

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

1. REPORT DATE (DD-MM-YYYY) 04/29/2019	2. REPORT TYPE Master's of Military Studies	3. DATES COVERED (From - To) SEP 2018 - APR 2019
--	---	--

4. TITLE AND SUBTITLE Next Generation Intelligence Integration: Leveraging Artificial Intelligence to Facilitate Human-Machine Collaboration and Enhance Intelligence Collection and Analysis	5a. CONTRACT NUMBER N/A
	5b. GRANT NUMBER N/A
	5c. PROGRAM ELEMENT NUMBER N/A

6. AUTHOR(S) Gorman, Ryan, R, CIV, USMC	5d. PROJECT NUMBER N/A
	5e. TASK NUMBER N/A
	5f. WORK UNIT NUMBER N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) USMC Command and Staff College Marine Corps University 2076 South Street Quantico, VA 22134-5068	8. PERFORMING ORGANIZATION REPORT NUMBER N/A
--	--

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) Dr. Benjamin Jensen
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Advances in Artificial Intelligence (AI) and machine learning (ML) technologies have the potential to revolutionize how military organizations prioritize, collect, process, analyze, disseminate, and utilize intelligence in increasingly complex and contested future operating environments. By rapidly integrating large and diverse data sets AI/ML algorithms can accelerate traditional intelligence processes, quickly identify relevant trends and anomalies, and assist human analysts in making well-supported judgments regarding potential threats and opportunities. The capability to integrate machine-generated knowledge with human insight is vital to maintaining cognitive advantage in future operating environments.

15. SUBJECT TERMS
Artificial Intelligence, AI; Machine Learning, ML; Intelligence; Information Environment, IE; Operations in the Information Environment, OIE; collaboration; integration

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU	39	19b. TELEPHONE NUMBER (Include area code) (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE:
NEXT GENERATION INTELLIGENCE INTEGRATION: LEVERAGING ARTIFICIAL
INTELLIGENCE TO FACILITATE HUMAN-MACHINE COLLABORATION AND
ENHANCE INTELLIGENCE COLLECTION AND ANALYSIS

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR:
Ryan R. Gorman, CIV

AY 18-19

Mentor and Committee Member: Dr. Benjamin Jensen
Approved: [Signature]
Date: 4/29/19

Committee Member: Nathan M Packard, PhD
Approved: [Signature]
Date: 4/29/19

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

EXECUTIVE SUMMARY

Title: *Next Generation Intelligence Integration: Leveraging Artificial Intelligence to Facilitate Human-Machine Collaboration and Enhance Intelligence Collection and Analysis*

Author: CIV Ryan R. Gorman

Thesis: Advances in Artificial Intelligence (AI) and machine learning (ML) technologies have the potential to revolutionize how military organizations prioritize, collect, process, analyze, disseminate, and utilize intelligence in increasingly complex and contested future operating environments. By rapidly integrating large and diverse data sets AI/ML algorithms can accelerate traditional intelligence processes, quickly identify relevant trends and anomalies, and assist human analysts in making well-supported judgments regarding potential threats and opportunities. The capability to integrate machine-generated knowledge with human insight is vital to maintaining cognitive advantage as the Marine Corps persistently operates in a highly competitive Information Environment (IE).

Discussion: With the designation of “Information” as the seventh warfighting function, the Marine Corps has acknowledged the vital role of information in planning and conducting successful military operations. The capstone Marine Corps Operating Concept (MOC) further recognizes the need to exploit emerging technologies in order to wage successful informational warfare across all domains. While supporting concepts have been proposed to address various aspects of the IE, additional work remains to determine how AI/ML technologies might be systematically integrated to augment existing intelligence capabilities and processes. This proposed future operating concept paper explores some initial areas where new technologies and human-machine interfaces could pay significant dividends for Marine Corps Intelligence components as they operate and seek to anticipate changes in the rapidly evolving IE.

Conclusion: As an institution with a history of adaptation and innovation, the Marine Corps is well-positioned to play a leading role in determining how emerging AI and ML technologies are adopted and integrated to support a wide range of military operations. While policy debates typically have focused on whether AI should be used to enable lethal autonomous or semi-autonomous weapons, AI technology could serve numerous non-kinetic uses that raise fewer ethical concerns while increasing the effectiveness of intelligence and information operations. While artificially intelligent machines cannot replace the ingenuity and determination inherent in Marines and other U.S. service members, new modes of collaboration between human analysts and machines could dramatically increase the timeliness and utility of intelligence analysis generated in support of future military operations.

TABLE OF CONTENTS

Disclaimer	2
Executive Summary	3
Preface.....	5
Introduction.....	6
Purpose	8
Time Horizons	9
Assumptions	9
Risks	10
Military Problem.....	11
Central Idea.....	12
Application and Integration of Military Functions.....	15
Necessary Capabilities	18
Spatial and Temporal Dimensions	21
Conclusion	22
Appendix A: Insights from War Games.....	22
Appendix B: Historical Case Study.....	23
Background.....	25
The Nuclear Arms Race Case	27
Bibliography	32

PREFACE

This paper proposes an enabling operating concept to support the Intelligence and Information warfighting functions. This concept is subordinate to the capstone *Marine Corps Operating Concept (MOC)*,¹ as well as to the subordinate concepts *Littoral Operations in a Contested Environment (LOCE)*² and *Expeditionary Advanced Base Operations (EABO)*.³ It also helps enable the *Marine Air Ground Task Force (MAGTF) Information Environment Operations Concept of Employment*.⁴ This proposed concept paper focuses on how the Marine Corps likely will operate at the operational level of war, and it offers recommendations for capabilities that could be developed across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) spectrum to support future operations.⁵

This proposed future operating concept follows the guidelines in the Marine Corps' *Combat Development and Integration (CD&I) Concept Development Instruction 5401.1*,⁶ and it uses the specific framework outlined in the Defense Adaptive Red Team's *A Practical Guide for Developing and Writing Military Concepts*.⁷ I offer sincere thanks to all my colleagues at the Marine Corps Command and Staff College who have stimulated my thinking this year. In

¹ USMC. *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. September 2016. <https://www.mccdc.marines.mil/MOC/>.

² USMC. *Littoral Operations in a Contested Environment (LOCE)*, UNCLASSIFIED Edition. 2017. https://www.candp.marines.mil/Portals/216/documents/Concepts/LOCE%20full%20size%20edition_0.pdf?ver=2018-05-01-133728-797.

³ USMC. *Expeditionary Advanced Base Operations (EABO)*. UNCLASSIFIED Summary. <https://www.candp.marines.mil/Concepts/Subordinate-Operating-Concepts/Expeditionary-Advanced-Base-Operations>.

⁴ USMC. *Marine Air Ground Task Force Information Environment Operations Concept of Employment*. 6 July 2017. <https://www.candp.marines.mil/Portals/216/documents/Concepts/MCFC%205-5%20MAGTF%20INFORMATION%20ENVIRONMENT%20OPERATIONS.pdf?ver=2019-02-05-130208-943>.

⁵ Chairman of the Joint Chiefs of Staff (CJCS). *Joint Capabilities Integration and Development System (JCIDS), CJCSI 3170.011*. 23 January 2015. https://dap.dau.mil/policy/Documents/2015/CJCSI_3170_011.pdf.

⁶ USMC. *Combat Development and Integration (CD&I) Concept Development Instruction 5401.1*. 8 February 16. <https://www.candp.marines.mil/Portals/216/documents/Concepts/Concept%20Development%205401.1.pdf?ver=2018-05-01-133728-080>.

⁷ Schmitt, John F. *A Practical Guide for Developing and Writing Military Concepts*. Defense Adaptive Red Team (DART) Working Paper #02-4. McLean, VA: Hicks & Associates, Inc., Dec 2002. http://www.au.af.mil/au/awc/awcgate/writing/dart_paper_writing_mil_concepts.pdf.

particular, I am grateful for the opportunity to participate in the Gray Scholars program, managed and facilitated by Dr. Benjamin Jensen and Dr. Nathan Packard. This program has greatly expanded my understanding of the challenges and opportunities the Marine Corps likely will face in future operating environments. Finally, I am most grateful to my family for supporting, encouraging, and inspiring me throughout the years.

INTRODUCTION

The ever-evolving character of war appears to be in the midst of a paradigm shift, and perhaps on the cusp of revolutionary technological change.⁸ While war remains a violent, dynamic conflict between opposing wills determined to achieve political ends, each of the elements that comprise Clausewitz's famous "trinity of war"⁹ is rapidly changing due to transformative technologies that are poised to dramatically alter how humans interact with machines and with one another. Now and in the future, the primordial elements of violence and passion, which intensely influence human judgments in war, can be mitigated by greater reliance on objective criteria programmed into machine learning algorithms to aid human judgment and decision making. The element of chance will always remain in war, but artificially intelligent machines are becoming increasingly adept at forecasting probabilities and could reduce some of war's inherent fog and friction. War remains an instrument of policy intended to achieve rational political objectives; however, those objectives often appear to be in flux due to the highly globalized and enmeshed character of contemporary international relations, as well as the

⁸ For an insightful discussion of paradigm shifts and revolutionary changes in the scientific community, see Thomas S. Kuhn's classic *The Structure of Scientific Revolutions*, 4th Edition. University of Chicago Press, 2012.

⁹ Clausewitz, Carl von. *On War*. Edited and translated by Michael E. Howard and Peter Paret. Princeton University Press, 1984. Book 1, Chapter 1, Section 2. Clausewitz describes his trinity as follows: war is "composed of primordial violence, hatred, and enmity, which are to be regarded as a blind natural force; of the play of chance and probability within which the creative spirit is free to roam; and of its element of subordination, as an instrument of policy, which makes it subject to reason." See also "Teaching the Clausewitzian Trinity" by Christopher Bassford, <https://www.clausewitz.com/readings/Bassford/Trinity/TrinityTeachingNote.htm>.

exponential increase in the volume, variety, and velocity of information being created, shared, analyzed, and utilized across the interconnected globe. All of these changes have profound implications for how U.S. Marines and fellow service members will plan and operate in complex, contested future environments.

Recognizing the vital importance of maintaining informational and cognitive advantage against rivals and potential adversaries, the Marine Corps recently followed the Joint Chiefs of Staff's lead in officially establishing "Information" as the seventh warfighting function.^{10, 11} Additionally, the 2016 capstone *Marine Corps Operating Concept (MOC)*, recognizes the imperative to develop and integrate capabilities in order to conduct information warfare, and it declares the essential point: "The 21st century Marine Air Ground Task Force (MAGTF) conducts maneuver warfare in the physical and cognitive dimensions of conflict to generate and exploit psychological, technological, temporal, and spatial advantages over the adversary."¹² With this increased institutional emphasis on the informational and cognitive dimensions of war comes the need to better understand how emergent technologies can augment the military's capabilities to operate in the information environment.

This concept paper explores how the technologies of Artificial Intelligence (AI) and machine learning (ML) can help address emerging military problems that are likely to become even more pervasive and complex in future operating environments. It describes how AI and ML

¹⁰ USMC. *Marine Corps Bulletin (MCBul) 5400: ESTABLISHMENT OF INFORMATION AS THE SEVENTH MARINE CORPS WARFIGHTING FUNCTION*, 17 January 2019. <https://www.marines.mil/Portals/59/Publications/MCBUL%205400.pdf?ver=2019-02-06-082807-103>.

¹¹ Joint Chiefs of Staff. *Joint Publication (JP) 1: Doctrine for the Armed Forces of the United States*, updated 12 July 2017, Section I-19. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2017-12-23-160207-587.

¹² USMC. *The Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. September 2016, page 8. <https://www.candp.marines.mil/Portals/216/documents/Concepts/Marine%20Corps%20Operating%20Concept%20Sept%202016.pdf?ver=2018-05-01-133729-063>.

applications can enhance current intelligence collection and analysis processes and capabilities to provide more rapid and insightful intelligence support to military decision makers operating in those complex environments. Although these technologies hold enormous potential to help resolve challenges, no technological solution or set of solutions should be regarded as a panacea, since competitors will relentlessly seek to exploit vulnerabilities, and human creativity and character will continue to be the most decisive elements needed to gain advantages and win future battles.

PURPOSE

This proposed future operating concept is intended to provoke thought and inform development of capabilities that will help the Marine Corps smartly plan for and execute future intelligence and information operations. It suggests potential opportunities for mitigating challenges associated with operating in highly complex and adaptive information environments. Some technological capabilities suggested are speculative, but many sophisticated AI and ML applications are already commonplace and commercially available from a variety of vendors. Differentiating between applications that sound great in theory (or appear great in elegant presentations) from those that actually deliver reliable and replicable results will be critical. Much further experimentation will be necessary to test commercial AI and ML technologies' interoperability with existing military systems, to tailor specific algorithms using large quantities of training data, and to assess the effectiveness of the technologies in various simulated military scenarios.

Advances in AI and ML technologies have the potential to revolutionize how military organizations prioritize, collect, process, analyze, disseminate, and utilize intelligence in increasingly complex and contested future operating environments. By rapidly integrating large

and diverse data sets AI/ML algorithms can accelerate traditional intelligence processes, quickly identify relevant trends and anomalies, and assist military personnel in making well-supported judgments regarding potential threats and opportunities. The capability to integrate machine-generated knowledge with human insight is vital to maintaining cognitive advantage as the Marine Corps persistently operates in a highly competitive Information Environment (IE).

TIME HORIZONS

This proposed operating concept applies to the immediate future as it seeks to draw attention to existing and emerging capabilities that can be implemented gradually over the next decade or two. Given the rapidly changing technological landscape, it is difficult to predict how AI and ML applications might evolve in that timespan, but the time to begin experimenting with and leveraging them more robustly is now.

ASSUMPTIONS

This proposed operating concept assumes that American private sector technology firms and interagency partners will be willing to share information and cooperate with the U.S. military to help develop non-lethal AI and ML applications. It also assumes that competitor nations will actively militarize AI and ML technologies garnered from the commercial sector, often without the same degree of legal and ethical scrutiny that the U.S. government and populace demands. It further assumes that AI and ML innovations will progress rapidly, but not reach the break through to “general AI” capabilities (in which machines can perform as well or

better than humans at solving complex, adaptive problems and conducting most daily tasks)¹³ in the ten to twenty year time horizon of this concept paper.¹⁴

RISKS

The greatest risk regarding AI and ML technologies would be to reject them or to implement them so circumspectly that adversarial nations are able to outpace the U.S. military in developing more dynamic, resilient, and efficient systems. However, AI and ML applications do carry attendant risks that must be acknowledged. For example, the algorithms tend to work best when developed in fairly controlled environments with vast quantities of relevant training data – conditions which are not readily available in many military contexts. If the algorithms are insufficiently trained and validated, or if the data is corrupted or manipulated (whether intentionally or inadvertently), then the systems can perform unpredictably or in ways that seem contrary to common sense. Moreover, many of the inner workings of AI/ML algorithms are opaque, particularly when dealing with systems based on deep neural networks, so humans might not be able to fully understand how or why the machine generated a particular output or conclusion. This lack of process transparency can hinder accountability and dissuade people from trusting the systems, especially in risky environments where lives are at stake. A final risk should be mentioned, namely, that over reliance on technological solutions can lull people into a false sense of security that the machines will consistently provide accurate and reliable

¹³ For an overview of the distinction between “narrow” and “general AI,” see Baggaley, Kate, “There are Two Kinds of AI, and the Difference is Important.” *Popular Science*. 23 February, 2017. <https://www.popsci.com/narrow-and-general-ai#page-2>.

¹⁴ A 2017 survey indicates that AI researches believe there is a 50 percent chance that AI will be able to outperform humans in all tasks within the next 45 years. See Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, and Owain Evans, “When Will AI Exceed Human Performance? Evidence from AI Experts,” *Journal of Artificial Intelligence Research*. May 2017. <https://arxiv.org/abs/1705.08807>.

information. Human judgment and decision making must always remain paramount over technology, lest we endow AI-enabled machines with greater autonomy than is prudent.

MILITARY PROBLEM

The U.S. military generally, and the Marine Corps in particular, is inadequately prepared to implement and integrate AI and ML technologies in a systematic manner across the warfighting domains, despite growing recognition of the need to operate quickly, seamlessly, and coherently in a highly contested and data saturated Information Environment (IE). Commercial technologies that can rapidly convert large and diverse data sets into actionable information likely will continue to progress at an alarming rate, and these advances will present military organizations with significant opportunities to leverage as well as challenges to mitigate. Competitor nations, most notably China and to a lesser extent Russia, are counting on investments in AI technologies to gain asymmetric advantages in the information domain and in future battlespaces.^{15, 16} In the absence of codified international norms and agreements regarding military applications of AI and ML enabled systems, these competitor nations threaten to outpace the U.S. military in repurposing, implementing, and weaponizing commercial AI/ML technologies. Furthermore, competitor nations often encounter fewer legal, social, and ethical constraints to adopting new technologies for military use, which could put them in a position of advantage vis-à-vis the U.S. military in a potential AI arms race, unless the U.S. military sets

¹⁵Allen, Gregory C. "Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security." Center for a New American Security, 06 February 2019. <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.

¹⁶ Polyakova, Alina. "Weapons of the Weak: Russia and AI-driven Asymmetric Warfare." Brookings Institute, 15 November 2018. <https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare>.

favorable conditions for employing these technologies in a manner consistent with democratic values and international norms.

CENTRAL IDEA

The Marine Corps can play an important role in operationalizing AI and ML applications as it builds its capacity and capabilities to conduct Operations in the Information Environment (OIE).¹⁷ Focusing on the development and implementation of non-kinetic AI and ML applications would be less controversial than developing lethal AI-enabled autonomous weapons,¹⁸ and this approach likely would yield significant advantages in the Marine Corps' ability to sense and understand key aspects of future operating environments.¹⁹ By leveraging AI/ML investments to build robust and resilient Intelligence and Information Warfare capabilities, the Marine Corps and other U.S. Services could shape the perceptions of competitor nations and the international community writ large and perhaps dissuade adversary nations from applying AI and ML technologies in overly aggressive or provocative ways. In particular, the Marine Corps could play a key role in developing and implementing collaborative human-

¹⁷ In July 2018, the Joint Chiefs of Staff released guidance titled *Joint Concept for Operating in the Information Environment (JCOIE)*. The Marine Corps appears to be updating its 2013 *Operating Concept for Information Operations* and 2017 *Marine Air Ground Task Force (MAGTF) Information Environment Operations Concept of Employment* to align more closely with the joint concept's approach and terminology.

¹⁸ For an insightful presentation of how the U.S. military is adjusting to the evolution of automated and autonomous weapons systems, see Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company, April 2018.

¹⁹ For an assessment of the role of technology in future operating environments, see the Marine Corps Intelligence Activity (MCIA)'s, *The Future Operating Environment: Implications for Marines*, Quantico, VA, 2015, UNCLASSIFIED edition.

machine teams (sometimes known as “centaur teams”)²⁰ and augmenting intelligence collection and analysis capabilities to enhance “cognitive maneuver” in the Information domain.

First, the importance of facilitating human-machine collaboration will continue to increase as AI and ML technologies mature and become increasingly capable of conducting a wide range of tasks. In this environment, “centaur teams” will play a critical role in completing many routine and complex cognitive tasks, such as assessing potential adversaries’ order of battle and predicting probable courses of action. Such human-machine teams can leverage the speed and ability of artificially intelligent computers to rapidly process and analyze vast amounts of data from numerous different sources, to include ground, air, and space-based collection platforms, human intelligence sources, and publically available information. Additionally, the objective character of computer models and algorithms can augment the more subjective element of expert human judgment to more accurately predict future outcomes.²¹ Yet even the most technologically advanced machines lack vital attributes of human cognition, such as the ability to intuitively contextualize data and to make ethical decisions based on incomplete or ambiguous information. Therefore, it is vitally important to leave sufficient decision space within any AI-enabled systems for humans to apply judgment, expertise, and moral sensibility and to amend or override automated machine recommendations.

Furthermore, human-machine teams probably would be most effective if they include specialists with a variety of disciplinary perspectives (Human Intelligence, Signals Intelligence,

²⁰ The term “centaur team” derives from the mythical Greek beast that was half man, half horse. AI researchers have pointed out the advantages of combining human insight with machine speed and processing capacity to generate better solutions to complex problems. For an overview of this concept, see Stefik, Mark. “Half-Human, Half-Computer? Meet the Modern Centaur.” Palo Alto Research Center (PARC), 2 December 2016. <https://insights.conduent.com/conduent-blog/half-human-half-computer-meet-the-modern-centaur>.

²¹ Tetlock, Philip and Dan Gardner. *Superforecasting: The Art and Science of Prediction*. New York: Broadway Books, 2015.

Geospatial Intelligence, Open Source Intelligence, Data Science, etc.) in order to maximize the cognitive diversity of the teams and to optimize the different mental models and computer models that each team member contributes.²² These teams would function like high-speed intelligence fusion cells with AI-enabled machines operating as force multipliers and integral members of the team. The dynamic interplay between machines and humans likely will become increasingly complex as machines become more capable of learning and simulating human reasoning patterns, but genuine human judgment should continue to be the decisive element that directs human-machine interactions.²³

A second key element for conceptual development is discovering ways to integrate AI and ML capabilities with existing information systems and intelligence processes to enhance “cognitive maneuver” in the IE. The 2016 *MOC* recognizes, “changes in the operating environment and adversary capabilities drive us to increase emphasis on maneuver in the cognitive dimension.”²⁴ Operations in the IE (OIE) do not fit neatly with the traditional mode of phase-based military operations. As the *National Defense Strategy* suggests, the U.S. military operates persistently and globally in the contact layer with competitors and adversaries, especially in the cognitive dimension of the information domain.²⁵ The battle for informational and cognitive advantage will continue to be an essential precondition for conducting successful military operations. Adversaries actively will seek to exploit technologies that deny, degrade,

²² See Page, Scott. *The Diversity Bonus: How Great Teams Pay Off in the Knowledge Economy*. Princeton, NJ: Princeton University Press, 2017.

²³ Many prominent thinkers, including Stephen Hawking, have warned that AI-enabled systems could eventually develop an independent will that conflicts with that of its designer. See Hawking’s *Brief Answers to the Big Questions*. New York: Bantam Books, 2018, p. 186.

²⁴ USMC. *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. September 2016, p. 8. <https://www.mccdc.marines.mil/MOC/>.

²⁵ Department of Defense. *Summary of the 2018 National Defense of the United States of America: Sharpening the American Military’s Competitive Edge*. Arlington, VA, 2018.

<https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

distract, restrict, or otherwise obfuscate the U.S. military’s understanding of their capabilities and intentions. To generate cognitive advantage and maneuver space, new AI and ML technologies could be integrated with current Marine Corps systems to speed up intelligence processes, lighten the cognitive load on human analysts, and present decision makers with a more holistic and unbiased set of options to counter adversarial actions.

APPLICATION AND INTEGRATION OF MILITARY FUNCTIONS

Several existing and emergent AI and ML applications could be adapted to work with the Marine Corps’ intelligence and information systems to improve their functionality. For instance, intelligence specialists could use AI-enabled cognitive assistants to mitigate potential biases and prompt consideration of alternative conclusions or courses of action (COAs). The Marine Corps could leverage work by the Intelligence Advanced Research Projects Activity (IARPA), which is funding a research project called Crowdsourcing Evidence, Argumentation, Thinking and Evaluation (CREATE). This project is developing and testing systems that “use crowdsourcing and structured analytic techniques to improve analytic reasoning.”²⁶ One specific application is a cognitive assistant called Cogent, which was developed by George Mason University’s Learning Agents Center.²⁷ This application helps intelligence analysts construct probabilistic arguments based on incomplete and ambiguous evidence from multiple sources with varying degrees of credibility and relevance. Cognitive assistants, such as Cogent, could enhance the intelligence analysis that supports operational planning teams (OPTs) in various stages of the Marine Corps

²⁶ Office of the Director of National Intelligence, Intelligence Advanced Research Projects Activity (IARPA), <https://www.iarpa.gov/index.php/research-programs/create>.

²⁷ George Mason University, Learning Agents Center, <http://lac.gmu.edu/index.html>. Additional information about the theoretical foundations of the Cogent system is presented in *Intelligence Analysis as Discovery of Evidence, Hypotheses, and Arguments* by Gheorghe Tecuci, David A. Schum, Dorin Marcu, and Mihai Boicu (Cambridge: Cambridge University Press, 2016).

Planning Process (MCPPE).²⁸ Combining the powers of computational logic with the human reasoning patterns of intelligence analysts facilitates the creation of sound assessments of adversaries' capabilities and likely COAs in support of military planners and decision makers.

AI and ML applications also can perform tasks like pattern recognition and change detection faster and often more reliably than human analysts, thereby providing users with informational and cognitive advantage. Adversaries employ sophisticated AI/ML technologies to produce misinformation and propaganda in order to influence or deceive specific audiences, including U.S. citizens and military personnel.²⁹ The U.S. military could develop applications to detect and counteract adversaries' use of these technologies to produce "fake news" and "deep fake" images and videos.³⁰ Creating automated defenses against these types of offensive influence operations could reduce risks posed by adversaries' misinformation and lend credibility to the U.S. military as a more responsible broker of information.

AI and ML algorithms also can rapidly analyze large volumes of satellite imagery to detect significant changes or activities that are of interest to military intelligence organizations. Such automated analyses could allow human imagery analysts to more efficiently allocate their time, energy, and expertise. Other AI/ML algorithms could be designed to detect insider threats or network anomalies and be able to implement automated security patches in response to such anomalies. These automated systems would alert human security and network specialists who could assess the anomalies to determine appropriate follow-on actions. AI systems could also

²⁸ USMC. MCWP 5-10, *Marine Corps Planning Process*, 2 May 2016, <https://www.marines.mil/Portals/59/Publications/MCWP%205-10%20FRMLY%20MCWP%205-1.pdf?ver=2017-08-28-140131-227>.

²⁹ Padgett, Scott. "The Art of Digital Deception – Getting Left of Bang on Deep Fakes," *Small Wars Journal*, 24 April 2019. <https://smallwarsjournal.com/jrnl/art/art-digital-deception-getting-left-bang-deepfakes>.

³⁰ Several research and advocacy organizations are working to address the growing threat of misinformation in the media. See, for instance, the Berkman Klein Center for Internet and Society Project, "AI: Media and Information Quality," Harvard University, <https://cyber.harvard.edu/projects/ai-media-and-information-quality>.

support friendly forces' signature management (SIGMAN) by predicting how adversaries likely would perceive U.S. and allied forces' signals and by recommending options that would confuse or deceive adversaries' perceptions.

A popular branch of AI/ML technology known as natural language processing (NLP) allows computers to ingest large amounts of unstructured data and convert the data in to more understandable, user-friendly formats.³¹ NLP technology supports a range of useful automated applications, such as machine translation of foreign languages, speech recognition, and text-to-speech conversion. Advances in NLP enable virtual assistants (like Amazon's Alexa or Apple's Siri) to answer increasingly complex questions, as well as to generate more sophisticated sentiment analysis, produce concise summaries of large volumes of text, and even generate coherent paragraphs from limited pieces of information.³² Such NLP applications create potential vulnerabilities and security risks to military organizations that need to be mitigated; however, NLP technology can assist military personnel in comprehending large and diverse data sets and extracting key points that impact their specific missions. Experimentation and validation of NLP applications to facilitate and expedite military intelligence and information operations will be key to maintaining informational advantage.

In addition to enhancing processes typically associated with the Information and Intelligence warfighting functions, AI and ML technologies could serve a broader integrative role among all the warfighting functions. For example, AI and ML algorithms can offer enhanced expertise finders that discover and recommend links between personnel from different military occupational specialties who are working on similar problem sets or share similar

³¹ "Natural Language Processing," Techopedia.com, <https://www.techopedia.com/definition/653/natural-language-processing-nlp>.

³² Open AI is leading innovator in the field of natural language processing. See "Better Language Models and Their Implications," 14 February 2019, <https://openai.com/blog/better-language-models/>.

professional interests (similar to how Amazon and Google recommend products and tailor ads to specific users). Such automated expertise locators and recommenders will become increasingly useful as cloud architectures in Department of Defense and the Intelligence Community (IC) mature, and data sharing among military services U.S. agencies becomes more robust.^{33, 34} Ongoing experimentation with these and other emerging AI/ML technologies would create conditions for more effective OIE and could facilitate the planning and execution of future military operations across the warfighting functions. Although complete information dominance is unlikely in future battlespaces, the U.S. military must not allow competitors and adversaries to gain asymmetric informational advantages that degrade or diminish friendly capabilities. Ingenuity and adaptability of military forces will continue to be hallmarks of success as the technological terrain becomes increasingly competitive and complex.

NECESSARY CAPABILITIES

To effectively support future military operations, the Marine Corps and other Services will need to experiment with and implement a range of AI and ML capabilities across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities (DOTMLPF) spectrum. Regarding doctrine, current intelligence publications are not optimized to address the evolving technological landscape. The foundational publication, *MCDP 2: Intelligence*, is over twenty years old, and some key concepts and processes are outdated.³⁵ For example, the “intelligence cycle” depicted in *MCDP 2*, and even in more recent warfighting and

³³ Department of Defense. *DoD Cloud Strategy*, December 2018, <https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF>.

³⁴ Office of the Director of National Intelligence. “IC IT Enterprise (ICITE) Fact Sheet,” <https://www.dni.gov/files/documents/IC%20ITE%20Fact%20Sheet.pdf>.

³⁵ USMC. *Marine Corps Doctrinal Publication (MCDP) 2: Intelligence*. 7 June 1997. <https://www.marines.mil/Portals/59/Publications/MCDP%202%20Intelligence.pdf?ver=2012-10-11-164103-683>.

tactical publications,³⁶ implies a segmented and sequential method of generating useful intelligence. The cycle begins with Planning & Direction, then comes Collection, then Processing & Exploitation, then Production, then Dissemination, and finally Utilization.³⁷ However, AI and ML technologies would enable several phases in this “cycle” to be conducted simultaneously, iteratively, and/or non-sequentially. In today’s IE, the conversion of data to meaningful and useful intelligence is a more complex, dynamic process than current intelligence doctrine suggests, and the interrelationships between the parts of the process will need to be explored as AI and ML technologies are tested and implemented.

With respect to the personnel required to effectively implement AI and ML technologies, the Marine Corps would need to actively recruit more people with specialized skills in data science, coding, statistics, data engineering, and other burgeoning technological specialties. The demand for such professionals in the private sector is steadily increasing,³⁸ making it difficult for military organizations to compete with private companies that can offer higher salaries and greater career autonomy. Although some specialized technological skill sets can be contracted, the Marine Corps probably should establish inherent capabilities to perform critical tasks associated with developing, operating, and adjusting AI and ML applications. In addition to more skilled technical personnel, the Marine Corps and other Services need leadership buy-in and advocacy of senior officials who understand the threats and opportunities associated with AI and ML technologies. Military leaders at all levels likely will need familiarity with emerging AI and

³⁶ See *MCWP 2-10: Intelligence Operations*, 4 April 2018, <https://www.marines.mil/Portals/59/Publications/MCWP%202-10.pdf?ver=2018-12-20-092916-950>, and *MCTP 2-10B: MAGTF Intelligence Production and Analysis*, 4 April 2018, <https://www.marines.mil/Portals/59/Publications/MCTP%202-10B%20GN.pdf?ver=2019-01-31-111956-437>.

³⁷ USMC. *Marine Corps Doctrinal Publication (MCDP) 2: Intelligence*. 7 June 1997. <https://www.marines.mil/Portals/59/Publications/MCDP%202%20Intelligence.pdf?ver=2012-10-11-164103-683>.

³⁸ See Bureau of Labor Statistics, “Occupational Outlook Handbook,” last modified 12 April 2019, <https://www.bls.gov/ooh/fastest-growing.htm>.

ML applications and an understanding of how to navigate the unique operational and ethical challenges they entail.

Effective implementation of AI and ML applications also will necessitate changes in how the Marine Corps trains and educates personnel. While not every service member needs to be a data or programming specialist, all should have a greater awareness of how humans and machines process and use different types of data to plan and conduct military operations. Updating Training and Readiness (T&R) manuals to reflect emerging training needs with respect to data would be a worthwhile initial effort.³⁹ The Marine Corps also could offer more options and incentives for training personnel in high demand jobs, such as data science and coding, and expand learning partnerships and exchanges with private sector firms and educational institutions to broaden the perspectives and technical skill sets of personnel.

Regarding organization, facilities, and materiel, the Marine Corps appears to be fairly well positioned to begin testing and applying AI and ML capabilities. The recently established Marine Expeditionary Force (MEF) Information Group (MIG) construct provides a suitable organizational focal point for testing and fielding AI/ML applications.⁴⁰ Either MIG or MEF Intelligence Center (MIC) facilities could be used to house experimental “centaur team” collaboration cells and to experiment with other capabilities to enhance cognitive maneuver, as described above. Most of the AI/ML capabilities discussed in this concept paper do not require

³⁹ USMC. *Intelligence Training and Readiness (T&R) Manual*, 20 August 2004, <https://www.marines.mil/Portals/59/Publications/MCO%203500.32%20W%20ERRATUM.pdf?ver=2012-10-11-163624-930>.

⁴⁰ USMC. *Marine Air Ground Task Force (MAGTF) Information Environment (IE) Operations Concept of Employment*. 6 July 2017. <https://www.candp.marines.mil/Portals/216/documents/Concepts/MCFC%205-5%20MAGTF%20INFORMATION%20ENVIRONMENT%20OPERATIONS.pdf?ver=2019-02-05-130208-943>.

major upfront materiel investments, and they likely could be designed to enhance existing programs and systems.

SPATIAL AND TEMPORAL DIMENSIONS

AI and ML applications have the potential to facilitate disaggregated yet integrated operations since disparate data streams from multiple collection platforms can be collected, processed, analyzed, and synthesized almost simultaneously to provide personnel in various locations with a near real-time common operating picture. In this environment the traditional division between collection and analysis of intelligence is becoming less rigid, as some of the sensors that collect data can immediately process and run analytics on the data to determine its relevance. These technologies can speed up the “Observe, Orient, Decide, Act (O-O-D-A) Loop”⁴¹ by automating many of the observation and orientation processes so that military decision makers can concentrate on making well-informed decisions and commanding appropriate actions. In some instances, specific decisions and actions also can be automated based on criteria programmed into the AI algorithms. With advances in ML and artificial neural networks,⁴² the relationship between human judgment and automation in the decision making process is becoming ever more complex. In order to outpace competitors and adversaries, the U.S. military likely will need to adapt its decision making processes and mindsets to leverage the efficiency of AI and ML technologies, while maintaining appropriate decision space for human judgment and prudence.

⁴¹ USMC. *MCDP 6: Command and Control*, Chapter 2. 4 October 1996.

<https://www.marines.mil/Portals/59/Publications/MCDP%206%20Command%20and%20Control.pdf>.

⁴² “Artificial Neural Network,” Techopedia, accessed 25 April 2019.

<https://www.techopedia.com/definition/5967/artificial-neural-network-ann>.

CONCLUSION

As a highly adaptive and innovative institution, the Marine Corps is well-positioned to play a formative role in shaping how emerging AI/ML technologies might be adopted and integrated to support a wide range of military operations, especially across the informational dimension of war. While policy debates typically have focused on the use of artificial intelligence to enable lethal autonomous or semi-autonomous weapons, AI technology could serve numerous non-kinetic uses that raise fewer ethical concerns. While artificially intelligent machines cannot replace the ingenuity and determination inherent in Marines, new modes of collaboration between human analysts and machines could significantly increase the timeliness and utility of intelligence analysis in support of future military operations.

APPENDIX A: INSIGHTS FROM WAR GAMES

As part of the Command and Staff College's 2018-2019 Gray Scholars program, participants had the opportunity to conduct two series of wargames in conjunction with the Marine Corps Warfighting Lab and the Ellis Group. The fall semester wargames were designed to simulate how a Marine Expeditionary Unit (MEU) might operate in the contact layer to establish expeditionary advanced bases in conjunction with an allied nation while under the Anti-Access/Area Denial (A2/AD) threat umbrella of a near peer adversary (Red). This scenario yielded the following observations pertinent to this proposed concept. As the wargame unfolded, it became apparent that the Red forces had the upper hand in sensing and acting in the IE; for example, adversary forces were able to track, target, and disrupt the MEU's mobile HIMARS locations despite Blue force's attempts to maintain a small footprint and conceal its movements. Faster integration of incoming sensor data could have enabled Blue forces to counteract these threats more effectively. Additionally, while the USMC's notional autonomous capabilities

helped provide situational awareness regarding traditional military threats, the platforms were less effective in anticipating threats from Red's maritime militia and other non-conventional forces. Blue forces would have benefited from having more robust and rapid integration of multiple data sources, including more social media and cellular data along with traditional intelligence sources, to detect potential threats to the temporary Forward Arming and Refueling Points (FARPs) that they were attempting to establish on the island.

During the spring semester wargames, our Gray Scholars team focused on how a Marine Expeditionary Brigade (MEB) might prepare to support operations from afar by leveraging opportunities to engage with key partner nations in order to increase maritime domain awareness in the vicinity of key strategic chokepoints. In this scenario, the following observations appear germane to this proposed future operating concept. First is the advantage of integrating data collection and analysis capabilities with partner nations, especially in the Indo-pacific region. For example, the U.S. military could provide partners with advanced sensors that use algorithms to anticipate dangerous weather events, environmental hazards, or other threats, and our partners could share relevant information about threat activity in areas of mutual concern. In the scenario we explored, India was concerned about mounting Chinese aggressiveness in its territorial waters. The U.S. military could assist the Indian Armed Forces with AI-enabled data collection, analysis, and integration capabilities to rapidly identify and respond to emerging threats in this key maritime region.

APPENDIX B: HISTORICAL CASE STUDY

Transformative Technology and Restraint: How Key Lessons from the Nuclear Arms

Competition can Inform Military Applications of Artificial Intelligence (AI)

In recent years, numerous studies have highlighted significant implications of transformative technological advances in artificial intelligence (AI) and machine learning (ML) on the future of the national security enterprise in general and military operations more specifically.^{43, 44, 45, 46} The growing interest and concern about potential military applications of AI technology is in some ways reminiscent of challenges confronted during the nuclear arms race competition between the U.S. and Soviet governments during the Cold War.⁴⁷ Recently, visionary entrepreneur Elon Musk warned that general AI technology (that is, AI that enables machines to perform as well or better than humans in most tasks) will pose an even greater threat to human existence than nuclear weapons.⁴⁸ While such apocalyptic views of AI remain outside the mainstream, a growing body of researchers recognizes the profoundly disruptive potential of AI in the coming century.^{49, 50} The analogy to the development and subsequent restraints placed on nuclear weapons technology can be instructive and offers insight into how the U.S. military

⁴³ U.S. House of Representatives, Subcommittee on Information Technology Committee on Oversight and Government Reform, “Rise of the Machines: Artificial Intelligence and its Growing Impact on U.S. Policy,” September 2018, <https://oversight.house.gov/wp-content/uploads/2018/09/AI-White-Paper-.pdf>.

⁴⁴ Mary L. Cummings, “Artificial Intelligence and the Future of Warfare,” The Royal Institute of International Affairs, January 2017, <https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>.

⁴⁵ Richard Potember, “Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD,” The MITRE Corporation, January 2017, <https://fas.org/irp/agency/dod/jason/ai-dod.pdf>.

⁴⁶ Department of Defense Office of Net Assessment, “Summer Study: (Artificial) Intelligence: What questions should DoD be asking?” July 2016.

⁴⁷ Greg Allen and Taniel Chan, “Artificial Intelligence and National Security,” Harvard Belfer Center Study, July 2017, <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>. Allen and Chan explore four transformative technology case studies that are relevant to the development of AI technology, namely: nuclear, aerospace, cyber, and biotech. While each of these cases is helpful, the nuclear weapons example provides the most vivid comparison to the potential weaponization of AI technologies.

⁴⁸ At the March 2018 South by Southwest technology conference, Musk, a visionary entrepreneur who work with cutting edge AI technology, stated boldly, “Mark my words — A.I. is far more dangerous than nukes.” <https://www.cnn.com/2018/03/13/elon-musk-at-sxsw-ai-is-more-dangerous-than-nuclear-weapons.html>.

⁴⁹ Stanford’s One Hundred Year Study on Artificial Intelligence (AI100), “Artificial Intelligence and Life in 2030: Report of the 2015 Study Panel,” September 2016, <https://ai100.stanford.edu/2016-report>. This report concludes, “Contrary to the more fantastic predictions for AI in the popular press, the Study Panel found no cause for concern that AI is an imminent threat to humankind.”

⁵⁰ Katja Grace, John Salvatier, Allan Dafoe, Baobao Zhang, and Owain Evans, “When Will AI Exceed Human Performance? Evidence from AI Experts,” *Journal of Artificial Intelligence Research*, May 2017. <https://arxiv.org/abs/1705.08807>. According to this study, “Researchers believe there is a 50% chance of AI outperforming humans in all tasks in 45 years and of automating all human jobs in 120 years, with Asian respondents expecting these dates much sooner than North Americans.”

might pursue development of AI capabilities that fit within an internationally recognized system of legal, ethical, and social restraints to help prevent catastrophic doomsday scenarios.

While there is no scholarly or industry consensus regarding the suitability of comparing the development of nuclear and AI technologies, apparent parallels warrant at least an initial “plausibility probe” to explore potential implications.⁵¹ This paper hypothesizes that some of the general processes and mechanisms that encouraged restraint during the nuclear arms competition could provide a framework for proactively addressing dangers associated with rapid advances in AI technology. These processes include 1) recognition of a potential existential threat, 2) promotion of regulations and restrictions to avoid catastrophic scenarios, 3) development of competitive strategies to deter or offset the threat, and 4) improvement of assessment mechanisms to gauge relative advantages in capabilities.

Although obvious differences exist between the development nuclear weapons and the potential for AI-enabled autonomous weapon systems, the lessons of Cold War history should at least give pause to those developing, implementing, and regulating AI technologies for military use. In particular, Marine Corps leaders, planners, and capabilities developers, can benefit from such a study as the institution seeks to anticipate future technological challenges in increasingly complex operating environments. By implementing AI technologies that provide cognitive advantage in complex and contested information environments, the USMC could better defend against and deter adversaries who might use emerging AI technologies for nefarious purposes.

BACKGROUND

Nuclear weapons provide the most vivid example of the cataclysmic power that transformative technology can unleash on the battlefield and the devastating consequences of

⁵¹ Jack Levy, “Case Studies: Types, Designs, and Logics of Inference,” *Conflict Management and Peace Science*, 25:1–18, 2008, <https://journals.sagepub.com/doi/10.1080/07388940701860318>.

such power for humankind. When atomic bombs annihilated the cities of Hiroshima and Nagasaki, Japan in 1945, the world witnessed unprecedented destruction and entered a new era of international relations commonly known as the Cold War.⁵² This era was characterized not only by great power competition to acquire technological and weapons superiority, especially as manifest in the nuclear arms race between the U.S. and USSR, but also by the development of an elaborate system of internal and international restraints designed to prevent a World War of annihilation.⁵³ Several regulatory bodies were created to mitigate the nuclear threat, including the U.S. Atomic Energy Commission (AEC) in 1946, which became the Nuclear Regulatory Commission (NRC) in 1975,⁵⁴ as well as the International Atomic Energy Agency (IAEA) in 1957.⁵⁵ Additionally, numerous arms control treaties were implemented, including the Test Ban Treaty of 1963, the Nuclear Non-Proliferation Treaty of 1968, the Anti-Ballistic Missile Treaty and the Interim Agreement on the Limitation of Strategic Offensive Arms of 1972, the Strategic Arms Limitation Treaty (SALT) II of 1979, and Intermediate-Range Nuclear Forces (INF) Treaty of 1987.⁵⁶ In addition to regulatory and diplomatic pressure, ethical arguments and social pressures helped create a “nuclear taboo” that restrained nations from employing atomic weapons.⁵⁷ When the Soviet Union collapsed in 1991, the Cold War officially ended after nearly half a decade without a major direct conflict between the world’s two nuclear superpowers.

⁵² The term “cold war” was coined by George Orwell in “You and the Atom Bomb,” *London Tribune*, October 1945, <https://www.orwellfoundation.com/the-orwell-foundation/orwell/essays-and-other-works/you-and-the-atom-bomb>. The term was popularized by journalist Walter Lippmann in “The Cold War: A Study in U.S. Foreign Policy,” *Harper*, 1947. <https://babel.hathitrust.org/cgi/pt?id=mdp.39015002588997>.

⁵³ Cold War: A Brief History, <http://www.atomicarchive.com/History/coldwar/index.shtml>.

⁵⁴ J. Samuel Walker and Thomas R. Wellock, *A Short History of Nuclear Regulation, 1946-2009*, U.S. Nuclear Regulatory Commission, October 2010, <https://www.nrc.gov/docs/ML1029/ML102980443.pdf>.

⁵⁵ International Atomic Energy Agency (IAEA), <https://www.iaea.org/about/overview/history>.

⁵⁶ Atomic Archive Online, *Arms Control Treaties*, <http://www.atomicarchive.com/Treaties/index.shtml>.

⁵⁷ Nina Tannenwald, “Stigmatizing the Bomb: Origins of the Nuclear Taboo,” *International Security*, Vol. 29, No. 4 (Spring 2005), 5–49, https://www.belfercenter.org/sites/default/files/files/publication/intsec29-4_tannenwald.pdf. Tannenwald provides detailed analysis of how the nuclear taboo developed in international politics and U.S. policy.

Perspectives on the efficacy and enduring legacy of the nuclear arms competition abound. Three common schools of thought are the traditionalists (who regard Soviet expansionist ambitions as the main driver of the nuclear competition), revisionists (who regard America's desire for hegemonic power as the main determinant) and post-revisionists (who regard the Cold War as an inevitable consequence of balance of power politics). Another more recent interpretation is offered by renowned international relations scholar Graham Allison, who cites the U.S.-Soviet Cold War case as one of the rare examples in which rival superpowers managed to avoid the Thucydides' Trap, the phenomenon whereby ruling powers tend to engage in armed conflict with rising powers. Allison notes, "By developing vehicles for competition outside of armed conflict, the two powers peacefully managed the highest-stakes great power competition in history."⁵⁸ From this perspective, exploring the U.S.-Soviet nuclear rivalry can provide insight contemporary challenges regarding great power competition in the technological, economic, informational, and military realms.

The Nuclear Arms Race Case

The nuclear arms competition during the Cold War serves as an instructive case study for how to manage strategic competition among superpowers under the umbrella of enormous destructive capacity of transformative weapons technology. While detailed process tracing of key events in the nuclear arms race is well beyond the scope of this brief case study, the following four highly generalized observations from the era highlight pertinent lessons that can be drawn from studying the case.

⁵⁸ Graham Allison, *Destined for War: Can America and China Escape Thucydides's Trap?*, Houghton Mifflin Harcourt: New York, 2017, 281-283. The "Thucydides Trap" case files are also available online at <https://www.belfercenter.org/thucydides-trap/case-file>.

The first key lesson to be drawn from the nuclear arms case is that the potential existential threat posed by nuclear weapons was not fully realized until after the weapons were used. For example, Japan initially scoffed at the Potsdam Declaration, which threatened “the inevitable and complete destruction of the Japanese armed forces and just as inevitably the utter devastation of the Japanese homeland” unless Japan agreed to unconditional surrender.⁵⁹ Not until the atomic bombs were dropped did Japan or the rest of the world realize their destructive potential. Similarly, the destructive potential of thermobaric hydrogen bombs surprised even nuclear scientists. The hydrogen bomb test of “Mike” in 1952 created a larger cloud and crater than anticipated, and the detonation of “BRAVO” in 1954 yielded nearly three times the predicted destructive yield.⁶⁰

A second important lesson from the nuclear arms race case is that legal, ethical, and social restraints can evolve to reduce the likelihood of catastrophic scenarios unfolding. As mentioned above, numerous regulatory agencies and treaties were developed during the Cold War to limit the proliferation and use of nuclear weapons. Additionally, ethical principles of just war theory evolved to consider new dangers posed by nuclear weapons in decisions of when to use military force (*ius ad bellum*) and how military force might be used appropriately in a conflict (*ius in bello*). Moreover societal pressures and intentional norms evolved to create a taboo against the use of nuclear weapons.⁶¹ The combination of legal, moral, and social pressures exerted significant influence on national policies and likely helped to avert a nuclear Armageddon.

⁵⁹ The Potsdam Declaration, 26 July 1945, posted at <http://afe.easia.columbia.edu/ps/japan/potsdam.pdf>.

⁶⁰ The Atomic Archive, “Cold War: A Brief History,”
<http://www.atomicarchive.com/History/coldwar/page05.shtml>,
<http://www.atomicarchive.com/History/coldwar/page06.shtml>.

⁶¹ Nina Tannenwald, “Stigmatizing the Bomb: Origins of the Nuclear Taboo,” *International Security*, Vol. 29, No. 4 (Spring 2005), 5–49, https://www.belfercenter.org/sites/default/files/files/publication/intsec29-4_tannenwald.pdf.

Third, the strategies developed during the Cold War to counter the existential nuclear threat, most notably deterrence and détente, provide valuable lessons for how to navigate great power competition. The basic goal of the U.S. nuclear deterrence strategy was to convince potential adversaries that the danger of initiating nuclear war against the U.S. or our allies would greatly outweigh any advantages they might hope to attain.⁶² A corollary to this strategy was the concept of “mutual assured destruction,” whereby the U.S. would retain the capability to annihilate an adversary even if that adversary initiated an offensive nuclear strike against the U.S. This concept was supported by the development of the nuclear triad, which allowed the U.S. to maintain a robust second strike capability even if attacked. These competitive strategies provided a strong incentive for nuclear superpowers not to engage in overly provocative actions against one another.

A final lesson can be discerned from the improved methods that were developed during the latter stages of the Cold War to assess relative military capabilities. The Office of Net Assessment was created in 1972 to serve as the Department of Defense’s think tank regarding future trends in military capabilities. The office was headed by Andy Marshall, who published an influential study titled, “Long-Term Competition with the Soviets: A Framework for Strategic Analysis.” Marshall’s work at the Office of Net Assessment helped create a more robust analytic framework “for evaluating the long-term strategic political-military competitions in which states engage.”⁶³ The implementation of a multi-disciplinary, forward looking approach to assessing relative military capabilities empowered policy makers and military decision makers with more useful, insightful, and accurate information about both enemy and friendly capabilities.

⁶² Richard C. Bush, Vanda Felbab-Brown, Martin S. Indyk, Michael E. O’Hanlon, Steven Pifer, and Kenneth M. Pollack, “U.S. Nuclear and Extended Deterrence: Considerations and Challenges,” *The Brookings Institution*, June 2010, <https://www.brookings.edu/research/u-s-nuclear-and-extended-deterrence-considerations-and-challenges>.

⁶³ Thomas M. Skypek, “Evaluating Military Balances Through the Lens of Net Assessment: History and Application,” *Journal of Military and Strategic Studies*, Vol 12, Issue 2, Winter 2010.

The legacy of the Cold War’s nuclear arms competition remains relevant and influential as an era of great power competition has returned to the strategic forefront. The 2017 *National Security Strategy of the United States of America* identifies revisionist powers of Russia and China as the primary threat to U.S. security.⁶⁴ Similarly, the *National Defense Strategy* of 2018 affirms, “The central challenge to U.S. prosperity and security is the reemergence of long-term, strategic competition by what the National Security Strategy classifies as revisionist powers.”⁶⁵ In the media and in academic circles there are frequent references to an “economic cold war” between the U.S. and China over tariffs, the theft of intellectual property, and predatory economic practices.⁶⁶ As the world’s great powers continue to compete vigorously in the economic, technological, informational, and military spheres, lessons from the nuclear arms competition will remain pertinent to contemporary national security challenges.

The elaborate system of restraints, strategies, and methods of assessment developed during the Cold War to counter the existential threat of nuclear annihilation serves as an illustrative case study for considering how the U.S. might pursue the development, implementation, and regulation of AI technologies so they enhance military capabilities and competitive advantages while avoiding miscalculations or misunderstandings that could have catastrophic consequences. A recent study on “Artificial Intelligence and National Security,” notes similarities as well as significant differences between the nuclear technology case and the

⁶⁴ White House, *National Security Strategy of the United States of America*, December 2017, p. 25, <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.

⁶⁵ Department of Defense, *Summary of the National Defense Strategy of the United States of America: Sharpening American Military’s Competitive Edge*, 2018, p. 2, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

⁶⁶ Recent articles include titles like, “China-U.S. Trade Spat Is Just a Start to the Economic Cold War,” <https://www.bloomberg.com/opinion/articles/2018-08-13/china-u-s-trade-spat-is-just-a-start-to-the-economic-cold-war>; “An Economic Cold War Looms Between the U.S. and China,” <https://www.wsj.com/articles/an-economic-cold-war-looms-between-the-u-s-and-china-1537968600>; and “Some Fear an Economic Cold War as Trump and Xi Meet at G-20,” <http://time.com/5467258/trump-xi-g20-economy>.

development of AI technology.⁶⁷ Both technologies have transformative, if not revolutionary, potential to disrupt national and international bases of power and radically alter the strategic landscape.

Conspicuous differences between the nuclear case and the AI case, however, must be acknowledged. First, the primary purpose of developing nuclear technology was to use it as a weapon of war, as Secretary of War Henry Stimson noted in his 1947 article “The Decision to Use the Bomb.”⁶⁸ On the other hand, most AI developers have explicitly renounced using the technology to create autonomous weapon systems, and some have protested against providing even limited support to military operations.⁶⁹ Second, whereas the development of nuclear technology was funded primarily by governments, research and design (R&D) funding for AI technology has come mostly from the private sector. While U.S. government organizations like the Defense Advanced Research Projects Agency (DARPA) have provided funding for R&D related to AI for decades, the public sector has struggled to keep up with the pace of private sector investments and advances.⁷⁰ Third, from the onset nuclear technology was controlled, regulated, and highly classified by national governments. In contrast, there has been much less government oversight and regulation of AI technological developments, and a great deal of AI technology is shared openly with (or easily acquired by) other nations, enabling greater collaboration and innovation but also raising risks that the technology might be used by malign

⁶⁷ Greg Allen and Taniel Chan, “Artificial Intelligence and National Security,” Harvard Belfer Center Study, July 2017, <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>.

⁶⁸ Henry Lewis Stimson, “The Decision to Use the Bomb,” *Harper’s Magazine*, February 1947, reproduced at http://afe.easia.columbia.edu/ps/japan/stimson_harpers.pdf.

⁶⁹ Paresh Dave and Heather Somerville, “Google Plans not to Renew Military Deal Protested by Employees: Source,” *Reuters*, <https://www.reuters.com/article/us-alphabet-defense/google-plans-not-to-renew-military-deal-protested-by-employees-source-idUSKCN1IX5YB>.

⁷⁰ Recent initiatives like DARPA’s AI Next Campaign and Artificial Intelligence Exploration (AIE) program aim to mitigate the gap between public and private sector AI technological advancement. See <https://www.darpa.mil/work-with-us/ai-next-campaign>; <https://www.darpa.mil/news-events/2018-07-20a>.

actors. These notable differences between the development of nuclear and AI technologies reveal both potential dangers to be mitigated and opportunities to be leveraged as the U.S. military in general, and USMC in particular, seeks to implement AI-enabled systems that provide a technological edge over its strategic competitors and potential adversaries.

BIBLIOGRAPHY

- Allen, Gregory and Taniel Chan. “Artificial Intelligence and National Security,” Harvard Belfer Center Study, July 2017. <https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf>.
- Allen, Gregory. “Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security,” Center for a New American Security, 06 February 2019. <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy>.
- Allison, Graham. *Destined for War: Can America and China Escape Thucydides’s Trap?* New York: Houghton Mifflin Harcourt, 2017. <https://www.belfercenter.org/thucydides-trap/case-file>.

Bush, Richard C., Vanda Felbab-Brown, Martin S. Indyk, Michael E. O’Hanlon, Steven Pifer, and Kenneth M Pollack. “U.S. Nuclear and Extended Deterrence: Considerations and Challenges,” *The Brookings Institution*, June 2010.

<https://www.brookings.edu/research/u-s-nuclear-and-extended-deterrence-considerations-and-challenges>.

Carter, William, Emma Kinnucan, and Josh Elliot. *A National Machine Intelligence Strategy for the United States*. Washington, DC: Center for Strategic and International Studies (CSIS), March 2018. <https://www.csis.org/events/national-machine-intelligence-strategy-united-states>.

Chairman of the Joint Chiefs of Staff (CJCS). *Joint Capabilities Integration and Development System (JCIDS)*, CJCSI 3170.011. 23 January 2015.

https://dap.dau.mil/policy/Documents/2015/CJCSI_3170_011.pdf.

Chairman of the Joint Chiefs of Staff (CJCS). *Joint Concept for Operating in the Information Environment (JCOIE)*, 25 July 2018.

https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.

Chairman of the Joint Chiefs of Staff (CJCS). *Joint Publication (JP) 1: Doctrine for the Armed Forces of the United States*, updated 12 July 2017.

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf?ver=2017-12-23-160207-587.

Clausewitz, Carl von. *On War*. Edited and translated by Michael E. Howard and Peter Paret. Princeton University Press, 1984.

Cummings, Mary L. “Artificial Intelligence and the Future of Warfare,” London: The Royal Institute of International Affairs, January 2017.

<https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf>.

Defense Advanced Research Project Activity (DARPA). *AI Next Campaign*.

<https://www.darpa.mil/work-with-us/ai-next-campaign>.

Department of Defense. *Summary of the National Defense Strategy of the United States of America: Sharpening American Military's Competitive Edge*, 2018.

<https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

Department of Defense Office of Net Assessment. "Summer Study: (Artificial) Intelligence: What questions should DoD be asking?" July 2016.

Department of Homeland Security. *Artificial Intelligence: Narrative Analysis Research Paper*. July 2017.

Gelder, Tim van. "Crowdsourcing Security Intelligence." 13 June, 2018.

<https://www.labonline.com.au/content/computing-hardware-software/article/crowdsourcing-security-intelligence-398933309>.

George Mason University, Learning Agents Center. <http://lac.gmu.edu/index.html>. Cogent Training Resources. <https://sites.google.com/site/learncogent/>.

Grace, Katja, John Salvatier, Allan Dafoe, Baobao Zhang, and Owain Evans, "When Will AI Exceed Human Performance? Evidence from AI Experts," *Journal of Artificial Intelligence Research*, May 2017. <https://arxiv.org/abs/1705.08807>.

Hawking, Stephen. *Brief Answers to the Big Questions*. New York: Bantam Books, 2018.

Ilachinski, Andrew. *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies*.

CNA, January 2017. https://www.cna.org/cna_files/pdf/DRM-2017-U-014796-Final.pdf.

- Intelligence Advanced Research Programs Activity (IARPA). Crowdsourcing Evidence, Argumentation, Thinking and Evaluation (CREATE) Program.
<https://www.iarpa.gov/index.php/research-programs/create>.
- Kania, Elsa B. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*. Washington, DC: Center for a New American Security (CNAS), November 2017. <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.
- Kimmons, Jeff and Graham Gilmer. *Analyst 2.0: Redefining the Analysis Tradecraft*. McLean, VA: Booz Allen Hamilton Inc., 31 October 2018.
- Kuhn, Thomas S. *The Structure of Scientific Revolutions, 4th Edition*. Chicago: University of Chicago Press, 2012.
- Levy, Jack. "Case Studies: Types, Designs, and Logics of Inference," *Conflict Management and Peace Science*, 25:1–18, 2008.
<https://journals.sagepub.com/doi/10.1080/07388940701860318>.
- Office of the Director of National Intelligence (ODNI). *National Intelligence Strategy of the United States of America*, 2019.
https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.
- Padgett, Scott. "The Art of Digital Deception – Getting Left of Bang on Deep Fakes." *Small Wars Journal*, 24 April 2019. <https://smallwarsjournal.com/jrnl/art/art-digital-deception-getting-left-bang-deepfakes>.
- Page, Scott. *The Diversity Bonus: How Great Teams Pay Off in the Knowledge Economy*. Princeton, NJ: Princeton University Press, 2017.
- Paresh, Dave and Heather Somerville. "Google Plans not to Renew Military Deal Protested by Employees: Source," Reuters, 1 June 2018. <https://www.reuters.com/article/us-alphabet->

[defense/google-plans-not-to-renew-military-deal-protested-by-employees-source-idUSKCN1IX5YB.](https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare)

Polyakova, Alina. “Weapons of the Weak: Russia and AI-driven Asymmetric Warfare,”

Brookings Institute, 15 November 2018. [https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare.](https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare)

Potember, Richard. “Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD,” The MITRE Corporation, January 2017.

[https://fas.org/irp/agency/dod/jason/ai-dod.pdf.](https://fas.org/irp/agency/dod/jason/ai-dod.pdf)

Scharre, Paul. *Army of None: Autonomous Weapons and the Future of War*. New York: W. W. Norton & Company, April 2018.

Schmitt, John F. *A Practical Guide for Developing and Writing Military Concepts*. Defense Adaptive Red Team (DART) Working Paper #02-4. McLean, VA: Hicks & Associates, Inc., December 2002.

[http://www.au.af.mil/au/awc/awcgate/writing/dart_paper_writing_mil_concepts.pdf.](http://www.au.af.mil/au/awc/awcgate/writing/dart_paper_writing_mil_concepts.pdf)

Skypek, Thomas M. “Evaluating Military Balances Through the Lens of Net Assessment: History and Application,” *Journal of Military and Strategic Studies*, Vol 12, Issue 2, Winter 2010.

Stanford’s One Hundred Year Study on Artificial Intelligence (AI100), “Artificial Intelligence and Life in 2030: Report of the 2015 Study Panel,” September 2016.

[https://ai100.stanford.edu/2016-report.](https://ai100.stanford.edu/2016-report)

Stimson, Henry Lewis. “The Decision to Use the Bomb,” *Harper’s Magazine*, February 1947, reproduced at [http://afe.easia.columbia.edu/ps/japan/stimson_harpers.pdf.](http://afe.easia.columbia.edu/ps/japan/stimson_harpers.pdf)

Tannenwald, Nina. “Stigmatizing the Bomb: Origins of the Nuclear Taboo.” *International Security*, Vol. 29, No. 4 (Spring 2005).

https://www.belfercenter.org/sites/default/files/files/publication/intsec29-4_tannenwald.pdf.

Tecuci, Gheorghe, David Schum, Dorin Marcu, and Mihai Boicu. *Intelligence Analysis as Discovery of Evidence, Hypotheses, and Arguments*. Cambridge: Cambridge University Press, 2016.

Tetlock, Philip and Dan Gardner. *Superforecasting: The Art and Science of Prediction*. New York: Broadway Books, 2015.

U.S. House of Representatives, Subcommittee on Information Technology Committee on Oversight and Government Reform, “Rise of the Machines: Artificial Intelligence and its Growing Impact on U.S. Policy,” September 2018. <https://oversight.house.gov/wp-content/uploads/2018/09/AI-White-Paper-.pdf>.

USMC/Army. *Marine Corps Reference Publication (MCRP) 2-10B.1/Army Tactical Publication (ATP) 2-01.3, Intelligence Preparation of the Battlefield/Battlespace*. November 2014. <https://www.marines.mil/Portals/59/MCRP%202-10B.1.pdf?ver=2018-10-04-131000-610>.

USMC/Army. *Multi-Domain-Battle: Combined Arms for the 21st Century*, United States Army-Marine Corps White Paper. <https://ccc.amedd.army.mil/PolicyPositions/Multi-Domain%20Battle%20-%20Combined%20Arms%20for%20the%2021st%20Century.pdf>

USMC. *Expeditionary Advanced Basing Operations (EABO)*, UNCLASSIFIED Summary. <https://www.candp.marines.mil/Concepts/Subordinate-Operating-Concepts/Expeditionary-Advanced-Base-Operations>.

USMC. *The Future Operating Environment: Implications for Marines*. Quantico, VA: Marine Corps Intelligence Activity, 2015.

USMC. *Littoral Operations in a Contested Environment (LOCE)*, UNCLASSIFIED Edition.

https://www.candp.marines.mil/Portals/216/documents/Concepts/LOCE%20full%20size%20edition_0.pdf?ver=2018-05-01-133728-797.

USMC. *Marine Air Ground Task Force (MAGTF) Information Environment (IE) Operations Concept of Employment*. 6 July 2017.

<https://www.candp.marines.mil/Portals/216/documents/Concepts/MCFC%205-5%20MAGTF%20INFORMATION%20ENVIRONMENT%20OPERATIONS.pdf?ver=2019-02-05-130208-943>.

USMC. *Marine Corps Bulletin (MCBul) 5400: ESTABLISHMENT OF INFORMATION AS THE SEVENTH MARINE CORPS WARFIGHTING FUNCTION*. 17 January 2019.

<https://www.marines.mil/Portals/59/Publications/MCBUL%205400.pdf?ver=2019-02-06-082807-103>.

USMC. *Marine Corps Doctrinal Publication (MCDP) 2: Intelligence*. 7 June 1997.

<https://www.marines.mil/Portals/59/Publications/MCDP%202%20Intelligence.pdf?ver=2012-10-11-164103-683>.

USMC. *MCDP 6: Command and Control*. 4 October 1996.

<https://www.marines.mil/Portals/59/Publications/MCDP%206%20Command%20and%20Control.pdf>.

USMC. *Marine Corps Operating Concept: How an Expeditionary Force Operates in the 21st Century*. September 2016. <https://www.mccdc.marines.mil/MOC/>.

USMC. *Marine Corps Operating Concept for Information Operations*. 4 February 2013.

<https://www.candp.marines.mil/Portals/216/documents/Concepts/Marine%20Corps%20Operating%20Concept%20for%20IO.pdf?ver=2018-05-01-133727-983>.

USMC. *Marine Corps Tactics Publication (MCTP) 2-10B: MAGTF Intelligence Production and Analysis*. 4 April 2018. <https://www.marines.mil/Portals/59/Publications/MCTP%202-10B%20GN.pdf?ver=2019-01-31-111956-437>.

USMC. *Marine Corps Warfighting Publication (MCWP) 2-10, Intelligence Operations*. 4 April 2018. <https://www.marines.mil/Portals/59/Publications/MCWP%202-10.pdf?ver=2018-12-20-092916-950>.

USMC. *Marine Corps Warfighting Publication (MCWP) 5-10, Marine Corps Planning Process*. 2 May 2016. <https://www.marines.mil/Portals/59/Publications/MCWP%205-10%20FRMLY%20MCWP%205-1.pdf?ver=2017-08-28-140131-227>.

Walker, J. Samuel and Thomas R. Wellock. *A Short History of Nuclear Regulation, 1946-2009*. U.S. Nuclear Regulatory Commission, October 2010. <https://www.nrc.gov/docs/ML1029/ML102980443.pdf>.

White House. *National Security Strategy of the United States of America*. December 2017. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>.