the potential to fundamentally change analytical processes and analyst roles within MCISRE. AI, however, will not replace the need for a human in the loop. With the integration of new technology to assist analysts, roles and responsibilities for the human and machine will be fluid at first, taking valuable time to set into place. Research which leverages human-machine teaming aspects and considerations in the context of AI provides an opportunity to shape the relationship and avoid an extended trial and error period.

4. Examination of training requirements to support AI integration

This thesis avoided specific AI algorithmic material solutions, resulting in training recommendations presented in a broad nature focused on higher level considerations. The aforementioned human-machine team training as well as data management training will be transient across any material capability introduced. Future research should focus on discrete and detailed training recommendations which address specific requirements Marine Corps Intelligence Schools (MCIS) should consider, including an expansion of the already identified human-machine team and data management training.

APPENDIX: CONSOLIDATED DOTMLPF-P RECOMMENDATIONS

Doctrine	
Update MCWP 2-10, <i>Intelligence Operations</i>	Modify the current intelligence cycle to depict processing and exploitation as a continuous step. Reflect changes in personnel and staff sections including addition of data engineers, data scientists, and the potential establishment of a new MOS, Data Intelligence (DATINT)
Update MCTP 2-10A, <i>MAGTF Intelligence Collection</i>	Modify the current intelligence cycle to depict processing and exploitation as a continuous step. Evaluate the requirements analysis criteria to determine a need for new requirements or updates to the existing ones. With the implementation of AI, the collection criteria of validation may be unnecessary as this will occur automatically.
Update MCTP 2-10B, <i>MAGTF Intelligence Production and Analysis</i>	Modify the current intelligence cycle to depict processing and exploitation as a continuous step. Evaluate the production steps and their relation to implementation of AI and ML. Analysis will become more automated with AI/ML systems, and parsing out irrelevant information may change the filtering process with the housing of big data. Automation of the analytical process will place a greater emphasis on the feedback loop and analyst input into the accuracy and reliability of the AI system will become increasingly more important.
Organization	
Update the MCISRE Enterprise Architecture to better address AI standards	Develop a data strategy that specifies analytic, interpretability, technical, and data standards. Common established

	standards support data sharing across the Enterprise and the broader DoD, enable evaluation of AI tools, and support explainable AI.
Establish an AI Community of Practice (CoP)	Establish a cross-functional AI CoP to provide MCISRE a bottom up and top down integrated approach to share best practices, address issues, and support a unified approach to future AI developmental efforts.
Training	
Establish training to support human-machine teaming	AI solutions will overhaul human centric analytical processes, placing a greater reliance on machines. Trust in the human-machine team is key and requires development of training curriculums that detail roles and responsibilities as well as provide repetition.
Develop training to better support data annotation	Developing and training AI capabilities relies upon proper input data. Analysts are not adequately trained and do not invest enough time into employing data annotation techniques. For AI to be successful across MCISRE, a renewed focus on training analysts to properly tag and annotate data feeding into the system is required.
Materiel	
Establish an artificial intelligence program of record (PoR)	Establishing an AI PoR will consolidate developmental efforts into a single program, force development of formal requirement documents, and provide better funding justification and defensibility.
Employ an agile development process for AI capabilities	Employing an agile development process reduces programmatic risk by enabling technology development to fail early and often in the RDT&E phase without incurring significant programmatic delay or funding loss. It also enables expedited fielding since capabilities are produced in manageable pieces compared to a traditional waterfall approach delivering one final capability.

Develop an AI Information Systems (IS) Initial Capabilities Document (ICD)	JROC approval of an AI IS ICD would support rapid requirements approval for software-based capabilities, avoiding delays associated with the traditional MROC and JROC approval chain.
Establish open architecture (OA) to expedite AI integration	OA enables commoditization of capabilities across multiple systems by developing established product lines for common shared capabilities. The OA approach increases affordability and decreases development time. DCGS-MC should serve as the MCISRE OA product line with AI built in as a functional component, enabling other PoRs to tie into it.
Shift processing, exploitation, and dissemination (PED) to the point of collection	Developing capabilities that support PED at the point of collection increases effectiveness of platforms in a communication degraded environment, supports signature management, and enables optimal tasking and re-tasking of sensors.
Develop and employ systems that provide explainable AI (XAI)	Implement AI tools which provide context and reasoning to the end user through XAI. Employing explainable models makes the AI system understandable by providing rationale to explain how outputs were arrived at, ultimately building trust in the system and increasing its use.
Develop cross domain solutions	AI requires data input that spans all classification levels. If the Enterprise is going to more frequently merge data sets across all classification levels to enable better use of AI, it needs tools to immediately and easily parse out lower classified, but useful findings, to operators cleared only to SECRET
Leadership and Education	
Joint approach to AI Integration	Approaching AI integration in a joint manner through the JAIC provides external resource capacity. MCISRE can leverage additional personnel and financial resources, reduce development time, and

	support AI effort synchronization with the broader DoD.
Personnel	
Evaluate the task organization of intelligence units across MCISRE to seek reduction opportunities	AI tools increase analyst efficiency and may reduce the manpower footprint required to support operations. MCISRE should evaluate and adjust its T/O to reflect proper manning levels. Any reduction in manpower should be based upon sufficient data gathered subsequent to AI implementation.
Create structure to support data management across the Marine Corps	The Marine Corps is implementing AI across all warfighting functions and the need to provide data management capabilities is a service wide problem, not just an intelligence one. The Marine Corps should develop a data management capability to replace MCISRE's DATINT proposal. The utilization of data management Marines in the data science and engineering fields should be supported by training and T/O across the service, not pulled from MCISRE.
Facilities	
Evaluate the need for additional facility space to support the increase in data repository required for AI.	Data required for AI capabilities goes beyond traditional organic collection and encompasses data gathered across the internet of things. Storage capacity for the amount of data required for AI toolsets may require an increase in facilities for storage. The need for additional storage facilities will be influenced by the data strategy on whether to use cloud services via PaaS, IaaS, and/or SaaS.
Policy	
Develop a cloud strategy in coordination with the JAIC	Develop a cloud strategy to address data storage and accessibility. The strategy should be informed by the joint strategy being worked by the JAIC. The JAIC is working a common foundation cloud environment which users across the DoD can access through their respective portals

Employ edge computing in concert with cloud computing	Edge computing moves computing and storage resources away from a geographically separated cloud to the edge of the network close to end devices. It speeds up access and dissemination of information, increases security and reliability, and supports scalability of the Enterprise.
Develop a data storage plan	All data is not equal in the intelligence field. Determining what data to house in a cloud repository, how to store it, and for how long are important determinations which should be identified within the overall data strategy.
Develop policy to implement Enterprise wide cross domain solutions (CDS)	CDS is not only a materiel requirement, it is a policy one as well. MCISRE should work with DC I, DISA and the NSA to develop CDS capabilities and corresponding policy to support it.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Adelyar, S. and Norta, A. (2016). Towards a Secure Agile Software Development Process. In: *10th International Conference on the Quality of Information and Communications Technology (QUATIC)*. IEEE Xplore. Retrieved from <https://ieeexplore.ieee.org/document/7814525/authors#authors>. [Accessed 17 Apr. 2019].
- Aghabozorgi, S. (2016). *Data Scientist vs. Data Engineer, What's the difference?*. Cognitive Class. Retrieved from <https://cognitiveclass.ai/blog/data-scientist-vs-data-engineer/>. [Accessed 21 Mar. 2019].
- Alderton, M. (2017). Embracing the Enterprise. *Trajectory*. Retrieved from <http://trajectormagazine.com/embracing-the-enterprise/>. [Accessed 11 Oct. 2018].
- Allen, G. and Chan, T. (2017). *Artificial Intelligence and National Security*. Harvard Kennedy School. Retrieved from <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>. [Accessed 24 Aug. 2017].
- Amazon. (2018). *Nex Gen Stats Powered by AWS*. Retrieved from <https://aws.amazon.com/nextgenstats/>. [Accessed 19 Oct. 2018].
- Atwood, C. (2015). Activity-Based Intelligence Revolutionizing Military Intelligence Analysis. *Joint Forces Quarterly*, 77 (2nd Quarter), pp. 24–33. Retrieved from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-77/jfq-77_24-33_Atwood.pdf. [Accessed 2 May 2019].
- Bernard, S. (2012). An introduction to Enterprise Architecture (Third edition, International edition.). Bloomington, IN: Authorhouse.
- Bmva.org. (n.d.). What is computer vision. Retrieved from <http://www.bmva.org/visionoverview>. [Accessed 10 Mar. 2019].
- Boury-Brisset, A. (2004). *Ontological Approach to Military Knowledge Modeling and Management*. Val-Belair.
- Colman, E. (2013). *When to use SaaS, PaaS, and IaaS*. ComputeNext. Retrieved from <https://www.computenext.com/blog/when-to-use-saas-paas-and-iaas/>. [Accessed 11 Oct. 2018].
- Concepts and Programs, U. (2018). *DCGS - MC*. Candp.marines.mil. Retrieved from <http://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/DCGS-MC/>. [Accessed 11 Oct. 2018].

- Conklin, B. (2010). *Activity Based Intelligence - A Perilous Journey to Intelligence Integration*. Retrieved from <https://www.esri.com/~media/E1ED40B76F7F4DA5ABDCC4FB310171D0.pdf>. [Accessed 11 May 2018].
- DAU (2016). *The Information Technology (IT) Box*. Ft. Belvoir: Defense Acquisition University. Retrieved from <https://www.dau.mil/training/Documents/IT%20Box%20Primer%20revised%2019%20Aug%202016.pdf>. [Accessed 15 Feb. 2019].
- DAU (2018). *DOTMLPF-P Analysis*. Defense Acquisition University. Retrieved from <http://acqnotes.com/acqnote/acquisitions/dotmlpf-analysis>. [Accessed 5 Apr. 2019].
- DCGS-MC Sharing information to the tactical edge. (2015). *The Chronical*, 21(1), p.6. Retrieved from https://www.public.navy.mil/spawar/Atlantic/Documents/Chronicle/2014-15_Winter.pdf. [Accessed 13 Dec. 2018].
- Dhande, M. (2017). What is the difference between AI, machine learning and deep learning?. [Blog] *Geospatial World*. Retrieved from <https://www.geospatialworld.net/blogs/difference-between-ai%EF%BB%BF-machine-learning-and-deep-learning/>. [Accessed 12 Dec. 2018].
- DISA. (2019). *Cross Domain Enterprise Services (CDES)*. Retrieved from <https://www.disa.mil/cybersecurity/cross-domain-enterprise-services>. [Accessed 20 Feb. 2019]. Kamis, G. (2019). *DoD must embrace cross-domain security and continuous monitoring*. Defense Systems. Retrieved from <https://defensesystems.com/articles/2019/02/15/cross-domain-security.aspx>. [Accessed 20 Feb. 2019].
- DoD ESI (2018). *What is Cloud Computing and How Does It Impact Software Licensing Practices?*. DoD ESI. Retrieved from <http://www.esi.mil/contentview.aspx?id=931>. [Accessed 11 Oct. 2018].
- Domingos, P. (2012). A few useful things to Know about machine Learning. *Communications of the ACM*, 55(10), 78–87.
- Dsiac.org. (2015). Modeling Intelligence PED With FOCUS: A Tactical-Level ISR Simulation | DSIAC. Retrieved from <https://www.dsiac.org/resources/journals/dsiac/fall-2015-volume-2-number-4/modeling-intelligence-ped-focus-tactical-level>. [Accessed 10 Mar. 2019].
- Expeditionary Force 21. (2014). [ebook] Washington: United States Marine Corps. Retrieved from https://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/EF21/EF21_Capstone_Concept.pdf. [Accessed 1 Jun. 2018].

- Faltemier, T. and Middendorff, C. (2018). Surveillance, Persistent Observation, and Target Recognition. Retrieved from <http://www.spotrtech.com/products.php>. [Accessed 2 May 2018].
- Fensel, D. (2001). *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce*. New York: Springer-Verlag Berlin Heidelberg GmbH.
- Forge.AI. (2019). *Our Technology*. Retrieved from <https://www.forge.ai/our-technology>. [Accessed 16 Jan. 2019].
- Freedberg, S. (2018). *Show Me The Data: The Pentagon's Two-Pronged AI Plan*. Breaking Defense. Retrieved from <https://breakingdefense.com/2018/12/show-me-the-data-the-pentagons-two-pronged-ai-plan/>. [Accessed 1 Apr. 2019].
- Fumo, D. (2017). *Types of Machine Learning Algorithms You Should Know*. Towards Data Science. Retrieved from <https://towardsdatascience.com/types-of-machine-learning-algorithms-you-should-know-953a08248861>. [Accessed 19 Oct. 2018].
- Garrett, W. (2013). Headquarters Marine Corps. Retrieved from <https://www.hqmc.marines.mil/Portals/142/Docs/USCENTCOM%20Bastion%20Attack%20Investigation%20Executive%20Summary.pdf>. [Accessed 17 Jan. 2019].
- Goodfellow, I., Bengio, Y. and Courville, A. (2016). *Deep Learning*. Cambridge: The MIT Press.
- Gruber, T. (1995). *Toward principles for the design of ontologies used for knowledge sharing*. Palo Alto: Stanford Knowledge Systems Laboratory.
- Gunning, D. (2019). *Explainable Artificial Intelligence (XAI)*. Defense Advanced Research Projects Agency (DARPA). Retrieved from <https://www.darpa.mil/program/explainable-artificial-intelligence>. [Accessed 1 Apr. 2019].
- Gurteen, D. (2019). *Communities of Practice (Gurteen Knowledge)*. Gurteen.com. Retrieved from <http://www.gurteen.com/gurteen/gurteen.nsf/id/communities-of-practice>. [Accessed 2 May 2019].
- Gyarmathy, K. (2018). The 5 Best Benefits of Edge Computing. [Blog] *VXCHNGE*. Retrieved from <https://www.vxchnge.com/blog/the-5-best-benefits-of-edge-computing>. [Accessed 11 Dec. 2018].
- Hendrickson, K. (2018). Overcoming the Barriers to Human-Machine Teams. *Defense Systems Information Analysis Center*, 5(4). Retrieved from <https://www.dsiac.org/resources/journals/dsiac/fall-2018-volume-5-number-4/overcoming-barriers-human-machine-teams>. [Accessed 4 Apr. 2019].

- Hoogervorst, J. (2004). Enterprise Architecture: Enabling Integration, Agility, and Change. *International Journal of Cooperative Information Sciences*, 13(3), 213–233. Retrieved from <https://www.worldscientific.com/doi/abs/10.1142/S021884300400095X>. [Accessed 5 Dec. 2018].
- HQMC (2018). *Data Intelligence: Marine Corps Concept for “Making Sense.”* Washington, D.C.
- HQMC-I (2014). *Marine Corps Intelligence, Surveillance, and Reconnaissance Plan 2015–2020*. Washington, D.C.: United States Marine Corps Intelligence Department. Retrieved from http://www.hqmc.marines.mil/Portals/133/Docs/MCISRE_Final_Sept2014.pdf. [Accessed 26 Apr. 2018].
- IEEE Standards Association (2011). *What are Standards? Why are They Important?*. Institute of Electrical and Electronics Engineers. Retrieved from <https://beyondstandards.ieee.org/general-news/what-are-standards-why-are-they-important/>. [Accessed 1 Apr. 2019].
- Jones, R. (2019). *Defense Acquisition System [PowerPoint Slides]*. Naval Postgraduate School. Monterey, CA.
- Jones, R. (2019). *Introduction and Program Management [PowerPoint Slides]*. Naval Postgraduate School. Monterey, CA.
- JROC (2013). *Persistent ISR Information Systems ICD*. Quantico: USMC.
- Kamel, M. (2019). *Introduction to Big Data and Data Science [PowerPoint Slides]*. Naval Postgraduate School. Monterey, CA.
- Kamis, G. (2019). *DoD must embrace cross-domain security and continuous monitoring*. Defense Systems. Retrieved from <https://defensesystems.com/articles/2019/02/15/cross-domain-security.aspx>. [Accessed 20 Feb. 2019].
- Kimmons, J., Makuta, R. and Gilmer, G. (2017). *Remaking Intelligence Processing Exploitation and Dissemination*. [ebook] Booz Allen Hamilton. Retrieved from <https://www.defenseone.com/media/ped-thought-piece-presentedby-booz-allen.pdf>. [Accessed 10 Mar. 2019].
- Kojac, J. (2019). *Joint AI Center (JAIC) [PowerPoint Slides]*. AI Cross Leveling Summit, USMC. Quantico, VA.
- Komorowski, M. (2014). *A History of Storage Cost*. mkomo.com. Retrieved from <http://www.mkomo.com/cost-per-gigabyte>. [Accessed 30 Oct. 2018].
- Lai, A. (2018). Five Standards for Responsible AI Use. [Blog] *Strategy + Business*. Retrieved from <https://www.strategy-business.com/blog/Five-Standards-for-Responsible-AI-Use?gko=a2f1c>. [Accessed 1 Apr. 2019].

- Lai, P. (2017). The Literature Review of Technology Adoption Models and Theories for the Novelty Technology. *Journal of Information Systems and Technology Management*, 14(1), 21–38.
- Lee, K. (2018). *The Era of AI: The Rise of China and the Future of Work*. Retrieved from <https://www.slideshare.net/AIFrontiers/kaifu-lee-at-ai-frontiers-the-era-of-artificial-intelligence>. [Accessed 15 Feb. 2019].
- Lee, S. (2016). *Applications and benefits for big data sets using tree distances and the t-SNE algorithm*. Monterey: Naval Postgraduate School. Retrieved from https://calhoun.nps.edu/bitstream/handle/10945/48546/16Mar_Lee_Suyoung.pdf?sequence=1&isAllowed=y. [Accessed 18 Oct. 2018]
- Llinas, J. and Scrofani, J. (2014). *Foundational technologies for activity-based intelligence-a review of the literature*. Master's Degree. Naval Postgraduate School.
- Llinas, J., Bowman, C., Rogova, G., Steinberg, A., Waltz, E. and White, F. (2004). *Revisiting the JDL Data Fusion Model II*. Researchgate. Retrieved from <https://www.researchgate.net/publication/2932954>. [Accessed 12 Apr. 2019].
- Long, L. (2013). Activity Based Intelligence: Understanding the Unknown. *The Intelligencer - Journal of U.S. Intelligence Studies*, 20(2), 1–15. Retrieved from https://www.afio.com/publications/LONG_Tish_in_AFIO_INTEL_FALLWINTER2013_Vol20_No2.pdf. [Accessed 18 Jul. 2018].
- Marine Corps Intelligence, Surveillance, & Reconnaissance Enterprise Plan 2015–2020. (2014). [Ebook] United States Marine Corps. Retrieved from https://www.hqmc.marines.mil/Portals/133/Docs/MCISRE_Final_Sept2014.pdf. [Accessed 1 Jun. 2018].
- Mattis, J. (2018). *National Defense Strategy*. Washington, D.C.: Department of Defense. Retrieved from <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>. [Accessed 20 Mar. 2019].
- MC.AI. (2018). *How to make it simple to explain AI, ML, DL and Data Science?*. Retrieved from <https://mc.ai/how-to-make-it-simple-to-explain-ai-ml-dl-and-data-science/>. [Accessed 19 Oct. 2018].
- MCDP 1 Warfighting*. (1997). Washington, D.C.: Headquarters United States Marines Corps.
- MCDP 2 Intelligence*. (1997). Washington, D.C.: Headquarters United States Marines Corps.

- McKinsey Global Institute (2011). *Big data: The next frontier for innovation, competition, and productivity*. Retrieved from <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>. [Accessed 2 Aug. 2017].
- MCTP 2-10A MAGTF Intelligence Collection*. (2016). Washington, D.C.: Headquarters United States Marines Corps.
- MCTP 2-10B MAGTF Intelligence Production and Analysis*. (2016). Washington, D.C.: Headquarters United States Marines Corps.
- MCWP 2-10 Intelligence Operations*. (2016). Washington, D.C.: Headquarters United States Marines Corps.
- Merriam-Webster. (2018). Retrieved from <https://www.merriam-webster.com/dictionary/artificial%20intelligence>. [Accessed 12 Dec. 2018].
- Ming, V. (n.d.). *Vivienne Ming Quotes*. Retrieved from https://www.brainyquote.com/quotes/vivienne_ming_822211. [Accessed 8 Apr. 2019].
- Mitchell, B. (2019). *White House looks to fund DoD's Joint AI Center*. fedscoop. Retrieved from <https://www.fedscoop.com/joint-ai-center-dod-fiscal-2020-budget/>. [Accessed 20 Mar. 2019].
- National Commission on Terrorist Attacks Upon the United States (2004). *The 9/11 Commission Report*. 9/11 Commission. Retrieved from http://govinfo.library.unt.edu/911/report/911Report_Exec.htm. [Accessed 22 Aug. 2017].
- NIST. (2018). *NIST Cloud Computing Program - NCCP*. Retrieved from <https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp>. [Accessed 30 Oct. 2018].
- Pace, H. (2019). *Open Architecture Strategy*. [PowerPoint Slides].
- Paul, C., Thie, H., Webb, K., Young, S., Clarke, C., Straus, S., Laha, J., Osowski, C. and Serena, C. (2011). *Alert and Ready - An Organizational Design Assessment of Marine Corps Intelligence*. [ebook] RAND Corporation. Retrieved from <https://www.rand.org/pubs/monographs/MG1108.html>.
- Pearlson, K. and Saunders, C. (2013). *Strategic management of information systems*. 5th ed. Hoboken, NJ: Wiley.
- Pedersen, T., Liu, Y., Bill, R., Fiszman, M., Rindflesch, T., Melton, G. and Pakhomov, S. (2012). Using SemRep to Label Semantic Relations Extracted from Clinical Text. In: *AMIA Symposium*.

- Peters, H. (2018). *The DoD's JEDI Cloud Program*. Federation of American Scientists. Retrieved from <https://fas.org/sgp/crs/natsec/IN10990.pdf>. [Accessed 3 Apr. 2019].
- PremSankar, G., Di Francesco, M. and Taleb, T. (2018). Edge Computing for the Internet of Things: A Case Study. *IEEE*. Retrieved from <https://users.aalto.fi/~premsag1/docs/premsankar2018edge.pdf>. [Accessed 12 Dec. 2018].
- Prietula, M., Cokely, E. and Ericsson, K. (2007). The Making of an Expert. *Harvard Business Review*. Retrieved from [http://www.tevlin.ca/roberta/12U%20Course/3\)%20The%20Making%20of%20an%20Expert.pdf](http://www.tevlin.ca/roberta/12U%20Course/3)%20The%20Making%20of%20an%20Expert.pdf). [Accessed 8 Apr. 2019].
- Public-Private Analytic Exchange Program (2018). *AI: Using Standards to Mitigate Risks*. Retrieved from https://www.dni.gov/files/PE/Documents/2018_AEP-AI.pdf. [Accessed 1 Apr. 2019].
- Rahmani, A., Nguyen Gia, T., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. and Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 78(2), 641–658. Retrieved from <https://www.sciencedirect.com/science/article/pii/S0167739X17302121>. [Accessed 11 Dec. 2018].
- Ramadan, R. (2017). Big Data Tools - An Overview. *International Journal of Computer Science and Software Engineering*, 2(125), 1–2.
- Ramaswamy, S. (2017). How Companies Are Already Using AI. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/04/how-companies-are-already-using-ai>. [Accessed 25 Apr. 2018].
- Rogers, E. (2003). *Diffusion of Innovations*. New York: Free Press.
- Savitz, E. (2013). Big Data: Getting Ready For The 2013 Big Bang. *Forbes*. Retrieved from <https://www.forbes.com/sites/ciocentral/2013/01/15/big-data-get-ready-for-the-2013-big-bang/#4276138638c5>. [Accessed 23 Apr. 2018].
- Schrage, M. (2017). AI is Going to Change the 80/20 Rule. *Harvard Business Review*. Retrieved from <https://hbr.org/2017/02/ai-is-going-to-change-the-8020-rule>. [Accessed 26 Aug. 2017].
- Seif, G. (2017). *The 5 Clustering Algorithms Data Scientists Need to Know*. Towards Data Science. Retrieved from <https://towardsdatascience.com/the-5-clustering-algorithms-data-scientists-need-to-know-a36d136ef68>. [Accessed 12 Dec. 2018].
- Seltser, S. (2018). *Connecting the dots: AI, ML and data management and how it applies to Combat ID [PowerPoint Slides]*. Petacube Inc. Boston, MA.

- Shoham, Y., Perrault, R., Brynjolfsson, E. and Clark, J. (2017). *Artificial Intelligence Index 2017 Annual Report*. One Hundred Year Study on AI at Stanford University. Stanford: Stanford University. Retrieved from <http://cdn.aiindex.org/2017-report.pdf>. [Accessed 27 Apr. 2018].
- Statistical Analysis System (SAS). (2018). *Natural Language Processing What it is and why it matters*. Retrieved from https://www.sas.com/en_us/insights/analytics/what-is-natural-language-processing-nlp.html. [Accessed 12 Dec. 2018].
- Stefanowski, J. (2009). *Data Mining-Clustering*. Presented at Institute of Computing Sciences Poznan University of Technology.
- Sun-tzu, and Samuel B. Griffith. *The Art of War*. Oxford: Clarendon Press, 1964. Print.
- Tamhane, D. and Sayyad, S. (2015). Big Data Analysis Using Hace Theorem. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 4(1), 20.
- Tan, A. (n.d.). *Text Mining: The state of the art and the challenges*. Kent Ridge Digital Labs. Retrieved from http://www.ntu.edu.sg/home/asahtan/papers/tm_pakdd99.pdf. [Accessed 12 Dec. 2018].
- Taylor, A. (2017). A new 'FACE' for Aviation Acquisition. *Army AL&T magazine*. Retrieved from https://www.army.mil/article/195215/a_new_face_for_aviation_acquisition. [Accessed 20 Mar. 2019].
- Trump, D. (2017). *National Security Strategy*. p.13. Retrieved from <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>. [Accessed 20 Feb. 2019].
- The United States Intelligence Community Intelligence Careers. (2017). *Member Agencies*. Retrieved from <https://www.intelligencecareers.gov/icmembers.html>. [Accessed 24 Aug. 2017].
- United States Marine Corps (2017). *Marine Corps Strategy for Assured Command and Control*. United States Marine Corps. Retrieved from https://www.hqmc.marines.mil/Portals/61/Marine_Corps_Strategy_for_Assured_Command_and_Control_March_2017.pdf?ver=2017-05-30-160731-940. [Accessed 6 Nov. 2018].
- United States Marine Corps Service Campaign Plan 2014–2022. (2014). [ebook] Quantico: United States Marine Corps. Retrieved from http://pentagonus.ru/_ld/11/1177_United_States_M.pdf. [Accessed 1 Jun. 2018].
- Wang, J., Zuo, W., He, F. and Wang, Y. (2009). *A New Formal Description of Ontology Definition and Ontology Algebra*. IEEE. Retrieved from <https://ieeexplore.ieee.org/document/5362162>. [Accessed 1 May 2019].

- Watts, S. (2017). *SaaS vs. PaaS vs. IaaS: What's The Difference and How To Choose*. BMC. Retrieved from <https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/>. [Accessed 11 Oct. 2018].
- Wenger, E. (1999). *Communities of practice*. Cambridge: Cambridge Univ. Press.
- Willems, K. (2017). *Data Scientist vs. Data Engineer: The differences between data engineers and data scientists explained: responsibilities, tools, languages, job outlook, salary, etc..* DataCamp. Retrieved from <https://www.datacamp.com/community/blog/data-scientist-vs-data-engineer#gs.w3U8c2g>. [Accessed 21 Mar. 2019].
- Williams, L. (2018). *DoD releases \$10 billion JEDI cloud contract*. Defense Systems. Retrieved from <https://defensesystems.com/articles/2018/07/26/jedi-hits-the-street.aspx>. [Accessed 3 Apr. 2019].
- Wu, X., Zhu, X. and Wu, G. (2014). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering*, 26(1), 97–101. Retrieved from <http://ieeexplore.ieee.org/document/6547630/?part=1>. [Accessed 22 Aug. 2017].

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