

WHY THE DOD IS LOSING ITS ASYMMETRIC ROBOTICS AND AUTONOMOUS
SYSTEMS ADVANTAGE: AN ARGUMENT FOR THE CONCEPT OF
AUTONOMOUS FUNCTIONING WITHIN A SYSTEM

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE
Art of War Scholars

by

ARIEL M. SCHUETZ, MAJ, US ARMY
B.A., Tulane University, New Orleans, Louisiana, 2005

Fort Leavenworth, Kansas
2018

Fair use determination or copyright permission has been obtained for the inclusion of pictures, maps, graphics, and any other works incorporated into this manuscript. A work of the United States Government is not subject to copyright, however further publication or sale of copyrighted images is not permissible.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 15-06-2018		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) AUG 2017 – JUN 2018	
4. TITLE AND SUBTITLE Why the DoD is Losing its Asymmetric Robotics and Autonomous Systems Advantage: An Argument for the Concept of Autonomous Functioning Within a System				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
				5d. PROJECT NUMBER	
6. AUTHOR(S) Ariel M. Schuetz, MAJ				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
				8. PERFORMING ORG REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD Fort Leavenworth, KS 66027-2301					
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution is Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT As outlined in the National Security Strategy, National Defense Strategy and the “Third Offset Strategy”, the Department of Defense (DoD) is attempting to rapidly develop, acquire, and field increasingly autonomous technology in order to gain an asymmetric advantage over peer competitors. Issues with policy, doctrine, leadership, and acquisition are preventing the DoD from achieving these goals. The DoD lacks a conceptual framework that describes the physical and cognitive ways that humans and machines interact. This has resulted in leadership focusing on retaining humans in essential roles rather than capitalizing on the abilities that human machine teams provide. The private sector is developing information technology at a rate that the DoD is unable to keep pace with. The result that the private sector is increasingly driving the DoD's requirements based on available Commercial technology. This results in a technology gap between the DoD's required capabilities and those that are readily available to all parties within the commercial sector. The author's hypothesis is that the DoD could rapidly develop, acquire, and integrate RAS to retain a competitive advantage by re-framing the way that they conceptualize and define AI and autonomy in the realms of policy, doctrine, leadership, and materiel.					
15. SUBJECT TERMS Autonomy, Artificial Intelligence, Robotics, 3rd Offset Strategy, Unmanned Aircraft Systems, UAS, Remotely Piloted Aircraft, RPA					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. PHONE NUMBER (include area code)
(U)	(U)	(U)	(U)	159	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Ariel M. Schuetz

Thesis Title: Why the DoD is Losing its Asymmetric Robotics and Autonomous Systems Advantage: An Argument for the Concept of Autonomous Functioning Within a System

Approved by:

_____, Thesis Committee Chair
Jacob A. Mong, M.A.

_____, Member
Phillip G. Pattee, Ph.D.

_____, Member
MAJ Joel W. Bier, MMAS

Accepted this 15th day of June 2018 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

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

ABSTRACT

WHY THE DOD IS LOSING ITS ASYMETRIC ROBOTICS ADVANTAGE: AN ARGUMENT FOR THE CONCEPT OF AUTONOMOUS FUNCTIONING WITHIN A SYSTEM, by MAJ Ariel M. Schuetz, 159 pages.

As outlined in the National Security Strategy, National Defense Strategy and the “Third Offset Strategy”, the Department of Defense (DoD) is attempting to rapidly develop, acquire, and field increasingly autonomous technology in order to gain an asymmetric advantage over peer competitors. Issues with policy, doctrine, leadership, and acquisition are preventing the DoD from achieving these goals.

The DoD lacks a conceptual framework that describes the physical and cognitive ways that humans and machines interact. This has resulted in leadership focusing on retaining humans in essential roles rather than capitalizing on the abilities that human machine teams provide.

The private sector is developing information technology at a rate that the DoD is unable to keep pace with. The result that the private sector is increasingly driving the DoD’s requirements based on available Commercial technology. This results in a technology gap between the DoD’s required capabilities and those that are readily available to all parties within the commercial sector.

The author’s hypothesis is that the DoD could rapidly develop, acquire, and integrate RAS to retain a competitive advantage by re-framing the way that they conceptualize and define AI and autonomy in the realms of policy, doctrine, leadership, and materiel.

ACKNOWLEDGMENTS

My husband Max and children Felix and Leonie have been an incredible source of support during the last year, I can't thank them enough for putting up with my countless days working in the library, research trips, and long nights spent writing on the couch.

First, I would like to thank COL Thomas von Eschenbach and COL Paul Cravey for recommending this topic, I have truly enjoyed continuing to work with them to benefit the Army aviation community. I also truly appreciate the assistance of Paul Scharre, Dr. Missy Cummings, and Ian MacLeod during my research. Their guidance and suggestions have been invaluable to this project. Thank you to LTC Jason West and Dr. Owen Gaden for their support in linking me in with the right people during my research trip to Washington DC and continuing support for my work. It's also been a pleasure working with LTC Thomas Tauer and Mr. Shawn Steene, I greatly appreciate your willingness to consider my proposals and discuss ways to improve DoD RAS.

Huge thanks to LTC Noah Spataro, Tim Healy, Nicole Bier, and Aaron Brown who have helped me constantly throughout this research from laying the foundation of my AI and autonomy knowledge to framing the walls and eventually putting the shingles on the roof. I could not have done this without your constant assistance and encouragement, especially the time all of you took to explain very complex concepts to me (sometimes repeatedly)!

Lastly, I would like to thank the faculty and staff of the Command and General Staff college specifically Mr. Jacob Mong, Dr. Philip Pattee, MAJ Joel Bier, and Dr. Dean Nowowiejski. I have learned so much from all of you this year and truly appreciate the help and guidance that you and the Art of War Scholars program have provided.

TABLE OF CONTENTS

	Page
MASTER OF MILITARY ART AND SCIENCE THESIS APPROVAL PAGE	iii
ABSTRACT.....	iv
ACKNOWLEDGMENTS	v
TABLE OF CONTENTS.....	vii
ACRONYMS.....	ix
ILLUSTRATIONS	xi
TABLES	xiii
CHAPTER 1 INTRODUCTION	1
Assessment of Capabilities, Gaps, and Mitigations.....	8
Research Questions	11
Assumptions.....	12
Limitations	13
Scope and Delimitations	13
Aim and Relevance of Research	14
Summary and Conclusion	15
CHAPTER 2 LITERATURE REVIEW	16
Introduction.....	16
Background: Framing the Spectrum of Autonomy.....	16
Background: Defining Autonomy	21
Background on the DoD's Approach to Framing and Developing Autonomy	29
Categorical and Linear Scales.....	30
Multi-Dimensional Scales.....	33
Contextual Scales.....	37
Current DoD Framework for Autonomy: The Joint Concept for Robotics and Autonomous Systems	43
Strategic Guidance and Policy for Autonomy and AI	45
CHAPTER 3 RESEARCH METHODOLOGY	55
Introduction.....	55
Primary Research Method	55

CHAPTER 4 ANALYSIS	57
Analysis of the US RAS Development Relative to Peer Competitors	57
Gap 1: Policy	67
Gap 2: Doctrine.....	79
Gap 3: Leadership.....	89
Gap 4: Material	90
Addressing Acquisition Challenges	90
Innovation versus Adaptation: Changing Culture to become “Fast Followers”	106
CHAPTER 5 CONCLUSIONS AND RECOMMENDATIONS	122
Conclusions.....	122
Recommendations.....	123
Recommendations for Policy and Doctrine	126
Recommendations for Leadership	128
Recommendations for Acquisition.....	130
GLOSSARY	136
BIBLIOGRAPHY	142

ACRONYMS

3OS	Third Offset Strategy
AI	Artificial intelligence
ALFUS	Autonomous Levels for Unmanned Systems Framework
CJCS	Chairman of the Joint Chiefs of Staff
CNA	Center for Naval Analyses
COTS	Commercial off the shelf
CRC	Concept Required Capability
DAS	Defense Acquisition System
DIUx	Defense Innovation Unit Experimental
DoD	Department of Defense
DoDD	Department of Defense Directives
DoDI	Department of Defense Instructions
DOTMLPF-P	Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Policy
DSB	Defense Science Board
IT	Information Technology
JCRAS	Joint Concept for Robotics and Autonomous Systems
JCIDS	Joint Capability Integration and Development System
NDS	National Defense Strategy
NSIB	National Security Innovation Base
NSS	National Security Strategy
R&D	Research and Development
RAP	Rapid Acquisition Process

RAS	Robotics and Autonomous Systems
RDT&E	Research, Development, Testing and Evaluation
S&T	Science and Technology
T&E	Testing and Evaluation
UAS	Unmanned Aircraft Systems
USAF	United States Air Force

ILLUSTRATIONS

	Page
Figure 1. The Spectrum of Autonomy.....	18
Figure 2. How to Determine Autonomous Functioning within a System	19
Figure 3. Defining Autonomy	21
Figure 4. Automation versus Autonomy	23
Figure 5. Department of the Navy Taxonomy of UxS	25
Figure 6. ALFUS Linear Scale Illustration	31
Figure 7. USAF Flexible Autonomy Roadmap.....	32
Figure 8. ALFUS Contextual Scale.....	38
Figure 9. 2012 DSB Framework for the Design and Evaluation of Autonomous Systems.....	40
Figure 10. Autonomous System Reference Framework (ASRF).....	41
Figure 11. Generalizing UAS as a Complex Adaptive System of Systems	42
Figure 12. Overview of the Pillars of the NDS	49
Figure 13. China versus US AI Development.....	59
Figure 14. Overview of Investment in Chinese AI Technology.....	60
Figure 15. Human versus Machine Optimization Areas	76
Figure 16. USAF Vision of Human-Machine Collaboration for UAS.....	78
Figure 17. Basic Overview of AI Functions within a System.....	80
Figure 18. How Artificial Intelligence Enables Autonomy.....	82
Figure 19. Human-in-the-Loop versus Human-on-the-Loop	84
Figure 20. Defense Outlays versus Gross Domestic Product FY 1940–FY 2023	91
Figure 21. Historical DoD Budget by Category.....	93

Figure 22. Recent and Projected RDT&E Funding as of PB 2017	94
Figure 23. Building Blocks of Future Capability	96
Figure 24. NITRD Budget Trends 2000-2018 by Agency	98
Figure 25. Standard V Development and Testing Model.....	103
Figure 26. The Four Types of Innovation	115
Figure 27. Comparing Breakthrough and Disruptive Innovations	116
Figure 28. Conceptual Framework and Taxonomy for Human Machine Collaboration.....	125
Figure 29. Conceptual Framework and Taxonomy for Human Machine Collaboration.....	126
Figure 30. Proposed Changes to the Standard V Model	134

TABLES

	Page
Table 1. Explanation of “Autonomous Functioning Within a System”	27
Table 2. Excerpt from Proud’s Levels of Autonomy	35
Table 3. Levels of Robotic Autonomy Taxonomy	36
Table 4. Hierarchy and Relationships between Guidance	45
Table 5. DoD Issuances that Provide Policy and Standards for Autonomy	51
Table 6. DoDD 3000.09 Overview	70
Table 7. Comparing Terminology	85
Table 8. DoD S&T Budget including Base and OCO	97

CHAPTER 1

INTRODUCTION

The military is on the cusp of a major technological revolution as it enters the *Robotic Age*, in which warfare is conducted by unmanned and increasingly autonomous weapon systems, operating across all domains (air, sea, undersea, land, space, and cyber), and across the full spectrum of military operations. The question is not *whether* the future of warfare will be filled with autonomous, AI-driven robots, but *when* and in what *form*.

— Andrew Ilachinski, *AI, Robots, and Swarms*

In the article “Thinking about revolutions in warfare,” a military revolution is defined as something that “fundamentally changes the framework of war . . . Military revolutions recast society and the state as well as military organizations. They alter the capacity of states to create and project military power.”¹ The Robotic Age described above by Dr. Andrew Ilachinski is a military revolution that will change the very character of warfare. This is because the “technological advances in artificial intelligence (AI), automation, and machine learning, combined with the growing availability of big data, have set the stage for a new era of sophisticated, inexpensive, and highly impactful political warfare.”² The 2018 National Defense Strategy (NDS) recognizes and addresses this fundamental change along with the forthcoming challenges it presents to maintaining conventional overmatch:

New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the

¹ Macgregor Knox and Williamson Muarry, ed., *The Dynamics of Military Revolution 1300-2050* (Cambridge: Cambridge University Press, 2001).

² Alina Polyakova and Spencer P. Boyer, “The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition” (Paper, Brookings-Robert Bosch Foundation Transatlantic Initiative, March 2018), 2.

commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base.³

To achieve the defense objective of sustaining Joint Force military advantages, the Department of Defense (DoD) is pursuing the Third Offset Strategy (3OS) which seeks to collaborate with the National Security Innovation Base (NSIB) to develop asymmetric technology advantages like robotics, autonomy, and artificial intelligence (AI).⁴ While global society is focused on the ethical debate of developing "Killer Robots,"⁵ the DoD is heavily investing in AI to enable increasingly autonomous systems. Despite the \$18 billion FY 17 budget for the 3OS (of which \$3 billion alone was dedicated to autonomy)⁶ the DoD is rapidly losing its asymmetric robotics and autonomous systems (RAS) advantage as compared to the peer competitors defined in the National Defense Strategy (NDS). In terms of funding innovation, developing policy

³ Department of Defense, "Remarks by Secretary Mattis on the National Defense Strategy," News Transcript, 19 January 2018, 3, accessed 22 January 2018, <https://www.defense.gov/News/Transcripts/Transcript-View/Article/1420042/remarks-by-secretary-mattis-on-the-national-defense-strategy/>.

⁴ Cheryl Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence," DOD News, Defense Media Activity, 31 October 2016, 4, accessed 27 November 2017, <https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/>.

⁵ Colin Roberts, "Killer Robots: Moral Concerns vs Military Advantages," *The National Interest*, 3 November 2016, accessed 20 December 2017, <http://nationalinterest.org/blog/the-buzz/killer-robots-moral-concerns-vs-military-advantages-18277>.

⁶ Joshua Pavluk and August Cole, "From Strategy to Execution: Accelerating the Third Offset," *War on the Rocks*, 9 June 2016, accessed 20 September 2017, <https://warontherocks.com/2016/06/from-strategy-to-execution-accelerating-the-third-offset/>.

supportive to RAS integration, and modernization of legacy equipment, the DoD is being outpaced by Russia and China's strategic plans and ability to develop breakthrough technology while modernizing current equipment at scale.

The DoD is also struggling with how to rapidly capitalize on the science and technology (S&T), research and development (R&D), and testing and evaluation (T&E) done by the US commercial sector. This is complicated because the DoD is constrained from efficient collaboration with industry by bureaucratic layers of regulation and oversight within the acquisition process.⁷ The current structure of the Defense Acquisition System (DAS) does not support the rapid and cost effective development and acquisition of weapons systems specifically those that are intricately melded with IT.⁸ In contrast, Russia and China have established whole of government approaches to the development of RAS with each country planning to become a leading world power in AI by 2050. Their forecast spending for R&D and stated modernizations plans to achieve AI supremacy puts both countries on a timeline to generally outpace US capability beginning as soon as 2020.⁹

⁷ Larry Lewis, *Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations* (Arlington, VA: Center for Naval Analyses, September 2017), 56.

⁸ Andrew P. Williams and Paul Scharre eds., *Autonomous Systems: Issues for Defence Policymakers* (NATO Communications and Information Agency), 6, accessed 20 September 2017, <http://www.act.nato.int/>. "Military bureaucracies that build complex, intricate weapons systems on 20- or 30- year timelines . . . are at an inherent disadvantage in keeping pace with rapidly advancing information technology."

⁹ China is particularly poised to gain an advantage relative to the US in the realm of AI development. "R&D corporations based in Japan, Korea, Chinese Taipei, and China account for about 70% of all AI related inventions belonging to the world's 2000 top corporate R&D investors and their affiliates, and US based companies for 18%." See <https://read.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and->

Recognizing the increasing threat of peer competitors,¹⁰ the National Security Strategy (NSS) contains strategic guidance “to maintain our competitive advantage, the United States will prioritize emerging technologies critical to economic growth and security, such as . . . autonomous technologies . . . and artificial intelligence.”¹¹ Tying the development of autonomy and AI to economic growth and security is also echoed in Chinese and Russian AI strategies so it seems clear that competition will arise as each country races to develop breakthrough technology and modernize legacy equipment.

Peer countries are not the only competitors in the AI arms race. The US private sector is outspending and outpacing the DoD on research and development (R&D) funding for IT at a 5 to 1 ratio.¹² Disruptive innovations like smart phones, big data, and cloud computing are improved on ever more rapid cycles with new models coming out with increasing regularity. The speed of commercial IT development proceeds based on

industry-scoreboard-2017_9789264268821-en#page35, page 33 for further information and statistics.

¹⁰ For the purpose of this research peer competitors are defined as Russia and China as identified in the NDS. “The evolution of technology—and Russia’s and China’s stated desire to lead on artificial intelligence (AI) research—signals that Western democracies will face increasing threats in the cyber and information domain.” Polyakova and Boyer, “The Future of Political Warfare,” 3.

¹¹ Office of the President of the United States, *The National Security Strategy of the United States of America* (Washington, DC: The White House, December 2017), 20.

¹² MGI estimates that in 2016 US companies invested \$39 billion on AI related technology. In contrast, in FY 2017 the DoD invested only \$7.4 billion on AI technology (\$13.2 billion on overall S&T) which is an increase of 32.4 percent from the \$5.6 billion invested in FY 2012. The President’s 2018 budget request for the entire NITRD program is \$4.46 billion. The DoD’s entire 2017 budget was only \$606 billion; IT funding within the commercial sector is comparable to the entire 2018 budget for aircraft and shipbuilding. Jacques Bughin et al., “Artificial Intelligence the Next Digital Frontier?” (Discussion Paper, McKinsey Global Institute, June 2017).

user demand while the average DoD IT program acquisition remains stagnant at around 81 months.¹³

Unlike the private sector, the DoD is hampered by a general policy of “require then acquire”. Based on the constraint of free and open competition, capability developers and acquisition professionals cannot easily conduct early and frequent communication of requirements to the commercial sector before an official request for proposal is issued. Outside of research laboratories, academic conferences, and home on home events or organization like the Defense Innovation Unit Experimental (DIUx) and the Strategic Capabilities Office (SCO), there are limited venues through which the DoD can currently communicate emerging requirements unless technology already exists at a sufficient system maturity to conduct testing. This overarching result is increasing use of the Rapid Acquisition Process (RAP) to acquire a commercial solution at the warfighter’s request. The reality of the RAP is that available commercial technology increasingly determines acquisition timelines and programmatic costs based on the urgency of the operational needs. Existing commercial technology is generally adequate to meet RAP guidelines for acquisition and fielding however it comes with sunk costs especially in the fields of maintenance and upgrades as it is generally proprietary equipment.

This is not the first instance in which the private sector has driven military acquisition by developing commercial technology at a faster and cheaper pace than the DoD can develop the requirements for them via JCIDS.¹⁴ After WWII, the DoD’s

¹³ Lewis, *Insights for the Third Offset*, 10.

¹⁴ *Ibid.*, 20.

purchase and development capacity was surpassed by that of the commercial aerospace sector due to the performance of aviation during the war. Despite this, the DoD was able to retain air supremacy in almost all operational theaters since WWII through successful collaboration with the NSIB. Today, the DoD remains primarily responsible for the for the development of breakthrough aerospace technology like fighter aircraft but capitalizes on R&D from the commercial sector for air mobility to the point that many aviation lift and reconnaissance platforms are now based on commercial off the shelf systems (COTS).

Like the aerospace industry after WWII, the commercial RAS industry is expanding at a rate that exceeds the DoD's ability to acquire and field materiel without significant changes to the DAS.¹⁵ Increasingly complex IT centric materiel becomes obsolete almost upon fielding to units who are in turn courted by industry to purchase newer models at increasing costs to keep pace with what is commercially available.¹⁶ "Experts estimate that by 2018 global spending on military robotics will reach \$7.5 billion a year" as contrasted with an estimated \$43 billion on robotics in the commercial and industrial sector and an estimated \$3.8 trillion on the global information technology industry which enables the technology behind autonomy.¹⁷ While the DoD is a small

¹⁵ Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems (JCRAS)* (Washington, DC: Joint Chiefs of Staff, October 2016), 16.

¹⁶ "It's to the point that the world's greatest land force moves so slowly in fielding new capabilities that some things—especially when it comes to advanced technology and computer systems—are almost obsolete by the time they end up in the hands of soldiers." Rick Maze and Gina Cavallaro, "Battling Bureaucracy: The Way Forward Requires Modernizing the Modernization Process," *Army Magazine* (AUSA), 22 February 2018.

¹⁷ Williams and Scharre, *Autonomous Systems*, 5.

portion of the global robotics sector, tremendous potential exists for collaboration with the commercial sector to jointly fund and develop RAS in ways that modernize the current fleet of legacy equipment with existing technology while focusing on the development of breakthrough technology for future critical defense needs.

While funding does not always equate to capability, IT is ultimately developed based on funding for S&T and R&D. Because the US government stance is that “the private sector will be the main engine of progress on IT,”¹⁸ the DoD is in turn relegated to becoming a “fast follower” the private sector’s development of IT. “Unlike past offset strategies, this approach must reflect the new reality . . . [that] commercial R&D efforts are going to be much greater than that of DOD. Thus the Third Offset must rely on developments in the commercial sector as well as DOD R&D.”¹⁹

To balance the simultaneous needs for innovation, modernization, and growing the force, the DoD should consider changing its culture to become a “fast follower” of IT by aligning Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, Policy (DOTMLPF-P) in anticipation of the adoption of new technology. Similar to how the Germans developed doctrine, changed organizations, and even conducted training centered around mechanization during the interwar period before they actually acquired tanks, the DoD must structure DOTMLPF-P to adopt RAS while the technology is being developed and tested within the private sector. The DoD must

¹⁸ Jason Furman, “Is This Time Different? The Opportunities and Challenges of Artificial Intelligence” (Remarks, AI Now: The Social and Economic Implications of Artificial Intelligence Technologies in the Near Term, New York University, New York, 7 July 2016), 10.

¹⁹ Lewis, *Insights for the Third Offset*, 6.

learn lessons from the private sector and improve collaboration with industry and academia throughout the capability development process in order to shorten acquisition and fielding timelines or it will fall behind increasingly capable unconstrained peer competitors.²⁰

Assessment of Capabilities, Gaps, and Mitigations

Based on the NSS guidance and the current state of global competition, the DoD must make changes to policy, acquisition, and doctrine if it is to regain its asymmetric robotics advantage over peer adversaries. To address this point, the author assesses the forecast capabilities, current gaps and proposed mitigations as follows.

1. Policy.

- a. Capability: The DoD requires policy supportive of developing, modernizing, and utilizing RAS as outlined in doctrine, the Joint Operating Concept (JOC), and the Joint Concept of Robotics and Autonomous Systems (JCRAS).
- b. Gap: Current policy does not support the rapid development of autonomous systems or integration of AI into legacy systems because it is ambiguous and does not establish sufficient standards for capability development.
- c. Mitigation: The concept of autonomous functioning within a system should be the foundation for framing DoD policy. Policy should define roles to be retained by humans and cognitive, physical, and operational tasks that can be allocated to machines within human-machine systems.

²⁰ Lewis, *Insights for the Third Offset*, 19.

2. Doctrine

- a. Capability: The DoD currently employs automated systems that have a high degree of operational autonomy and seeks to develop flexible autonomous systems in accordance with the JOC and JCRAS that adapt to changing environments as part of human-machine teams.
- b. Gap: The majority of DoD literature on AI and autonomy resides in concepts or within the S&T and R&D communities resulting in a misunderstanding of how AI enables autonomy and autonomous system capabilities. The DoD lacks a conceptual framework, taxonomy, and lexicon for describing autonomy beyond the term “flexible autonomy”.
- c. Mitigation: The DoD should develop a framework for understanding and describing AI and autonomy and publish a standardized taxonomy that describes human-machine collaboration in terms of required capabilities. The concept of autonomous functioning within a system should be the foundation for the framework and taxonomy.

3. Leadership

- a. Capability: Implementation of the DoD’s operating concepts requires humans and machines to work together to achieve goals. Machines augment, enable, and team with humans to accomplish cognitive and physical work. Humans are ultimately responsible for mission accomplishment as well as ethical and moral decisions specifically regarding the application of lethal force.

b. Gap: There is limited trust within the DoD between humans and machines specifically those viewed as having some level of cognitive intelligence.

While operators of machines tend to have confidence in machine ability to perform to standard, DoD leadership has primarily focused on limiting machine capabilities based on a perception of failure and mistrust. DoD leadership is generally under-educated or mis-informed on AI and autonomy due to the lack of a conceptual framework, taxonomy, and terminology that accurately describes these terms in relation to DoD required capabilities.

c. Mitigation: DoD leadership must provide clear intent on the roles that humans will retain and tasks that machines can do within the cognitive, physical, and operational domains. They must develop a culture that builds trust in human-machine teams and focuses on developing technology that augments and enables humans. A holistic study of the performance of DoD RAS should be conducted to confirm the assumptions of increasing reliability, predictability, flexibility, and robustness of human-machine collaboration. The DoD should also develop metrics to measure the performance of RAS beyond simply tracking the failure rate of systems and components.

4. Materiel

a. Capability: The DoD must agilely acquire and field technology “at the speed of relevance”. The DoD must simultaneously fund innovation,

modernization, and force growth as prioritized by the Services within a limited budget.

- b. Gap: The DAS does not generally support the rapid acquisition and upgrading of IT unless it is acquired as commercial technology through the RAP. This results in the commercial sector increasingly driving DoD requirements because commercial technology is often proprietary and comes with sunk costs. The DoD cannot fund the development of or acquire IT in parity with the US commercial sector resulting in a technology gap that further increases the DoD's dependence on acquiring COTS through the RAP.
- c. Mitigation: The DoD should prioritize the funding of breakthrough technology that is critical to its core competencies especially in areas where insufficient private sector investment exists. The DoD should assume a "fast follower" strategy for RAS (specifically IT) in areas where there is significant overlap with the private sector that would support cost savings and increase force generation. Fast Followership must be applied across the entire DOTMLPF-P spectrum. The DoD should consider an "acquire then require" strategy for disruptive innovations that lend themselves to rapid acquisition and improvements through iterative prototyping.

Research Questions

The primary question that this research seeks to answer is what capability gaps exist pertaining to autonomous capability development within the DoD. Subordinate questions that will also be answered include:

1. How should the DoD frame the spectrum of autonomy to describe the cognitive and physical capabilities of humans and machines to support the development of autonomy?
2. In what ways could a conceptual framework and taxonomy for autonomous capabilities shared between the DoD and the private sector enhance the DoD's ability to rapidly develop, acquire, and integrate scalable autonomous capabilities into weapons systems?
3. How can humans and machines work together to achieve goals resulting in enhanced perception, cognition, and action to achieve overmatch?

Assumptions

The following assumptions were made during the course of the research:

1. The DAS, JCIDS, and Planning, Programming, Budgeting, and Execution systems discussed within the research are based on current published models and unless specifically stated do not include any of the revisions ongoing in defense acquisition reform.
2. Artificial General Intelligence is still years away from development and is not required for systems to operate autonomously.
3. The DoD is losing its asymmetric RAS advantage as compared to Russia and China as defined by the metrics of funding innovation, developing supportive policy, modernizing and integrating equipment to include AI.
4. The private sector will continue to invest more money than the DoD in IT S&T and R&D due to user demand.
5. The DoD is legally capable of adopting fast follower techniques.

6. The DoD budget will remain generally as published for FY 2019.
7. Narrow AI currently enables autonomy. Automated machines are not inherently autonomous although they can conduct physical and cognitive work largely independent of human control. The structure of cognitive architectures to support goal based as opposed to rule based reasoning is what determines machine automation versus machine autonomy.
8. Russia and China are the only peer competitors of significance for AI and autonomy as identified in the NDS.

Limitations

All information on acquisition reform is limited to published system structures and does not include ongoing acquisition reform due to limited access to information. The most current funding data is always utilized when documentation is published to support tracking current trends in funding even if funding is forecast rather than allocated. Research data, analysis, and recommendations are all Unclassified, no FOUO or classified information was considered in the research or writing of this document.

Scope and Delimitations

This research does not seek to examine any aspects of RAS other than the development, acquisition, and integration of those capabilities. AI itself is not the focus of this research and is only discussed in the capacity of how it enables autonomy. The scope of this research is limited specifically to research and recommendations for policy, doctrine, and acquisition at the DoD level. This research will only propose a taxonomy and basic terminology, the development of an ontology linking the axes within the

spectrum of autonomy is recommended for further research. Due to the large amount of material on this topic available in the private sector, only scholarly publications pertinent to recommendations for terminology, taxonomy, and conceptual framework are included. Ethical concerns regarding autonomous capability development are not included in this paper and are instead recommended as a topic for further study due to the depth and breadth of information on this topic.

The research is limited to identification and recommendations to fill broad capability gaps regarding policy, doctrine, leadership, and acquisition. It does not seek to provide specific recommendations to reform the DAS but does offer general broad base recommendations for changes to the JCIDS process.

Aim and Relevance of Research

This research seeks to identify the major capability gaps within the DoD related to the development and integration of AI and autonomy. The DoD risks losing its asymmetric RAS advantage if it cannot develop, acquire, and field RAS at a speed to either deter or counter peer competitors. The DoD must unify its efforts into a whole of agency approach to developing AI to enable autonomy if it is to retain a competitive RAS advantage over peer adversaries.

The aim of this research is to recommend how the DoD could re-frame the way it thinks about autonomy and AI using the concept of autonomous functioning within a system. Information from DoD studies, academic articles, and published think tank papers related to autonomy and AI provide the foundational research supporting the author's attempt to define and recommend key terminology within a proposed conceptual framework for autonomy that spans the cognitive, physical, and operational

domains of human-machine interaction. These recommendations are specifically geared toward capability developers, acquisition professionals, policy makers, and doctrine writers.

Summary and Conclusion

“Western societies must harness their current—though fleeting—competitive advantage in technology to prepare for the next great leap forward in political warfare, especially AI.”²¹ In the context of this point, the DoD must develop a strategy to maintain a competitive RAS advantage while balancing the need to innovate, modernize, and grow the force. DoD leadership must establish clear guidance that resonates in policy, concepts, and doctrine concerning the development and employment of RAS. They must create a culture of trust in human-machine collaboration consistent with strategic guidance and policy. The DoD must also find creative ways to rapidly acquire materiel that is both relevant and easy to upgrade as technology changes. The DoD must increase collaboration with the private sector and take advantage of work done by the NSIB in order to maintain a qualitative and quantitative edge RAS over peer competitors. To achieve the asymmetric advantage goals outlined in the NDS and 3OS, the DoD must make changes regarding policy, doctrine, acquisition, and DoD leadership must understand and embrace the capabilities of emerging RAS technology.

²¹ Polyakova and Boyer, “The Future of Political Warfare,” 3.

CHAPTER 2

LITERATURE REVIEW

While the nature of warfare will remain intrinsically human as long as its aim is the imposition of will over an adversary, the character of warfare will change as the tools used to execute warfare become increasingly less human. Is the Soldier of the future a hyper-enhanced fighter with abilities beyond innate human capabilities, a force manager of unmanned and autonomous/semi-autonomous systems, or an amalgamation of the two?

— Ian Sullivan, Matthew Santaspirt, and Luke Shabro,
“Visualizing Multi-Domain Battle 2030-2050”

Introduction

The purpose of this research is to identify capability gaps with the way that the DoD develops, acquires, and fields autonomous capabilities and to recommend a way for the DoD to re-frame the way they look at autonomy from a complex adaptive systems approach. This chapter consolidates literature pertinent to answering the research questions and provides a background outlining the assessed capabilities and gaps. It also establishes the foundational knowledge required to support the author’s assumptions and recommendations for proposed mitigations.

Background: Framing the Spectrum of Autonomy

The amount of research devoted to human-machine collaboration is vast and can be summarized as conflictual at best. The RAS field contains a multitude of competing theories, terms, and concepts describing the interactions between man and machine. For the purpose of this research, the author proposes that the “spectrum of autonomy” refers to the degree to which humans are enabled by machines through autonomous functioning in a system.

The spectrum of autonomy is bounded on one side by human optimized cognitive and physical functions (expertise, morality, decision making) and other side by machine optimized cognitive and physical functions (skills, operation, tasks). Autonomy is viewed as multidimensional spectrum with axes that allow commanders, operators, and capability developers to select how much self-direction machines can have within each axis. The amount of self-direction is based on risk acceptance and machine cognitive and physical capability as defined by policy considerations, legal considerations, the complexity of the mission and environment, and functional trade space. The axes should be considered as follows:

1. Cognitive axis: How much self-direction should humans authorize for systems to conduct conscious intellectual activity such as decision making, reasoning, problem solving, and learning?
2. Physical axis: How much self-direction should humans authorize for systems to conduct tasks or physical work?
3. Operational axis: How much self-direction should humans authorize for systems to accomplish missions and goals? What type of controls must be developed to retain human responsibility and accountability for mission accomplishment?

Since the DoD does not have a standardized conceptual framework or taxonomy that describes the spectrum of autonomy, the graphics contained in figures 1 and 2 developed by the author are provided as the foundational framework to understand autonomy.

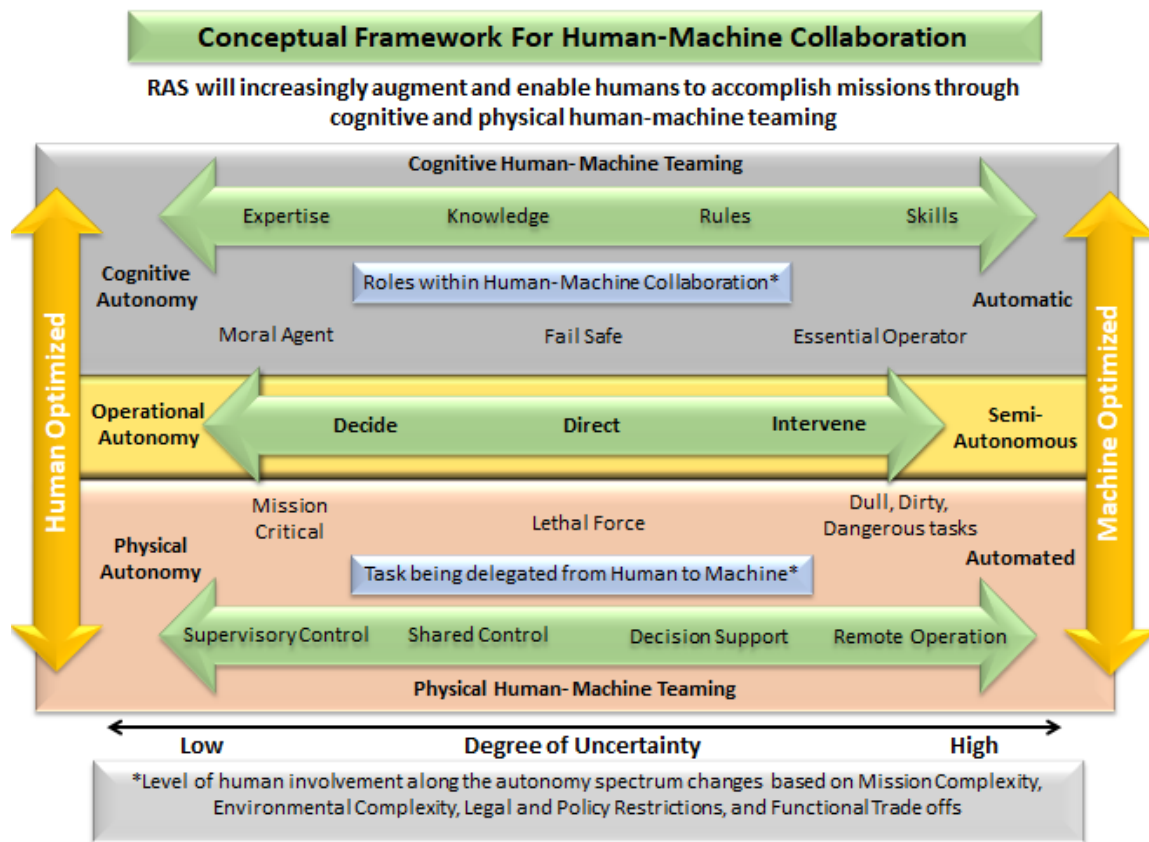


Figure 1. The Spectrum of Autonomy

Source: Concept developed by the author based on research and concepts developed by Mary (Missy) Cummings, “Artificial Intelligence and the Future of Warfare” (Research Paper, Chatham House, The Royal Institute of International Affairs, January 2017); Mary (Missy) Cummings, “Man vs. Machine or Man + Machine,” *IEEE Intelligent Systems* 29, no. 5 (September/October 2014): 62-69, accessed 26 February 2018, www.computer.org/intelligent; Jenay M. Beer, Arthur D. Fisk, and Wendy A. Rogers, “Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction,” *Journal of Human-Robot Interaction* 3, no. 2 (2014); and Paul Scharre, “Autonomous Weapons and Operational Risk” (Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016).

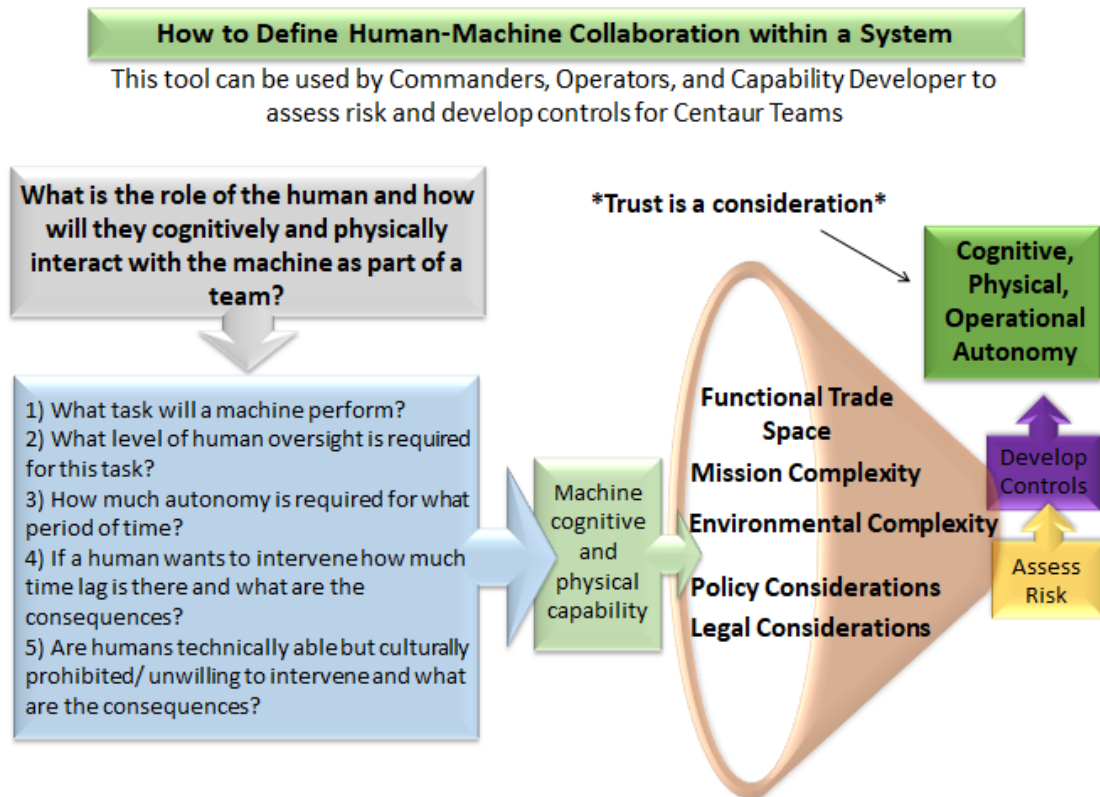


Figure 2. How to Determine Autonomous Functioning within a System

Source: Concept developed by the author based on research and concepts developed by Mary (Missy) Cummings, “Artificial Intelligence and the Future of Warfare” (Research Paper, Chatham House, The Royal Institute of International Affairs, January 2017); Mary (Missy) Cummings, “Man vs. Machine or Man + Machine,” *IEEE Intelligent Systems* 29, no. 5 (September/October 2014): 62-69, accessed 26 February 2018, www.computer.org/intelligent; Jenay M. Beer, Arthur D. Fisk, and Wendy A. Rogers, “Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction,” *Journal of Human-Robot Interaction* 3, no. 2 (2014); and Paul Scharre, “Autonomous Weapons and Operational Risk” (Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016).

While there is no singular taxonomy describing the spectrum of autonomy there are certain points that have become synonymous with common terms. As shown in figure 3 “Defining Autonomy” there are increasing levels of system capability that build up to autonomous cognition and action. Automated systems are fully capable from a

command and control perspective of conducting “autonomous operations” without AI; however, risk for these type of operations is greatly increased due to their inability to use cognition, knowledge, and experience to adapt to changing situations. Because of this, the DoD has chosen to automate specific functions within systems thereby generally pursuing the development of semi-autonomous systems. Weapons, specifically munitions, tend to be automated and many skill based tasks that humans formerly performed have become automatic supporting overall system functions.²² Figure 3 provides a graphic overview that explains the difference between these terms through a basic taxonomy that describes the levels between automatic and autonomous. The DoD has not yet developed a fully autonomous weapons system but they currently employ automatic and automated systems that are authorized high degrees of operational autonomy.

²² “The United States has incorporated autonomy into certain weapon systems for decades.⁷⁸ These technological improvements may allow for greater precision in the use of these weapon systems and safer, more humane military operations. Precision-guided munitions allow an operation to be completed with fewer weapons expended and with less collateral damage, and remotely-piloted vehicles can lessen the risk to military personnel by placing greater distance between them and danger.” Executive Office of the President, *Preparing for the Future of Artificial Intelligence* (Washington, DC: The White House, October 2016).

Defining Autonomy

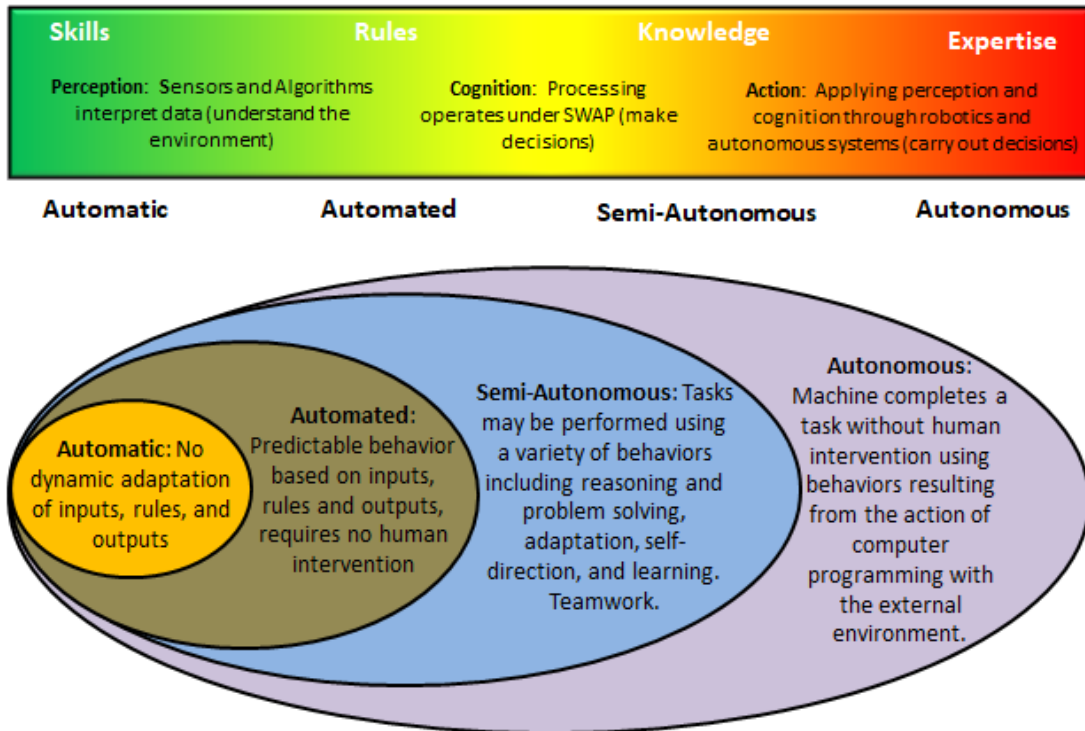


Figure 3. Defining Autonomy

Source: Figure developed using SRKE framework from Mary (Missy) Cummings, “Informing Autonomous System Design Through the Lens of Skill-, Rule-, and Knowledge-Based Behaviors,” *Journal of Cognitive Engineering and Decision Making* (October 2017): 58-61, and definition of autonomous functioning within a system from Andrew P. Williams, and Paul Scharre, eds., *Autonomous Systems: Issues for Defence Policymakers* (NATO Communications and Information Agency), accessed 20 September 2017, <http://www.act.nato.int/>.

Background: Defining Autonomy

As defined by autonomy expert Paul Scharre in his white paper, “Autonomous Weapons and Operational Risk,” “the essence of autonomy is delegating a task

previously done by a person to a machine.”²³ Attempts to define autonomy and categorize it into hierarchical levels have been called “a waste of both time and money spent debating and reconciling different terms (that) may be contributing to fears of unbounded autonomy.”²⁴ Because of this, terms like “intelligent,” “automated,” “automatic,” and “unmanned” tend to be used interchangeably. They also tend to be misused or grouped into categories that are misnomers for actual capability. An example of this is the use of the term “unmanned” to generally describe technology that is remotely operated or automatic.²⁵ Misuse of this term has created a belief that these systems operate with high degrees of autonomy and require less personnel than manned systems.²⁶ In fact, “increasing the autonomy of autonomous systems requires different kinds of human expertise and not always fewer humans.”²⁷

To understand the fundamental difference between automation and autonomy, consider figure 4 which shows how cognitive autonomy is enabled through neural networks (NN) and machine learning (ML) while physical autonomy is enabled through

²³ Paul Scharre, “Autonomous Weapons and Operational Risk” (Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016), 1.

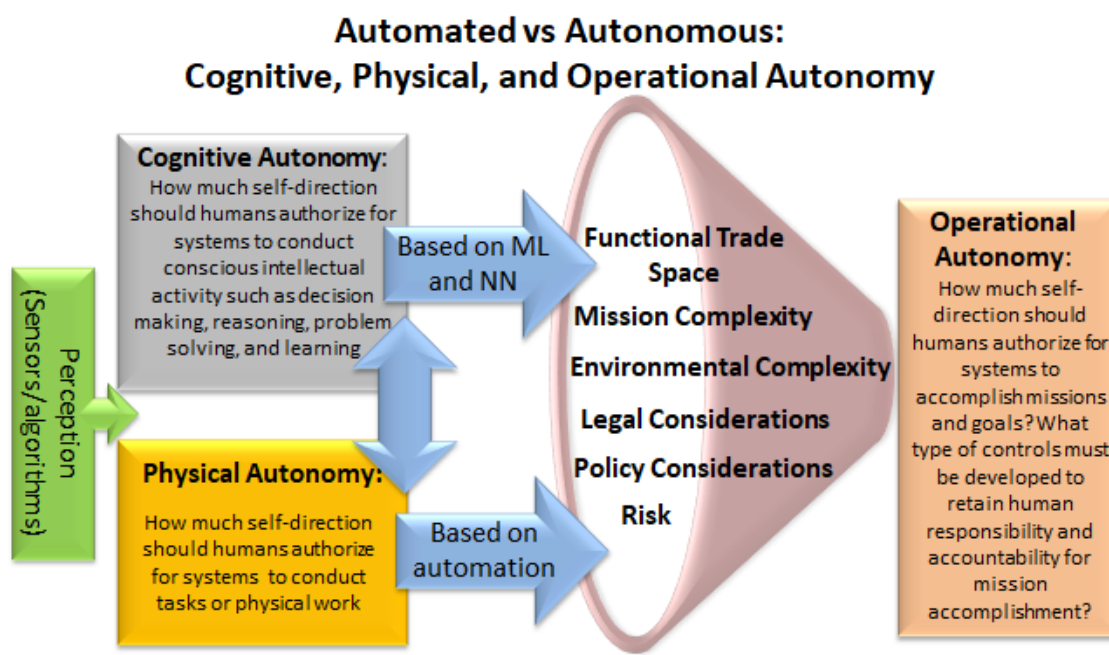
²⁴ Department of Defense, *Task Force Report: The Role of Autonomy in DoD Systems*, 23.

²⁵ Williams and Scharre, *Autonomous Systems*, 37.

²⁶ “The Air Force has declared that its most critical staffing problem is *manning its unmanned platforms*.” Defense Science Board, *Task Force Report: The Role of Autonomy in DoD Systems*, 57.

²⁷ Jeffrey M. Bradshaw et al., “The Seven Deadly Myths of Autonomous Systems,” *Human Centered Computing* (May-June 2013): 6.

automation. The difference between automation and autonomy lies in a system's ability to conduct goal based reasoning.



Automated machines with limited or no cognitive autonomy can execute missions with a high degree of operational autonomy but cognitive or physically autonomous systems may be limited in execution due to concerns with system trust. The difference between “automation” and “autonomy” is the ability of a system to execute goal based reasoning resulting from the action of computer programming with the external environment.

Figure 4. Automation versus Autonomy

Source: Developed by author.

Based on this understanding of autonomy, the author proposes the following definitions and concept which were not found within literature during the scope of the research.

Cognitive Autonomy: The degree of self-direction with which systems are authorized to conduct conscious intellectual activity such as decision making, reasoning, problem solving, and learning with limited or no human oversight during mission performance. This ability is largely based on the presence of artificial intelligence.

Physical Autonomy. The degree of self-direction with which systems are authorized to conduct tasks or physical work with limited or no human oversight during mission performance. This ability is largely based on automation resulting in rule based behavior. Artificial intelligence can be integrated into systems to achieve goal based behavior.

Operational Autonomy. The degree of self-direction with which systems are authorized to accomplish missions and goals with limited or no human oversight during mission performance. Self-direction is based on the cognitive and physical capabilities of the machine as factored against mission complexity, environmental complexity, legal considerations, policy considerations, functional trade space, and risk. Authorization of self-direction is contingent on human trust in machine ability.

Because automation and autonomy are generally used interchangeably or “binned” together, there is limited literature within the DoD that separates these terms based on either physical or cognitive capabilities of systems. The author has found no research that discusses operational autonomy in terms of command and control of machines based on their physical and cognitive capabilities.²⁸ DoD policy in DoDD 3000.09 limits the cognitive and physical autonomy of machines to allow humans to execute appropriate levels of judgement for lethal engagements in accordance with international humanitarian law. This differs from the definition of “meaningful human control” as described by the Non-Governmental Organization (NGO) “Article 36” which has become the international term of debate.²⁹

²⁸ The DoD Dictionary lists an entry for “autonomous operation: In air defense, the mode of operation assumed by a unit after it has lost all communications with higher echelons forcing the unit commander to assume full responsibility for control of weapons and engagement of hostile targets.” Department of Defense, *Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, February 2018), 24.

²⁹ For further analysis of the now ubiquitous term “meaningful human control” see the article Article 36.org, “Key Elements of Meaningful Human Control,” accessed 2 April 2018, <http://www.article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf>.

Conceptually binning terminology to collectively describe dissimilar physical and cognitive capabilities compounds understanding autonomy. For example, through creating the label “Robotic and Autonomous Systems” the DoD has effectively binned dissimilar automated and autonomous technology together. Categorizing all robotics as “autonomous systems” creates confusion as various components of robotics are automatic, automated, semi-autonomous and to some degree cognitively autonomous although as previously discussed automated systems can be “operationally autonomous” without integrating AI. Figure 5 is a useful way to understand RAS labelling as applied to unmanned systems.

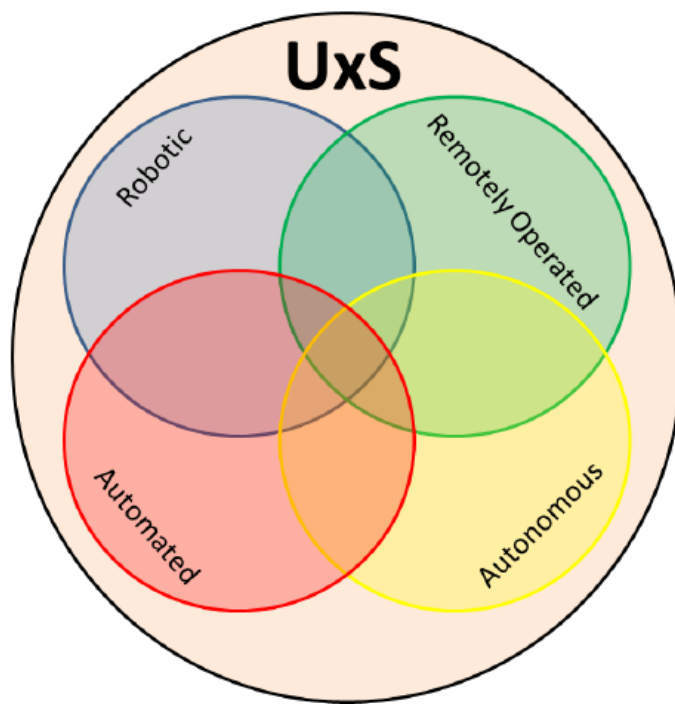


Figure 5. Department of the Navy Taxonomy of UxS

Source: Department of the Navy, *Strategic Roadmap for Unmanned Systems* (Washington, DC: Department of the Navy, 7 March 2018), 9. Note: An example of how the US Navy conceptually bins their unmanned systems.

A more holistic way to conceptualize autonomy is to think of it as enabling the functions within a system, or “autonomous functioning in a system” as defined in the following paragraphs.³⁰

In the Headquarters Supreme Allied Commander: Transformation publication “Autonomous Systems: Issues for Defence Policymakers” Williams and Scharre propose that a definition for autonomy should be based on its dimensions rather than the current context of control relationships and machine complexity. They propose that the most appropriate conceptual framework would include the dimensions of autonomy resident within a system. Thus, their definition for “autonomous functioning in a system” proposes a holistic solution for a complex concept:

Autonomous functioning in a system refers to the ability of a system, platform, or software to complete a task without human intervention, using behaviors resulting from the action of computer programming with the external environment. Tasks or functions executed by a platform, or distributed between a platform and other parts of a system, may be performed using a variety of behaviors which may include reasoning and problem solving, adaptation to unexpected situations, self-direction, and learning. Which functions are autonomous—and the extent to which human operators can direct, control or cancel functions—is determined by system design function trade-offs, mission complexity, external operating environment conditions, and legal or policy constraints. This can be contrasted with automated functions, which (although they require no human intervention) operate using a fixed set of inputs, rules, and outputs, the behavior of which is determined and largely predictable. Automatic functions do not permit the dynamic adaptation of inputs, rules, or outputs.³¹

The breakdown for the wording of this definition is shown in table 1. It is primarily based on the contextual scale developed by a group the National Institute of Standards and Technology established to address autonomy issues and recommendations

³⁰ Williams and Scharre, *Autonomous Systems*, 56.

³¹ Ibid., 56-57.

from the 2012 DSB study on autonomy. While this definition is lengthy, it is useful from a capability development perspective because it lays the groundwork for a taxonomy that defines autonomous characteristics by function.

Table 1. Explanation of “Autonomous Functioning Within a System”

Component of Definition	Derivation/Understanding
Autonomous Functioning in a System	Conveys the understanding that technology is very far from producing autonomy to the same extent as a sentient animal (i.e., human). It is more realistic to presume that any given defence system will perform a variety of functions, not all of which are autonomous.
...the ability of a system, platform, or software, to complete a task...	Ensures that the difference between system and platform is recognised. Furthermore, in many cases the computer software is the root of an autonomous function, thus this should be recognised in the definition.
...without human intervention...	A key criterion of autonomy.
... using behaviours resulting from the interaction of computer programming with the external environment.	Many definitions of autonomy or autonomous system, including the three listed in the first section of this chapter, could refer to an animal. Thus the definition should differentiate between machines and animals; the key difference is that regardless of how autonomy is conceptualised, it eventually boils down to a computer program interacting in some way with the external environment.

Tasks or functions executed either by a platform or distributed between a platform and other parts of the system...	Recognises that autonomy may allow more efficient distribution of functions between various parts of the system.
...which may include...	A rigorous description of <i>behaviour</i> is a very complex task, which involves drawing on a variety of academic disciplines. This phrase was chosen to give flexibility and to convey that autonomous behaviour must include <i>at least one</i> item from the following list.
...reasoning and problem solving, adaptation to unexpected situations, self-direction, and learning	These are drawn from the definitional and dimensional analysis of autonomy. While earlier definitions required the total set of characteristics to be considered autonomous, discussion from workshops revealed that a more flexible definition was preferable. Caution must be used when considering learning. Learning-like behaviour may be observed in system, but this may not actually be learning in the same way that sentient creatures learn. Further work is required to rigorously specify the distinction and overlaps between adaptation and learning.
Which functions are autonomous, and the extent to which human operators can direct, control, or cancel functions, is determined by...	Again, this attributes autonomy to system functions. Makes clear that human operators are able to direct, control, or cancel system functions, depending on certain factors.
...system design trade-offs, mission complexity, external operating environment conditions, and legal or policy	Caveats the extent of human control and notes that it could vary quite considerably depending on factors <i>external</i> to the system.

Component of Definition	Derivation/Understanding
This can be contrasted against automated functions, which although they require no human intervention, operate using a fixed set of inputs, rules, and outputs, the behaviour of which is deterministic and largely predictable. Automatic functions do not permit dynamic adaptation of inputs, rules, or outputs.	This is an optional caveat to the definition, which contrasts autonomy with automatic. It suggests the key difference between automated and autonomous: while both occur without human intervention, automated functions are to a large extent 'fixed', while autonomous functions have some dynamic adaptability. This also suggests that the majority of defence systems that are currently labelled as autonomous would be better described as automatic.

Source: Andrew P. Williams and Paul Scharre eds., *Autonomous Systems: Issues for Defence Policymakers* (NATO Communications and Information Agency), 57-59, accessed 20 September 2017, <http://www.act.nato.int/>.

Additional literature that discusses conceptualizing and defining autonomy is analyzed in chapter 4. The following section discusses the way in which the DoD conceptualized and developed autonomy and contrasts that process with the private sector.

Background on the DoD's Approach to Framing and Developing Autonomy

The following section explains the evolutionary development of the DoD's approach to autonomy through the comparison of different frameworks for autonomy that the Services and the private sector have developed. There is no consensus within either the private sector or the DoD as to which type of framework is best but the

Institute of Electrical and Electronics Engineers (IEEE) has adopted a multi-dimensional scale as the basis for its standards.

Categorical and Linear Scales

The DoD originally envisioned autonomy as a linear scale of ordinal levels because it helped track whether programmatic goals had been met.³² Models developed by Sheridan, Clough, the NATO Industrial Advisory Group (NIAG), and the Services themselves all generally depict machines enabled by AI increasingly assuming tasks and roles formerly filled by humans up to a level that is capable of “fully autonomous” operations.

Categorical and linear scale models are popular with capability developers, acquisition personnel, and DoD leadership mainly because they are relatively simple to understand. The level based chart developed by the National Institute of Standards and Technology as part of their Autonomous Levels for Unmanned Systems Framework (ALFUS) is the most common example of this type of framework as shown in figure 6. The ALFUS shows a series of ordinal levels depicting human-robot interaction (HRI) which decreases as automation increases from remote control up to full autonomy. This framework laid the foundation for the DoD’s development of unmanned systems.

³² Williams and Scharre, *Autonomous Systems*, 40.

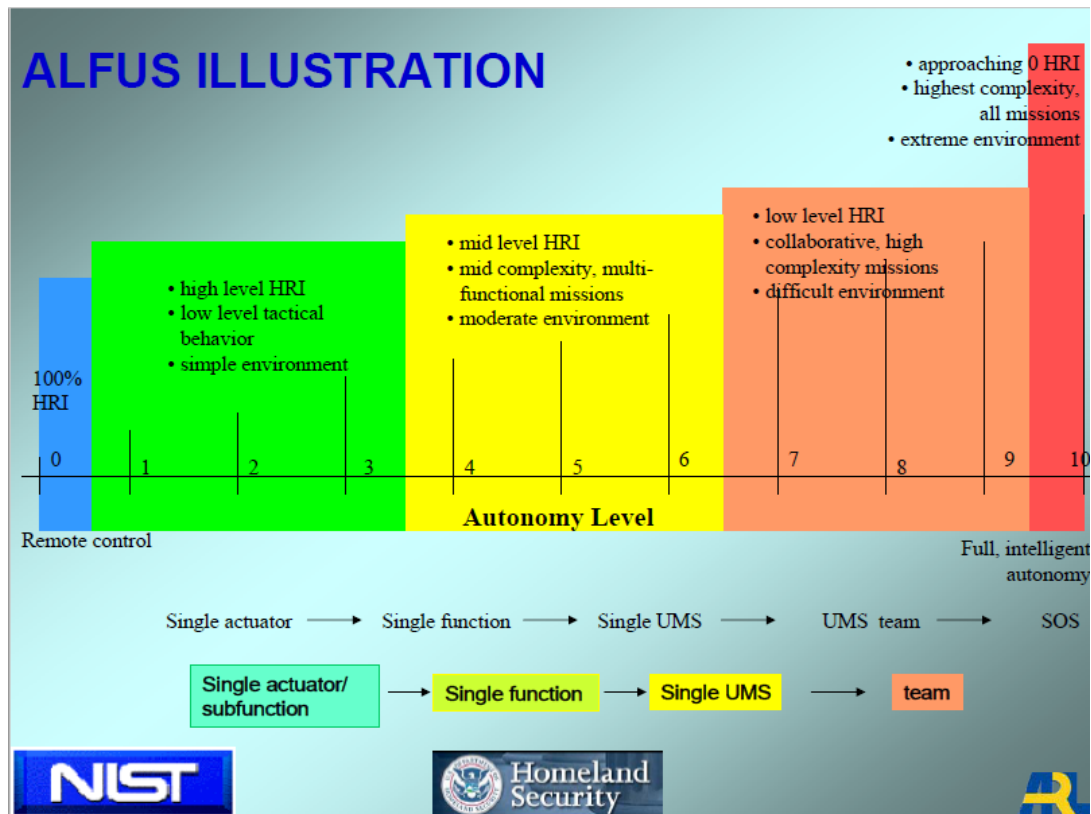


Figure 6. ALFUS Linear Scale Illustration

Source: Hui-Min Huang, “Autonomy Levels for Unmanned Systems (ALFUS), Slide 13, accessed 2 October 2017, <https://www.nist.gov/sites/default/files/documents/el/isd/ks/ALFUS-BG.pdf>.

In programmatic terms, each block in the ALFUS is essentially a stepping stone in capability development moving toward the end state goal of a fully autonomous system. The colored levels can basically be ascribed to US Army Training and Doctrine Command (TRADOC) G2’s proposed taxonomy for autonomous systems:

Non-Autonomous (Remote Control): “Human in the Loop”: machines guided via remote controls; no autonomy in system.

Semi-Autonomous: “Human in the Loop”: machines wait for human input before taking action.

Supervised Autonomous: “Human on the Loop”: humans can intervene in real time.

Fully Autonomous: “Human Out of the Loop”: no ability for human to intervene in real time.³³

Each Service has spent the last few years developing “levels of autonomy” scales similar to the ALFUS. The scale used by US Air Force (USAF) in its 2015 roadmap for autonomy as shown in figure 7 is an excellent example of a “levels of autonomy” ordinal scale. The USAF plans to convert specific functions (left axis) over time from man to machine delineated by milestone points (bottom axis) result in full autonomy through eventual data fusion.

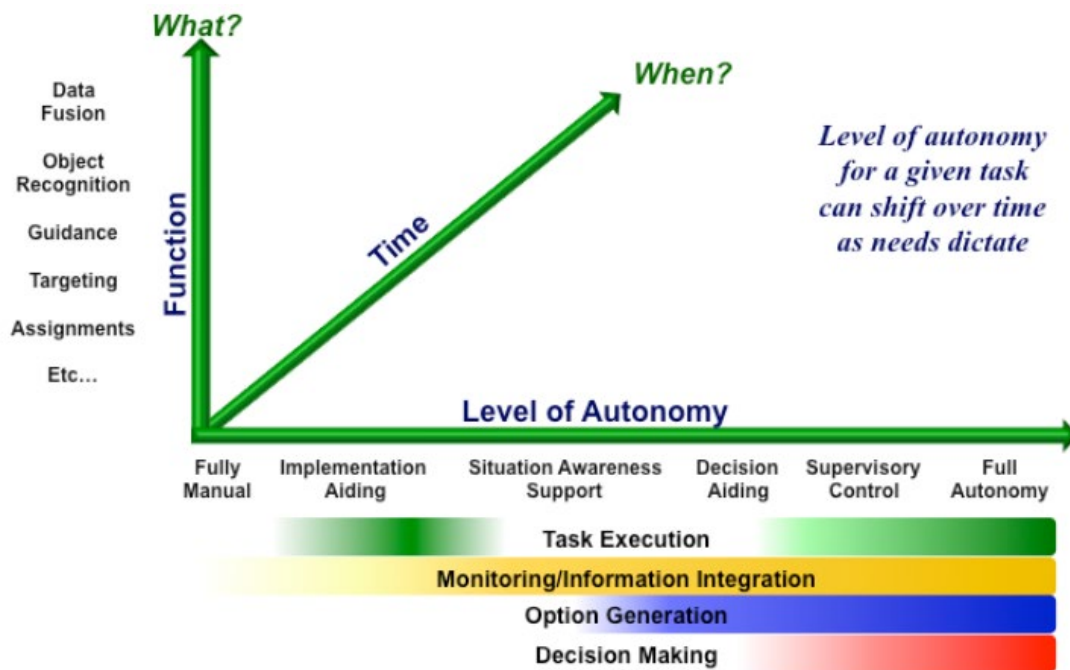


Figure 7. USAF Flexible Autonomy Roadmap

³³ TRADOC G2, *Mad Scientist Laboratory: Forecasting the Future of Warfare*, Blog, 27 November 2017, accessed 30 November 2017, <http://madsciblog.tradoc.army.mil/page/2/>.

Source: United States Air Force Office of the Chief Scientist, *Autonomous Horizons: System Autonomy in the Air Force – A Path to the Future*, vol I: *Human-Autonomy Teaming* (Washington DC: Government Printing Office, June 2015), 10.

While simple to understand at first glance, this chart is based on the overarching assumption that sequential functional interactions along an ordinal axis will ultimately result in intelligent machines assuming traditionally human roles.³⁴ The JCRAS cautions against using scales based on levels of autonomy to develop capability:

While many organizations define specific levels of autonomy to describe task and decision-making allocation, comparing levels of autonomy can be misleading. Designing systems to specific levels of autonomy is not the overarching goal. Rather, enhancing military capability should be the key metric for DoD systems.³⁵

Multi-Dimensional Scales

In contrast to the simplistic design of categorical and linear scales, multi-dimensional scales are complex. They are useful from a systems engineering perspective as they provide descriptions for the functional components that are ascribed to each level of autonomy. Concepts developed by Ryan W. Proud and Bruce Clough are the most commonly cited multi-dimensional scales. Derived from Thomas B. Sheridan's

³⁴ “Though attractive, the conceptualization of levels of autonomy as a scientific grounding for a developmental roadmap has been unproductive. . . . Research shows that a mission consists of dynamically changing functions, many of which can be executing concurrently as well as sequentially. Each of these functions can have a different allocation scheme to the human or computer at a given time. This dynamic view of human-machine interaction leads back to the definition of autonomy as a capability in which the milestones create the set of interactions needed to produce the desired result.” Defense Science Board, *Task Force Report: The Role of Autonomy in DoD Systems* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, June 2012), 24.

³⁵ Joint Chiefs of Staff, *JCRAS*, 14.

categorical scale, Proud and Clough envision increasing levels of autonomy described in terms of Col John Boyd's observe, orient, decide, act loop with each level functionally separated into descriptions of how machines will observe, orient, decide, and act.³⁶ An excerpt from Proud's scale is provided in table 2 as an example.

³⁶ Williams and Scharre, *Autonomous Systems*, 45-49.

Table 2. Excerpt from Proud's Levels of Autonomy

Level	Observe	Orient	Decide	Act
8	The computer gathers, filters, and prioritises data without displaying any information to the human.	The computer predicts, interprets, and integrates data into a result that is not displayed to the human.	The computer performs ranking tasks. The computer performs final ranking, but does not display results to the human.	Computer executes automatically and does not allow any human interaction.
7	The computer gathers, filters, and prioritises data without displaying any information to the human, though a 'program functioning' flag is displayed.	The computer analyses, predicts, interprets, and integrates data into a result that is only displayed to the human if it fits the programmed context (context-dependent summaries).	The computer performs ranking tasks. The computer performs final ranking and displays a reduced set of ranked options without displaying 'why' decisions were made to the human.	Computer executes automatically and only informs the human if required by context. It allows for over-ride ability after execution. Human is shadow for contingencies.
6	The computer gathers, filters, and prioritises information displayed to the human.	The computer overlays predictions with analysis and interprets the data. The human is shown all results.	The computer performs ranking tasks and displays a reduced set of ranked options while displaying 'why' decisions were made to the human.	Computer executes automatically, informs the human, and allows for over-ride ability after execution. Human is shadow for contingencies.
5	The computer is responsible for gathering the information for the human, but it only displays non-prioritised, filtered information.	The computer overlays predictions with analysis and interprets the data. The human shadows the interpretation for contingencies.	The computer performs ranking tasks. All results, including 'why' decisions were made, are displayed to the human.	Computer allows the human a context-dependent restricted time to veto before execution. Human shadows for contingencies.
4	The computer is responsible for gathering the information for the human and for displaying all information, but it highlights the non-prioritised, relevant information for the user.	The computer analyses the data and makes predictions, though the human is responsible for interpreting it.	Both the human and computer perform ranking tasks, and the results from the computer are considered prime.	Computer allows the human a pre-programmed restricted time to veto before execution. Human shadows for contingencies.

Source: Andrew P. Williams and Paul Scharre, eds., *Autonomous Systems: Issues for Defence Policymakers* (NATO Communications and Information Agency), 47-48, accessed 20 September 2017, <http://www.act.nato.int/>.

Versions of this type of scale are popular within engineering and academic communities. In the article "Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction," the authors propose a taxonomy describing levels of robot

autonomy based on the functions of sense, think, and act as depicted in table 3. This scale that has become the foundational standard for the IEEE's development of autonomy standards.³⁷

Table 3. Levels of Robotic Autonomy Taxonomy

LORA	Sense	Plan	Act	Description	Examples from Literature
Manual	H	H	H	The human performs all aspects of the task including sensing the environment, generating plans/options/goals, and implementing processes.	"Manual Control" Endsley & Kaber, 1999
Tele-operation	H/R	H	H/R	The robot assists the human with action implementation. However, sensing and planning is allocated to the human. For example, a human may teleoperate a robot, but the human may choose to prompt the robot to assist with some aspects of a task (e.g., gripping objects).	"Action Support" Endsley & Kaber, 1999; Kaber et al., 2000; "Manual Teleoperation" Milgram, 1995; "Tele Mode" Baker & Yanco, 2004; Bruemmer et al., 2005; Desai & Yanco, 2005
Assisted Tele-operation	H/R	H	H/R	The human assists with all aspects of the task. However, the robot senses the environment and chooses to intervene with task. For example, if the user navigates the robot too close to an obstacle, the robot will automatically steer to avoid collision.	"Assisted Teleoperation" Takayama et al., 2011; "Safe Mode" Baker & Yanco, 2004; Bruemmer et al., 2005; Desai & Yanco, 2005
Batch Processing	H/R	H	R	Both the human and robot monitor and sense the environment. The human, however, determines the goals and plans of the task. The robot then implements the task.	"Batch Processing" Endsley & Kaber, 1999; Kaber et al., 2000
Decision Support	H/R	H/R	R	Both the human and robot sense the environment and generate a task plan. However, the human chooses the task plan and commands the robot to implement actions.	"Decision Support" Endsley & Kaber, 1999; Kaber et al., 2000
Shared Control With Human Initiative	H/R	H/R	R	The robot autonomously senses the environment, develops plans and goals, and implements actions. However, the human monitors the robot's progress and may intervene and influence the robot with new goals and plans if the robot is having difficulty.	"Shared Mode" Baker & Yanco, 2004; Bruemmer et al., 2005; Desai & Yanco, 2005; "Mixed Initiative" Sellner et al., 2006; "Control Sharing" Tam et al., 1995
Shared Control With Robot Initiative	H/R	H/R	R	The robot performs all aspects of the task (sense, plan, act). If the robot encounters difficulty, it can prompt the human for assistance in setting new goals and plans.	"System-Initiative" Sellner et al., 2006; "Fixed-Subtask Mixed-Initiative" Hearst, 1999
Executive Control	R	H/R	R	The human may give an abstract high-level goal (e.g., navigate in environment to a specified location). The robot autonomously senses environment, sets the plan, and implements action.	"Seamless Autonomy" Few et al., 2008; "Autonomous mode" Baker & Yanco, 2004; Bruemmer et al., 2005; Desai & Yanco, 2005
Supervisory Control	H/R	R	R	The robot performs all aspects of task, but the human continuously monitors the robot, environment, and task. The human has override capability and may set a new goal and plan. In this case, the autonomy would shift to executive control, shared control, or decision support.	"Supervisory Control" Endsley & Kaber, 1999; Kaber et al., 2000
Full Autonomy	R	R	R	The robot performs all aspects of a task autonomously without human intervention with sensing, planning, or implementing action.	"Full Automation" Endsley & Kaber, 1999

*Note: H = Human, R = Robot. Manual represents a situation where no robot is involved in performing the task; this level is included for a complete taxonomy continuum.

Source: Jenay Beer, Arthur D. Fisk, and Wendy A. Rogers, "Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction," *Journal of Human-Robot Interaction* 3, no. 2, © (2014), Table 4: 87. Permission for use is granted under Creative Commons.

³⁷ Jenay Beer, Arthur D. Fisk, and Wendy A. Rogers, "Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction," *Journal of Human-Robot Interaction* 3, no. 2, © (2014), Table 4: 88

The DoD also refers to this scale in multiple studies and reports. For example, the Defense Science Board (DSB) conducted a summer study on autonomy in 2016 that uses the framework in table 3 to categorize RAS activities by sense, think, decide, act and team with current, near, and long-term goals for each category.³⁸

Multi-dimensional scales have more utility than categorical and linear scales because they present a more holistic view of autonomy in which users can “slide” between levels based on tasks within a functional area. For example, in a semi-autonomous weapons system such as a fighter aircraft a human may be in-the-loop for decide and act functions related to weapons engagements, on-the-loop for tasks related to observe and orient relative to threat along the route of flight, and out-of-the-loop for tasks related to the maneuver of the air vehicle along the route of flight.

Contextual Scales

Contextual scales are the most complex of the scales discussed in this research as they often operate in multiple axes and define autonomy relative to conditions external to the system.³⁹ A well known contextual scale is the ALFUS developed by the National Institute of Standards and Technology which defines autonomy along three separate axes: mission complexity, environment complexity, and human independence. The

³⁸ Defense Science Board, *Summer Study on Autonomy* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, June 2016), 11.

³⁹ Williams and Scharre, *Autonomous Systems*, 51.

scores from the sub-tasks along each axis are then weighted and tallied to provide an overarching score along the level of autonomy chart shown in figure 8.⁴⁰

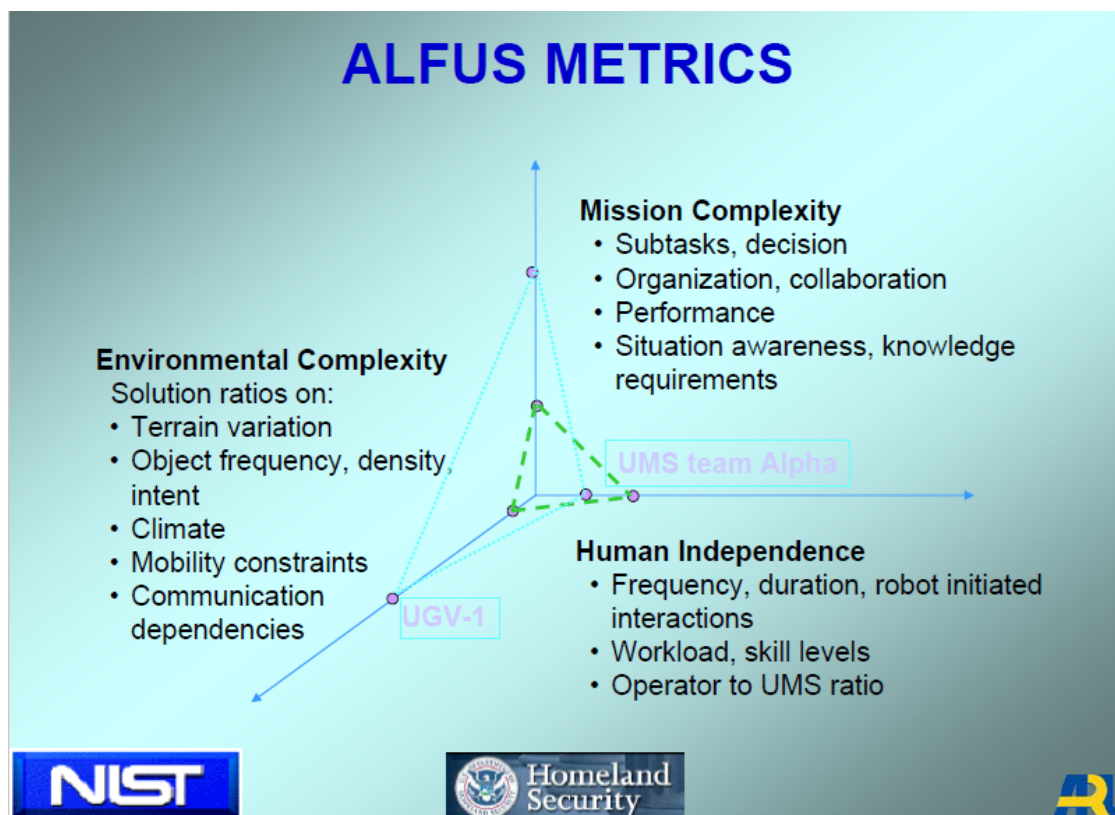


Figure 8. ALFUS Contextual Scale

Source: Hui-Min Huang, “Autonomy Levels for Unmanned Systems (ALFUS), Slide 8, accessed 2 October 2017, <https://www.nist.gov/sites/default/files/documents/el/isd/ks/ALFUS-BG.pdf>.

Paul Scharre also proposes a three axis concept for the dimensions of autonomy composed of the human-machine command-control relationship, the complexity of the

⁴⁰ Williams and Scharre, *Autonomous Systems*, 51.

machine, and the type of decision being automated.⁴¹ Autonomy is characterized along each axis as follows: the first by the relationship between the machine and controller (in/on/out of the loop), the second by the level of “automation” or “intelligence” possessed by the machine, and the third by the task that the machine is performing relatively to its complexity and risk.⁴² Scharre’s framework for autonomy supports the concepts for “autonomous functioning within a system” and “centaur teaming” which will be further discussed in the analysis section of the literature review.

Other contextual scales include the proposal from the 2012 DSB in figure 9 which recommends approaching autonomy from three different perspectives: the cognitive echelon view, the mission dynamics view, and the complex systems trade space view. The most comprehensive of the frameworks discussed in this literature review, the 2012 DSB concept was developed specifically to support capability developers. The authors of the 2012 DSB go so far as to state that the DoD should abandon the concept of levels of autonomy and develop a framework that focuses on delineating the functions and responsibilities between humans and machines.⁴³

⁴¹ Michael C. Horowitz and Paul Scharre, “An Introduction into Autonomy in Weapons Systems” (Working Paper, Center for a New American Security, Washington, DC, February 2015), 6.

⁴² Horowitz and Scharre, “An Introduction into Autonomy in Weapons Systems,” 6-7.

⁴³ Defense Science Board, *Summer Study on Autonomy*, 4.

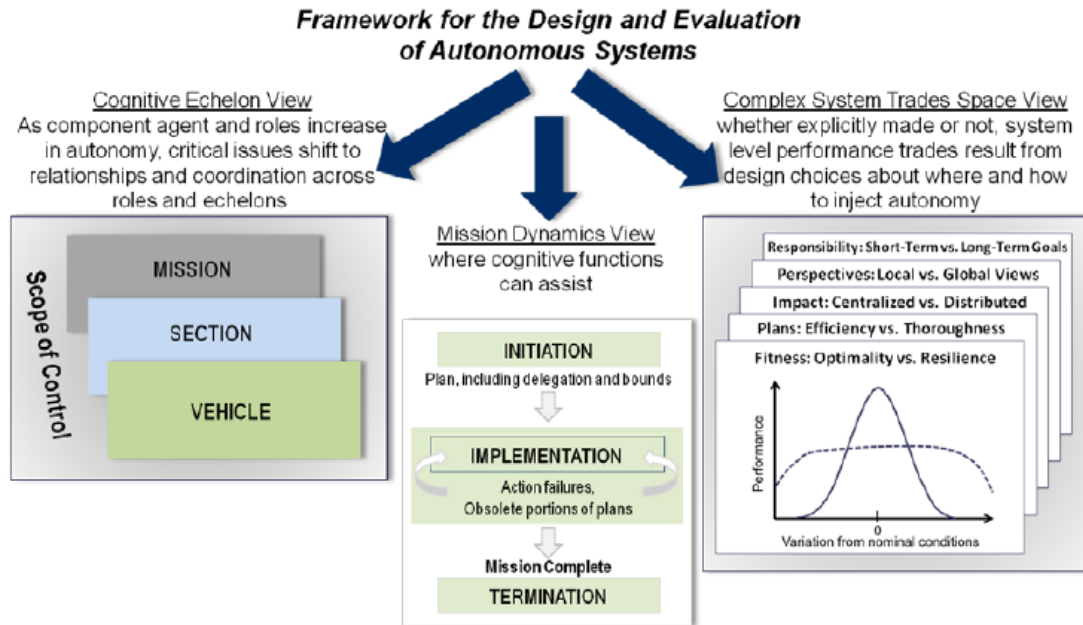


Figure 9. 2012 DSB Framework for the Design and Evaluation of Autonomous Systems

Source: Defense Science Board, *Summer Study on Autonomy* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, June 2016), 5.

The 2012 DSB authors make a point that any conceptual framework must visualize the challenges of autonomy from the standpoint of three separate stakeholders: the commander, the operator, and the developer.

For the commander, the design space and tradeoffs for incorporating autonomy into a mission are not well understood. Any changes in how missions are accomplished will result in new operational consequences, which the commander must manage.

For the operator, autonomy is experienced as human-machine collaboration, which often is overlooked during design.

For the developer, autonomy is primarily software. Software development is generally outside of the current hardware-oriented, vehicle-centric development and acquisition processes. Program managers may not know how to specify autonomy software, developers may not have sufficient expertise to write

autonomy software, and testing and evaluation have few metrics and test beds for verification and validation.⁴⁴

To further illustrate the points made in the 2012 DSB report, Dr. Illachianski produced the chart in figure 10 as part of his study entitled “AI, Robots, and Swarms: Issues, Questions, and Recommended Studies”. The key points regarding the cognitive echelon, trade space, and mission dynamics are overlaid on a three axes model similar to the ALFUS. Illachianski theorizes that:

A framework’s ability to support the requirements specification, design, development, and review/approval phases of the acquisition process . . . is therefore contingent upon it embodying three classes of design decisions for autonomy that reflect the larger abstract space in which each of the three notional stakeholders live.⁴⁵

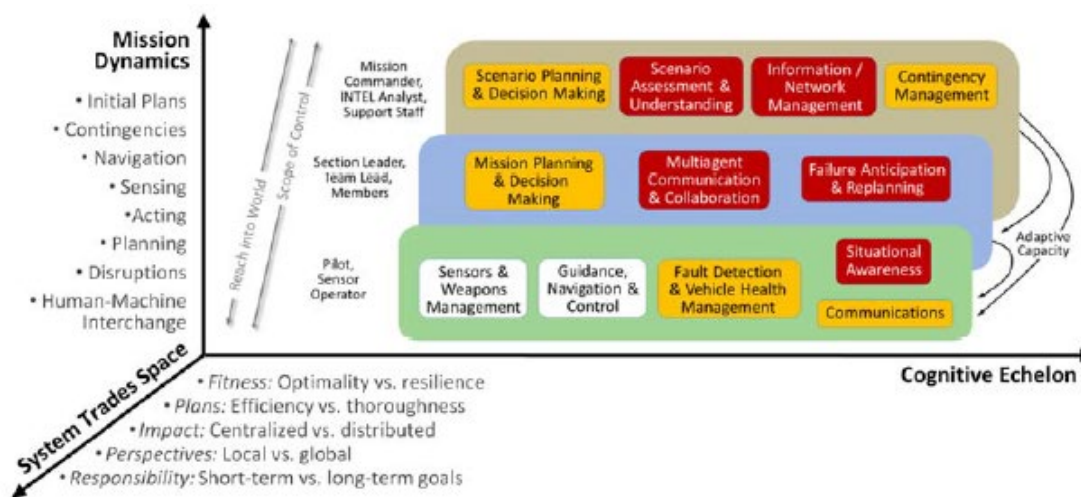


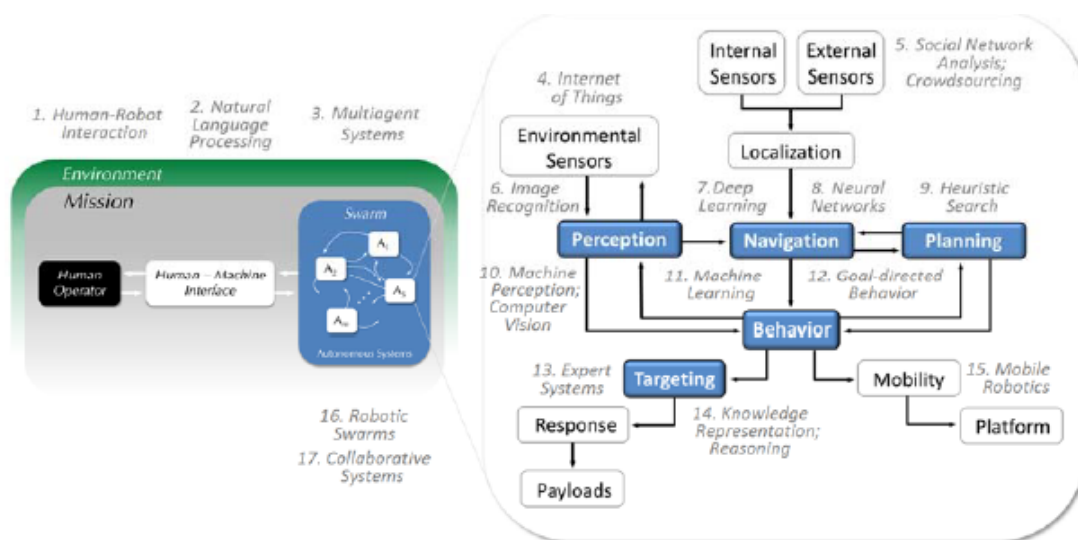
Figure 10. Autonomous System Reference Framework (ASRF)

Source: Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies* (Arlington, VA: Center for Naval Analyses, January 2017), 169.

⁴⁴ Defense Science Board, *Summer Study on Autonomy*, 23.

⁴⁵ Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies* (Arlington, VA: Center for Naval Analyses, January 2017), 169.

The last scale discussed in the literature review is really a conglomeration of categorical, multi-dimensional, and contextual scales representing a way to understand a complex adaptive system-of-systems. While the diagram in figure 11 is more of a “how to” build Unmanned Aircraft Systems (UAS) swarm behavior than a conceptual framework for autonomy, it shows the applicability of how a taxonomy linked within a conceptual framework could be used to establish both programmatic milestones and generate requirements. By adding couplings based on human interaction, environment, mission, and interactions with other UAS, this framework addresses all the points of sense, think, decide, act, and team in ways that are useful to capability developers, acquisition professionals, and policy makers.



Right-hand-side of figure based on figure 3.1 in A. Finn and S. Scheduling, *Developments and Challenges for Autonomous Unmanned Vehicles*, Springer-Verlag, 2010.

Figure 11. Generalizing UAS as a Complex Adaptive System of Systems

Source: Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies* (Arlington, VA: Center for Naval Analyses, January 2017), 99.

Current DoD Framework for Autonomy: The Joint Concept for Robotics and Autonomous Systems

The Joint Concept for Robotics and Autonomous Systems (JCRAS) provides the framework, taxonomy, and lexicon that the Services use to develop autonomous capabilities. It is general and more conceptual than the information already presented in this chapter. The JCRAS uses the terms “Robot” and “Robotic and Autonomous Systems” to discuss human-machine collaboration within the spheres described in figure 3:

Robot: a powered machine capable of executing a set of actions by direct human control, computer control, or a combination of both. It is comprised minimally of a platform, software, and a power source.

Robotic and Autonomous Systems (RAS): is an accepted term in academia and the science and technology (S&T) community; it highlights the physical (robotic) and cognitive (autonomous) aspects of these systems. For purposes of this concept, RAS is a framework to describe systems with a robotic element, an autonomous element, or more commonly, both. As technology advances, there will be more robotic systems with autonomous capabilities as well as non-robotic autonomous systems.⁴⁶

The JCRAS specifically discusses robots executing assigned tasks under human control as part of a system. The lowest degree of autonomy is generally associated with remote control or tele-operation in which robotic functions are either automatic or automated based on rules governing the system. The term “flexible autonomy” is used to describe the entire range of how humans collaborate with or transition work to machines up to, but not including, full autonomy.

The JCRAS defines the Concept Required Capability (CRC) for “flexible autonomy” as follows: “CRC 3. The Joint Force requires the ability to operate RAS

⁴⁶ Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, 2.

along the spectrum of autonomous operations, from full human to highly autonomous control.”⁴⁷ Of note, CRC 3 explicitly defines the high end of the spectrum as “highly autonomous control” versus the “fully autonomous” level generally envisioned in academic taxonomies. It also enforces a limitation of maintaining positive control over RAS.⁴⁸ The JCRAS also states that: “RAS will not replicate human judgment, intuition, empathy, morality, or understanding in military operations . . . humans will remain the essential team element, retaining overall responsibility for mission accomplishment.”⁴⁹ The concept does not contain any graphics that describe flexible autonomy or any taxonomy beyond the terms robot and RAS.

In summary, there are a variety of conceptual frameworks describing the spectrum of autonomy but the DoD does not use any of the scales discussed in this literature review in either Joint concepts or doctrine. The Services tend to default to the use of categorical or linear scales because they are easy to understand and support the establishment of programmatic milestones. The private sector tends to use multi-dimensional or contextual scales because they support approaching autonomy from an engineering perspective. The lack of common terms and standards resident in policy and guidance result in the Services developing similar autonomous capabilities from vastly different perspectives.

⁴⁷ Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, 14.

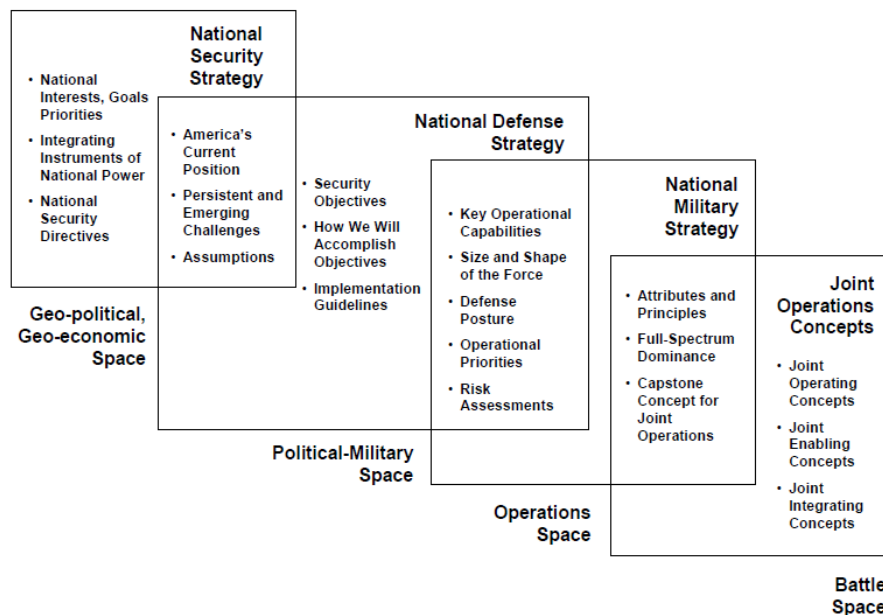
⁴⁸ It is imperative that the Joint Force develop positive controls to apply appropriate levels of human judgment commensurate with acceptable levels of risk. In some cases, such as a degraded communications environment, the appropriate level of human judgment may be last applied at the decision to employ an autonomous system. Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, 7.

⁴⁹ Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, 6.

Strategic Guidance and Policy for Autonomy and AI

This section reviews the hierarchy of strategic guidance and policy within the DoD pertaining to autonomy and AI. Table 4 is a visual depiction of this hierarchy which shows policy nested within a shared space between the NSS and the NDS. The National Military Strategy (NMS) will not be discussed in this research as it is currently under revision.

Table 4. Hierarchy and Relationships between Guidance



Source: Chairman of the Joint Chiefs of Staff, *Capabilities-Based Assessment (CBA) User's Guide: Version 3. Force Structure, Resources, and Assessments Directorate (JCS J-8)* (Washington, DC: Government Printing Office, March 2009), 16.
Note: Relationships between strategic documents.

The NSS, NDS, and 3OS strategies provide specific guidance to the DoD related to the development of autonomous capabilities. Their key tenants are translated into DoD policy through the Department of Defense Directives (DoDD) and Department of

Defense Instructions (DoDI) (hereafter referred to overarching as “issuances” unless a specific issuance is being discussed). Policy in turn results in guidance to the force for RAS published in the JCRAS and other Chairman of the Joint Chiefs of Staff (CJCS) directives, S&T/R&D strategies, and the JOC.

The NSS is the foremost strategic guidance document. It provides specific guidance for the US government regarding IT innovation:

To retain military overmatch the United States must restore our ability to produce innovative capabilities (and) restore the readiness of our forces for major war . . . by aligning our public and private sector efforts we can field a Joint Force that is unmatched. New advances in computing, autonomy, and manufacturing are already transforming the way we fight.⁵⁰

The NSS continues on to state that this will be accomplished by changing the acquisition process to leverage private capital and expertise to rapidly build and innovate:

The U.S. Government will use private sector technical expertise and R&D capabilities more effectively. Private industry owns many of the technologies that the government relies upon for critical national security missions. The Department of Defense and other agencies will establish strategic partnerships with U.S. companies to help align private sector R&D resources to priority national security applications.⁵¹

The executive branch receives policy advice for how these goals will be accomplished from the Office of Science and Technology Policy⁵² then coordinates

⁵⁰ Office of the President of the United States, *The National Security Strategy of the United States of America*, 28.

⁵¹ Ibid., 21.

⁵² As of July 2017, the “OSTP staff comprises 35 people. Under the administration of Barrack Obama, the OSTP had more than 100 employees, many of whom were detailed to the office for six-month stints from other federal agencies or were working on contract.” Bob Grant, “White House Science Office in Flux,” *The*

policy into action through the National Science and Technology Council. A whole of government policy for AI is still in development so Federal Agencies have developed their own policies consistent with strategic guidance. The 2016 National Artificial Intelligence Research and Development Strategic Plan states the desired outcome for coordinated governmental investment in AI development as follows:

The Federal government is the primary source of funding for long-term, high-risk research initiatives, as well as near-term developmental work to achieve department- or agency-specific requirements . . . that private industry does not pursue. The Federal government should therefore emphasize AI investments in areas of strong societal importance that are not aimed at consumer markets—areas such as . . . national security, as well as long-term research that accelerates the production of AI knowledge and technologies.⁵³

Since the AI R&D strategic plan does not define research agendas for Federal agencies, the DoD is able to pursue priorities consistent with its mission, budget, and authorities.⁵⁴ Because of this, the NDS focuses autonomy and AI policy, research priorities, and funding based on the tasks from the NSS specific to the DoD. It addresses separate lines of effort to expand the competitive space by reforming business practices and modernizing to achieve a more lethal Joint Force.⁵⁵ Specific to modernization: “The Department will invest broadly in military applications of autonomy, artificial

Scientist, 3 July 2017, accessed 23 April 2018, <https://www.the-scientist.com/?articles.view/articleNo/49787/title/White-House-Science-Office-in-Flux/>.

⁵³ National Science and Technology Council, “The National and Artificial Intelligence Research and Development Strategic Plan,” *Networking and Information Technology Research and Development Subcommittee* (October 2016), 7.

⁵⁴ Ibid.

⁵⁵ Department of Defense, “Remarks by Secretary Mattis on the National Defense Strategy,” 5.

intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages.”⁵⁶

The commitment in both documents to invest in emerging technology like autonomy in order to provide an asymmetric advantage to the Joint Force is clear. The NDS intent on bureaucratic and budgetary reform is to “deliver performance at the speed of relevance” as outlined below:

Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting. Current processes are not responsive to need; the Department is over-optimized for exceptional performance at the expense of providing timely decisions, policies, and capabilities to the warfighter. Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades. We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change. Delivering performance means we will shed outdated management practices and structures while integrating insights from business innovation.⁵⁷

Additional objectives contained within the NDS include streamlining the way the DoD develops and fields capabilities to “increase the speed of delivery, enable design tradeoffs in the requirements process, [and] expand the role of warfighters . . . throughout the acquisitions process.”⁵⁸ Increased emphasis on prototyping and experimentation early in the requirements development process coupled with modular electronics and software design could support rapid parts replacement and upgrade capability. The NDS also states that the DoD will seek to provide the defense industry

⁵⁶ Department of Defense, “Remarks by Secretary Mattis on the National Defense Strategy,” 6.

⁵⁷ Ibid., 10.

⁵⁸ Ibid., 11.

with more predictability to inform research and development as well as streamline processes to support new and non-traditional vendor participation.⁵⁹

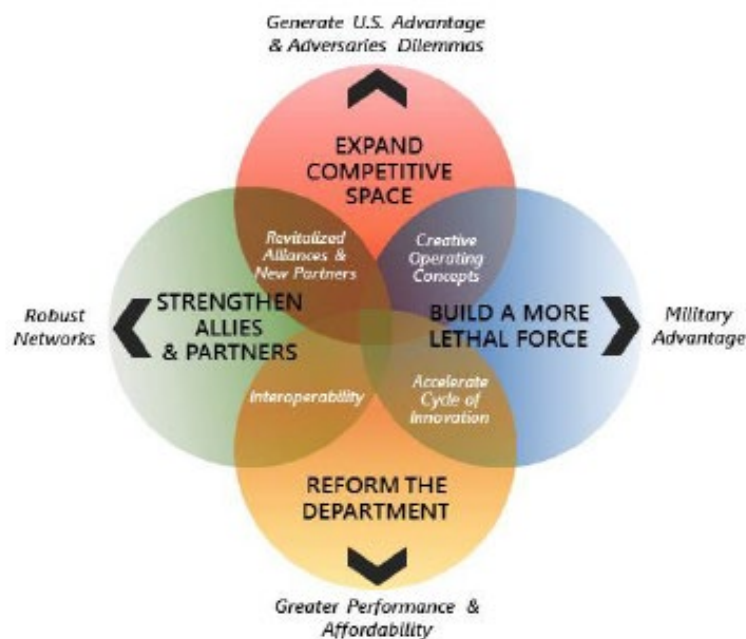


Figure 12. Overview of the Pillars of the NDS

Source: Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*, February 2018, 2-4, accessed 26 March 2018, <https://www.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf>.

Separate from and subordinate to the NSS and the NDS, the 3OS seeks to achieve conventional overmatch against near-peer threats by developing “machine learning and (AI)—and the vastly improved autonomous systems and operations they

⁵⁹ Department of Defense, “Remarks by Secretary Mattis on the National Defense Strategy,” 11.

will enable . . . involving human-machine collaboration and combat teaming.⁶⁰ The primary spokesman for the strategy, former Deputy Secretary of Defense Robert O. Work, has stated that “The 3OS exploits AI and autonomy, but it generally sees humans remaining either in the loop or on the loop—as is suggested by the terms *human-machine collaboration* and *human-machine combat teaming* . . . the human always comes first.”⁶¹ Specifically, the 3OS seeks to identify and invest in innovative ways to address the erosion of US technological superiority and advance US military dominance.⁶² “AI is seen as the key enabling technology (along with human computer interactions of various kinds) [for the 3OS] that seeks for the U.S. a unique, asymmetric advantage over near-peer adversaries.”⁶³ While the 3OS has been in place since 2014, it is still nebulously defined and executed based on technology development, acquisition reform, strategic partnerships with industry, and policy itself.

Within the DoD, various issuances pertain to autonomy and AI. The issuances listed in table 5 are not a holistic list of every regulatory document that could be applied

⁶⁰ Octavian Manea, “The Role of Offset Strategies in Restoring Conventional Deterrence,” *Small Wars Journal* (4 January 2018): 6, accessed 22 January 2018, <http://smallwarsjournal.com/jrnl/art/the-role-of-offset-strategies-in-restoringconventional-deterrence>.

⁶¹ Manea, “The Role of Offset Strategies in Restoring Conventional Deterrence,” 9.

⁶² Bob Work, Deputy Secretary of Defense, “The Third U.S. Offset Strategy and its Implications for Partners and Allies” (Speech, Willard Hotel, Washington, DC, 28 January 2015), 5, accessed 31 January 2018, <https://www.defense.gov/News/Speeches/Speech-iew/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.

⁶³ Richard Potember, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD* (McLean, VA: MITRE Corporation, 2017), 1.

to autonomous capability regulation but they cover the majority of the topics covered in this research and are focused on the development of autonomous and semi-autonomous weapons systems regardless of lethality.

Table 5. DoD Issuances that Provide Policy and Standards for Autonomy

DoDD 2311.01E	DoD Law of War Program
DoDD 3000.03E	DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy
DoDD 3000.09	Autonomy in Weapon Systems
DoDI 3200.19	Non-Lethal Weapons (NLW) Human Effects Characterization
DoDI 8320.07	Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense
DoDI 8330.01	Interoperability of Information Technology (IT), Including National Security Systems (NSS)
DoDI 8500.01	Cybersecurity
DoDI 5000.02	Operation of the Defense Acquisition System

Source: Developed by author.

Specific to this research, DoDD 3000.09 is the most pertinent issuance. It “establishes DoD policy and assigns responsibilities for the development and use of autonomous and semi-autonomous functions in weapon systems, including manned and unmanned platforms.”⁶⁴ It states that DoD policy for “autonomous and semi-

⁶⁴ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, change 1 (Washington, DC: Department of Defense, 8 May 2017), 1.

autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force.”⁶⁵ Fully autonomous weapons systems are authorized to be developed if approved in accordance with the review process in Enclosure 3 with the understanding that a human would still be making a decision to employ the weapons system.⁶⁶ Specific authorities are defined for the review and approval processes most notably the CJCS. In DoDD 3000.09, the CJCS is designated as the approval authority for autonomous weapons systems and is also responsible for assessing requirements, publishing joint doctrine for, and advising the Secretary of Defense on the capabilities and employment of such systems.⁶⁷

These responsibilities are derived from DoDD 5000.01 “Functions of the DoD and its major components.”⁶⁸ Guidance to the Service is contained in directives; of note none currently pertain to autonomy and AI. The closest document to Joint Doctrine in the CJCS library that discusses AI and autonomy is the JCRAS.⁶⁹

The JRCAS provides guidance for RAS capability development and integration to the Services stating that:

⁶⁵ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, 2.

⁶⁶ Ibid., 7.

⁶⁷ Ibid., 12.

⁶⁸ Department of Defense, Department of Defense Directive 5100.01, *Functions of the Department of Defense and its Major Components* (Washington, DC: Department of Defense, 21 December 2010), 15.

⁶⁹ Concepts are not doctrine. Concepts discuss emerging capabilities and identify implications of future requirements.

This concept's central idea is to integrate RAS into joint operations across all functions by 2035 to increase the joint force commander's options. . . . Emerging capabilities, such as Human-RAS teaming and autonomy, offer the Joint Force potential solutions to the challenges of the future operating environment.⁷⁰

According to the JCRAS, humans will always be the essential part of RAS and will retain responsibility for military decisions. JCRAS guidance to the Services espouses centaur teaming and human centric operations. It discusses limiting robots to performing tasks in support of humans, teaming with humans, and conducting tasks which reduce risk to personnel with at least the same efficiency as humans:

This concept envisions a future Joint Force that capitalizes on technological advances to embed highly-capable and interconnected RAS into every echelon and formation. RAS evolve from tools for basic tasks into team members capable of coordinating and collaborating across domains and Services. . . humans will remain the essential team element, retaining overall responsibility for mission accomplishment.⁷¹

Of note, the JCRAS disagrees with the NSS and NMS about RAS changing the nature of war. It also strongly espouses a comprehensive Joint approach to capability development focused on enhancing system interoperability and reducing overlaps and excessive costs. It cautions that:

If the Joint Force does not take a proactive role in guiding the development and integration of RAS among the Services and with partners and allies, there is the potential that development and implementation will remain stove-piped, with each organization developing its own platforms and capabilities.⁷²

In summary, there are a variety of conceptual frameworks that describe human-machine collaboration and no general consensus within the DoD as to which should be used as a standard for describing and developing autonomous capabilities. The terms the DoD currently uses to describe autonomous

⁷⁰ Joint Chiefs of Staff, *JCRAS*, iii.

⁷¹ *Ibid.*, 6.

⁷² *Ibid.*, 1.

capabilities are not the same as those used within the private sector and are generally more simplistic and ambiguous. Strategic guidance discusses the need to collaborative fund and develop AI and autonomy in conjunction with the private sector yet the DoD is able to largely pursue its own R&D with limited interaction with other federal agencies. Strategic guidance addresses the need to adapt policy and acquisition to develop, acquire, and integrate RAS rapidly but the CJCS has published limited information how to achieve these goals beyond the JCRAS. Because of all of these things, DoD leadership is generally under-educated on RAS and has developed misconceptions about human-machine collaboration. This results in both over-trust and under confidence in machines leading to efforts to both develop and limit the operational autonomy of systems.

CHAPTER 3

RESEARCH METHODOLOGY

Introduction

The intent of this paper is to identify why the DoD is losing its asymmetric RAS advantage as compared to peer competitors. The DoD's required RAS capabilities are analyzed, gaps in RAS development, acquisition and integration are identified, and mitigations are proposed to address each gap. Capabilities are assessed based on strategic guidance and Joint operating concepts. Gaps across DOTMLPF-P were identified specifically related to policy, doctrine, leadership, and materiel. Mitigations were developed based on a qualitative analysis of research focused on identifying ways that the DoD can innovate and modernize in a time of budget constraints.

Primary Research Method

The primary research methodology used for this paper is an analytic inductive qualitative research method looking for common themes and issues within the current published literature on autonomy. The secondary research method is the capabilities based assessment. The paper is organized as a crosswalk of current strategic guidance, policy, and directives with similar literature produced by the private sector defining AI development and policy. Background information is provided to explain how the DoD arrived at its current state of RAS development, acquisition and integration. DoD future operating concepts and acquisition plans are then compared to the strategic plans of peer competitors to assess gaps. Mitigations for gaps are then proposed as part of the conclusions and recommendations.

Chapters 1 introduces the subject material and presents a synopsis of the CBA. Chapter 2 provides background information on AI and autonomy, proposes a framework for understanding the research material, and provides an overview of strategic guidance and policy. Chapter 3 discusses the research methodology and format of the research. Chapter 4 consists of analytic inductive qualitative research looking for common themes and issues related to the development of autonomous capabilities both within the DoD and the private sector. Facts from strategic guidance, policy, and directives are compared and contrasted against research from the private sector to identify gaps in policy, doctrine, leadership, and materiel that are preventing the DoD from rapidly developing, acquiring, and integrating RAS to compete with peer competitors. Chapter 4 is subdivided into several sections to address each of these points as well as to provide analysis to support the assumption that the DoD is losing its asymmetric RAS advantage. The main hypothesis of this research is that the DoD's ability to rapidly develop, acquire, and integrate RAS can be streamlined through re-framing the way that they conceptualize and define AI and autonomy.

Chapter 5 provides the conclusions and recommendations for how the DoD can regain a competitive RAS advantage. The primary intent of this research methodology is to inform the Army's Future Vertical Lift and Future UAS Capability Development Documents. The secondary intent is to propose a conceptual framework, taxonomy and terminology for use in policy (specifically DoDD 3000.09), doctrine (specifically the DoD dictionary), and acquisition. This research is also designed to assist DoD leadership and military personnel who work with RAS about human-machine collaboration to inform their understanding of AI and autonomy.

CHAPTER 4

ANALYSIS

Artificial intelligence isn't able to compensate for human stupidity.
— Syndey J. Freedberg Jr.
“Artificial Stupidity”

This chapter is divided into five sections focused on analysis of the capabilities and gaps presented in the introduction. The chapter begins with an assessment of the strategic plans of China and Russia for funding, developing and integrating RAS. This section highlights key points of competitor develop that will be contrasted with DoD RAS funding, development, and integration in the domains of policy, doctrine, leadership, and acquisition. This analysis supports the recommended mitigations to be presented in chapter 5.

Analysis of the US RAS Development Relative to Peer Competitors

The continuum of conflict is escalating beyond the traditional domains of air, land, and sea: “The evolution of technology—and Russia’s and China’s stated desire to lead on AI research—signals that Western democracies will face increasing threats in the cyber and information domain.”⁷³ Both Russia and China are developing whole of government approaches toward achieving AI dominance by outlining plans to align public and private sector funding and research to support rapid capability development. The following section will analyze China and Russia’s plans and progress toward

⁷³ Polyakova and Boyer, “The Future of Political Warfare,” 3.

achieving qualitative and quantitative RAS advantages over the US in terms of funding, policy, and integration.

In July 2017 the State Council for the People's Republic of China published the "New Generation Artificial Intelligence Development Planning Notice."⁷⁴ The purpose of the plan is "to seize the major strategic opportunity for the development of AI, to build China's first-mover advantage in the development of AI, [and] to accelerate the construction of an innovative nation and global power in science and technology."⁷⁵ The plan provides a whole of government approach including an ideology for cultural acceptance of AI, principles to build lines of effort for its development, and strategic objectives with metrics and goals based on five year increments culminating in China becoming the world power in AI by 2030.⁷⁶ Figure 13 provides compares Chinese and US AI development projecting capabilities over time.

⁷⁴ Original text available at http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm but for the purposes of this research a translated document will be used to ensure accurate interpretation of content.

⁷⁵ Rogier Creemers et al., trans., "A Next Generation Artificial Intelligence Development Plan" (New America Cybersecurity Initiative, 2017), 2.

⁷⁶ Ibid., 2-6.

AI products: Who's ahead? China versus US

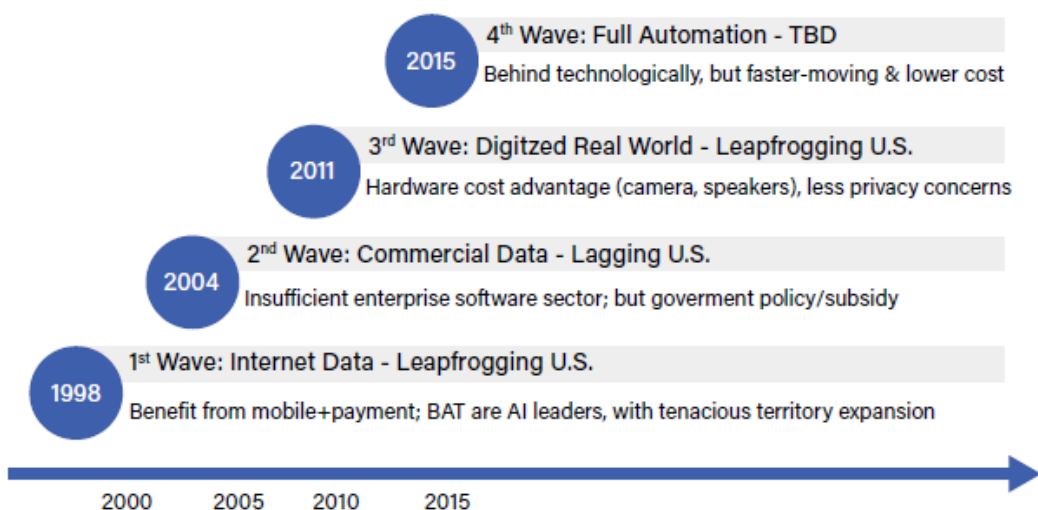


Figure 13. China versus US AI Development

Source: Kai-Fu Lee and Paul Triolo, “China’s Artificial Intelligence Revolution: Understanding Beijing’s Structural Advantages,” Sinovation Ventures, © December 2017, 4, accessed 22 March 2018, https://www.eurasiagroup.net/files/upload/China_Embraces_AI.pdf. Permission for use granted by Deputy Director, Communications Eurasia Group.

The extensive plan covers guidance for implementation across all sectors of society making AI development and integration essential to China’s economic and social prosperity. The economic impact of this plan is illustrated in figure 14 which provides an overview of investment in Chinese AI technology. In recent years China has tripled its science development efforts making it the second largest scientific powerhouse behind the US as well as the second largest investor in R&D in the world.⁷⁷

⁷⁷ The OECD Science, Technology and Industry Scoreboard 2017 contains relevant statistical comparisons of countries investments in technology that are too extensive to cite in this research. For further information see: The OECD Science, “Technology and Industry Scoreboard 2017,” accessed 30 April 2018, https://read.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-scoreboard-2017_9789264268821-en#page15, 13.

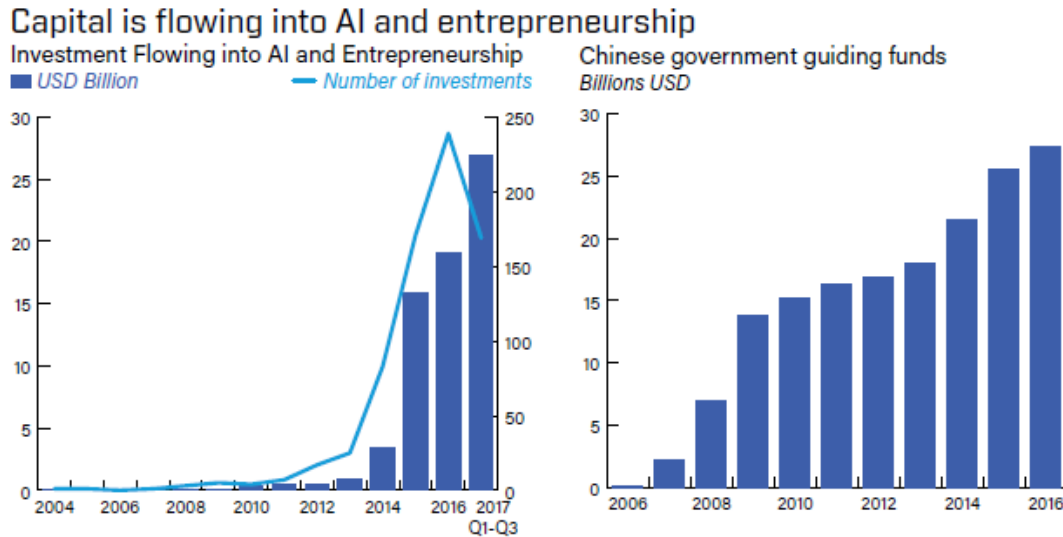


Figure 14. Overview of Investment in Chinese AI Technology

Source: Kai-Fu Lee and Paul Triolo, “China’s Artificial Intelligence Revolution: Understanding Beijing’s Structural Advantages,” Sinovation Ventures, © December 2017, 6, accessed 22 March 2018, https://www.eurasiagroup.net/files/upload/China_Embraces_AI.pdf. Permission for use granted by Deputy Director, Communications Eurasia Group.

While US government investment in S&T sand R&D stagnates⁷⁸ with the private sector expected to fill the funding gap, China’s government holistically supports technology development. In China, “the country’s AI advances stem from significant state support coupled with an increasingly vibrant private sector. Beijing . . . is directing massive capital and policy support to AI. It wants to be the world leader in this field by 2030, aiming to make the industry worth \$150 billion by then.”⁷⁹ China’s main focus is to develop a qualitative RAS advantage over the US. It plans to use RAS to project

⁷⁸ The OECD Science, “Technology and Industry Scoreboard 2017,” 64.

⁷⁹ Yue Wang, “Will the Future of Artificial Intelligence Look Chinese?” *Forbes*, 6 November 2017, accessed 2 February 2018, <https://www.forbes.com/sites/ywang/2017/11/06/will-the-future-of-artificial-intelligence-look-chinese/#306dac847fdc>.

power and contest domains in which the US has traditionally maintained superiority like air, sea, and space. China already possesses significant RAS capabilities that contest the US in cyber and information domains.⁸⁰ China is now modernizing their military through automation and increasing the number of unmanned air and sea vehicles⁸¹. The yearly Beijing air show routinely showcases Chinese advances in hypersonics and unmanned systems although China does not yet have the ability to produce these types of systems in mass. They do have the industrial base to produce disruptive innovations at a massive scale and to embed technology into these commercial systems for nefarious purposes⁸². Based on the strength of their industrial base and the holistic national effort to develop AI, it is possible that China will be able to achieve parity with the US in multiple domains within the next decade.

While lagging well behind the US and China in AI investment and development, Russia is firmly in the AI arms race: “Vladimir Putin said last fall that artificial intelligence is “humanity’s future” and that the country that masters it will “get to rule

⁸⁰ Michael S. Chase, *China’s Conception of Strategic Deterrence also Includes Deterrence in the Space and Information Domains* (Santa Monica, CA: RAND Corporation, 2018), 5, accessed 1 May 2018, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT489/RAND_CT489.pdf.

⁸¹ Eric Baculinao, “The U.S. No Longer Possesses Clear Military-Technical Dominance, and China is Rapidly Emerging as a Would-Be Superpower in Science and Technology,” *NBC News*, 17 February 2018, accessed 1 May 2018, <https://www.nbcnews.com/news/world/these-chinese-military-innovations-threaten-u-s-superiority-experts-say-n848596>.

⁸² US IT manufacturing has significantly declined relative to China since 1995; China now holds almost a 2:1 advantage over the US in this field. The OECD Science, “Technology and Industry Scoreboard 2017,” 59.

the world.”⁸³ Under the auspices of the Ministry of Defense and its research institutions, the Russian government is actively developing and funding AI related projects that span the spectrum from modernization of legacy equipment to tools to wage cyberwarfare.”⁸⁴ Similar to China, Russia is developing a whole of government approach focused on the economic and political security. “In March, Defense Minister Sergei Shoigu . . . [called] for civilian and military designers to join forces to develop artificial intelligence technologies to “counter possible threats in the field of technological and economic security of Russia.”⁸⁵

Russia’s current investment in AI is insignificant compared to US and Chinese funding: “Russia’s annual domestic investment in AI is probably around 700 million rubles (\$12.5 million) – a paltry sum next to the billions being spent by American and Chinese companies.”⁸⁶ While the US still leads Russia and China in both the quality and quantity of autonomous systems “Russia—and others—are catching up fast in important

⁸³ Samuel Bendett, “In AI, Russia is Hustling to Catch Up,” *Defense One*, 4 April 2018, accessed 9 April 2018, <http://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/>.

⁸⁴ “In March, Russian Deputy Minister of Defense Nikolai Pankov said that that hundreds of science and technology departments in the nation’s military universities are currently engaged in R&D related to “artificial intelligence, robotics, military cybernetics and other promising areas.” According to Pankov, the results of this scientific activity “are widely used in the development of new military systems.” Bendett, “In AI, Russia is Hustling to Catch Up.”

⁸⁵ Bendett, “In AI, Russia is Hustling to Catch Up.”

⁸⁶ “Even if private-sector investment rises as expected to 28 billion rubles (\$500 million) by 2020, that will still be just a fraction of the global total.” Bendett, “In AI, Russia is Hustling to Catch Up.”

ways.”⁸⁷ Russia is focused on gaining a quantitative advantage over the US by modernizing conventional weapons to become remotely operated and integrated with AI. They also seek to achieve a qualitative advantage over the US in cyber and the electromagnetic spectrum (EMS) through the development of tools that focus on disruption and disinformation.

Russia has already shown its capabilities to disinform and disrupt in the cyber domain through repeated offensive operations in Western Europe:

The future of political warfare is in the digital domain . . . technological advancements in artificial intelligence and cyber capabilities will open opportunities for malicious actors to undermine democracies more covertly and effectively than what we have seen so far. In addition, increasingly sophisticated cyber tools, tested primarily by Russia in Eastern Europe, have already affected Western systems. An attack on Western critical infrastructure seems inevitable.⁸⁸

Human communication in the digital space is being transformed by the evolution of AI combined with the increasing availability of big data: “It will become more difficult for humans and social media platforms themselves to detect automated and fake accounts, which will become increasingly sophisticated at mimicking human behavior.”⁸⁹ Russia has already shown their ability to utilize AI in this manner to disrupt elections and daily operations in Western countries, as technology evolves it will become more difficult to discern and discredit their social media disinformation campaigns. Russian capabilities to wage cyberwarfare will not be discussed in this

⁸⁷ Samuel Bendett, “Russia is Poised to Surprise the US in Battlefield Robotics,” *Defense One*, 25 January 2018, accessed 9 April 2018, <http://www.defenseone.com/ideas/2018/01/russia-poised-surprise-us-battlefield-robotics/145439/>.

⁸⁸ Polyakova and Boyer, “The Future of Political Warfare,” 6.

⁸⁹ *Ibid.*, 9.

research due to classification delimitations but Russian capabilities are expected to increase given funding, resources, and government sanction.

To achieve a quantitative overmatch on the conventional battlefield, Russia is developing a large and capable fleet of robotics. “The Russian Military Industrial Committee has approved an aggressive plan that would have 30% of Russian combat power consist of entirely remote-controlled and autonomous robotic platforms by 2030.”⁹⁰ Unlike the US, Russia envisions future conventional combat operations being physically conducted by robots, not humans: “The emphasis on armed robots underscores the difference between U.S. concepts of operations, in which unmanned ground systems largely support ISR and augment warfighters’ capabilities, while the Russian military contemplates small to large UGVs doing the actual fighting in the near future alongside or ahead of the human fighting force.”⁹¹

The evidence in this assertion is founded in the modernization and innovation plans across the Russian military. For example,

The future MiG-41 combat aircraft “will be provided with elements of artificial intelligence that will help the pilot to control the aircraft at speeds four to six times higher than the speed of sound,” . . . The Su-35 jet reportedly already has AI that can match available weapons to potential targets. And starting this year, the Russian military will acquire the “Bylina” electronic warfare system, touted as capable of “independent analysis” and “choosing ways to suppress enemy electronic signals.” Russian military experts have said the Bylina is “close to being an actual artificial intelligence system.”⁹²

⁹⁰ Greg Allen and Taniel Chan, “Artificial Intelligence and National Security” (Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA, 2017), 21.

⁹¹ Bendett, “Russia is Poised to Surprise the US in Battlefield Robotics.”

⁹² Bendett, “In AI, Russia is Hustling to Catch Up.”

Russia is developing AI integrated weapons to compete with Western powers in every domain from tactical missiles to unmanned undersea swarming vehicles. Even “Kalashnikov recently announced that it will launch a range of “autonomous combat drones” which will use AI to identify targets and make decisions “on their own.”⁹³ similar to the “slaughterbots” of social media fame. In the area of unmanned systems in particular Russia is seeking to achieve both a qualitative and quantitative overmatch⁹⁴. “Russia’s swift progress in unmanned systems suggest that the United States and its allies should prepare for battle against foes who can put U.S. forces at a disadvantage by inhibiting their operational capabilities.”⁹⁵ Russian ability to team unmanned systems with fires to destroy targets and swarm technology to disrupt ground forces is widely publicized. The US is working on material and training solutions to counter these threats but in other areas like EW Russia is poised to use AI to gain an asymmetric advantage over US conventional forces:

The biggest and fastest breakthroughs based on machine learning can be expected in the realm of electronic warfare. Last year saw the deployment of Russian EW units to Syria, eastern Ukraine, and Crimea, where they are amassing data about the performance and electronic signals and signatures of American and other western assets in the region: aircraft and airborne sensors,

⁹³ Bendett, “In AI, Russia is Hustling to Catch Up.”

⁹⁴ “Russia’s quick production and fielding of UAVs—especially the more affordable, tactical platforms—is resulting in exponential growth in its UAV inventory and in the country’s direct support of UAVs to the Donetsk area and Syria.” For an excellent overview of Russian UAV capability see Nicole Bier and Patrick Madden, “Unmanned Aerial Vehicle Assessment: Russia,” *Red Diamond* (January/February 2018): 9.

⁹⁵ Bendett, “Russia is Poised to Surprise the US in Battlefield Robotics.”

naval vessels, missiles, etc. This data will be fed to machine-learning systems and used to improve Russian EW.⁹⁶

In summary, the US currently maintains qualitative and quantitative advantages over peer competitors as measured by the funding, development, and integration of RAS but Russia and China are rapidly catching up by developing breakthrough technology and modernizing their militaries. Competition across all domains will further increase as AI is integrated as a force multiplier by peer competitors. This will place the US and its allies at a distinct disadvantage if they do not develop the tools to either counter or deter these threats.

Hyper war . . . will place unique requirements on defence architectures and the high-tech industrial base if the Alliance is to preserve an adequate deterrence and defence posture, let alone maintain a comparative advantage over peer competitors. Artificial Intelligence, deep learning, machine learning, computer vision, neuro-linguistic programming, virtual reality and augmented reality are all part of the future battlespace. They are all underpinned by potential advances in quantum computing that will create a conflict environment in which the decision-action loop will compress dramatically from days and hours to minutes and second . . . or even less . . . The United States is moving sharply in this direction in order to compete with similar investments being made by Russia and China, which has itself committed to a spending plan on artificial intelligence that far outstrips all the other players in this arena, including the United States. However, with the Canadian and European Allies lagging somewhat behind, there is now the potential for yet another dangerous technological gap within the Alliance to open up, in turn undermining NATO's political cohesion and military interoperability.⁹⁷

⁹⁶ Bendett, "In AI, Russia is Hustling to Catch Up."

⁹⁷ "Hyper warfare is the idea that future war could take place at such a high level of strategy, technology and destruction that its effects would be worse than the Second World War between 1939 and 1945." GLOBSEC NATO Adaptation Initiative Steering Committee, *One Alliance: The Future Tasks of the Adapted Alliance* (Slovak Republic: NATO, November 2017), 13, 21.

Gap 1: Policy

The National Science and Technology Council recommends that “the US Government should complete the development of a single, government-wide policy, consistent with international humanitarian law, on autonomous and semi-autonomous weapons.”⁹⁸ This is important because “public policies should help ease society’s adaptation to AI applications, extend their benefits, and mitigate their inevitable errors and failures.”⁹⁹ The lack of a whole of government policy for autonomy and AI that resonates with this intent has resulted in inconsistent standards, ambiguous policies, and gaps in R&D funding at the inter-governmental level. DoD policy on autonomous and semi-autonomous systems is vague enough to support current RAS employment within the range of military operations and specific enough to complicate the development of actual autonomous systems. DoD policy is shaped by two key considerations:

1. Acquisition constraints that hinder DoD ability to integrate and employ increasingly autonomous technology at a pace that matches technical advances.
2. DoD attempts to match the development pace of peer competitors who are unconstrained by policy.¹⁰⁰

⁹⁸ Executive Office of the President, *Preparing for the Future of Artificial Intelligence*, 38.

⁹⁹ Peter Stone et al., “Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence” (Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA, September 2016), 10, accessed 13 February 2018. <http://ai100.stanford.edu/2016-report>.

¹⁰⁰ John’s Hopkins Applied Physics Laboratory, “NSAD-R-16-045: Joint Concept for Robotic and Autonomous Systems (JCRAS) Baseline Assessment Report

Ambiguity allows for wide interpretation of policy resulting in public fears that the government is developing “slaughterbots” and “killer robots”. Ambiguity also results in programmatic overlaps and gaps because the Services misinterpret or misuse terminology when vying for funding for programmatic development. Public outcry arises from fears that the government is using AI to design robots capable of unconstrained lethality when in reality the Services are attempting to modernize through increasing automation and machine learning. Reputable studies have found that AI is not “an imminent threat to humankind. No machines with self-sustaining long-term goals and intent have been developed, nor are they likely to be developed in the near future.”¹⁰¹ “Weapons systems and platforms with varying degrees of autonomy exist today in all domains of modern warfare, including air, sea (surface and underwater), and ground . . . It is an important point that, while these systems have some degree of “autonomy” relying on the technologies of AI, they are in no sense a step—not even a small step—towards “autonomy” in the sense of AGI, that is, the ability to set independent goals or intent.”¹⁰² It is important to differentiate the future capabilities of AGI from the narrow AI employed in systems today. “AI . . . will supply enabling technologies for all of [the elements of the 3OS]. At the same time, none of these

Version 2.0” (Briefing prepared for the Joint Staff as an enclosure to task JSJB3, December 2016), 4-24.

¹⁰¹ Stone et al., “Artificial Intelligence and Life in 2030,” 4.

¹⁰² Potember, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, 4.

elements are dependent on future advances in AGI.”¹⁰³ By using the term “autonomous weapons” the DoD in the policy set forth in DoDD 3000.09 has created confusion between the current fleet of highly automated systems and an assumption of future proposals for systems enabled by AGI.¹⁰⁴

¹⁰³ Key elements of the 3OS include “(i) autonomous learning systems, e.g., in applications that require faster-than-human reaction times; (ii) human-machine collaborative decision making; (iii) assisted human operations, especially in combat; (iv) advanced strategies for collaboration between manned and unmanned platforms; and (v) network-enabled, autonomous weapons capable of operating in future cyber and electronic warfare environments.” Potember, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, 5.

¹⁰⁴ “Autonomous robots: Develop robotic systems capable of independently determining a course of action based upon their understanding of the task at hand, their environment, and their own states and capabilities. Autonomy should be sufficiently general, adaptive, and robust in a wide variety of tasks to perform reliably in uncertain or unstructured environments that include humans and other agents that may be friendly, neutral, or adversarial.” The Networking and Information Technology Research and Development Program, *Supplement to the President’s Budget for Fiscal Year 2018* (Washington, DC: The White House, October 2017), 59.

Table 6. DoDD 3000.09 Overview

DoD Directive 3000.09	
Application	Applies to autonomous or semi-autonomous systems weapons systems using lethal or non-lethal force.
Human judgment	Must allow for operators to exercise judgment; interface must be clear and provide traceable feedback; must have procedures for activation/deactivation of system functions.
Human-in-the-loop	A human must make the decision to initiate lethal force.
Function	Must be able to function as anticipated in realistic operational environments (rigorous verification and validation and testing and evaluation is required).
System failure	Systems must have mechanism to ensure they do not autonomously engage targets if communications are interrupted.
Compliance with law	Use requires compliance with IHL, treaties, and rules of engagement.
Commander/operator intent	Requires direction and use be done “with appropriate care” and in compliance with law/policy; does not specify timeframe between target selection and target engagement—only that timeframe must align with commander/operator intent
Systems not explicitly covered by the policy	<u>Does not actually prohibit development of lethal autonomous systems</u> , but requires a separate review process beforehand; systems must be able to comply with policy; waiver can be sought in cases of “urgent military operational need”

Source: John’s Hopkins Applied Physics Laboratory, “NSAD-R-16-045: Joint Concept for Robotic and Autonomous Systems (JCRAS) Baseline Assessment Report Version 2.0” (Briefing prepared for the Joint Staff as an enclosure to task JSJB3, December 2016), 4-27.

DoDD 3000.09 is the foremost policy document for autonomy and it is focused on the role of humans in increasingly autonomous weapons delivery. It does not apply to non-weaponized autonomous systems or systems that operate in cyberspace regardless of their lethal capabilities. As a regulatory document, it lacks the required level of

defined standards and terminology to describe autonomy.¹⁰⁵ The word “autonomy” is not defined in the document and the terms that are included are not mirrored in other guidance or Joint concepts. This is problematic because the Joint Force looks to the standards defined in policy for guidance in developing their capability based concepts. For example, the JCRAS states that “autonomy must comply with higher standards than those in the commercial sector in order to meet the unique demands of military operations.”¹⁰⁶ While there are no universally accepted or defined standards for autonomy and AI, the IEEE has published some standards for autonomy used by the commercial sector as discussed in the literature review.

The policy for autonomous and semi-autonomous weapons is covered in six different DoDD and DoDI, non-lethal autonomous weapons have two additional Directives and Instructions on top of these. None of them contain sufficient information to define useable, transparent standards for autonomous functioning within a system to

¹⁰⁵ The lack of clearly defined standards within DoDD 3000.09 is not endemic to the DoD alone. The National AI R&D Strategic plan addresses the overarching governmental issue as follows: “Standards provide requirements, specifications, guidelines, or characteristics that can be used consistently to ensure that AI technologies meet critical objectives for functionality and interoperability, and that they perform reliably and safely. Adoption of standards brings credibility to technology advancements and facilitates an expanded interoperable marketplace. One example of an AI-relevant standard that has been developed is P1872-2015 (Standard Ontologies for Robotics and Automation), developed by the Institute of Electrical and Electronics Engineers (IEEE). This standard provides a systematic way of representing knowledge and a common set of terms and definitions. These allow for unambiguous knowledge transfer among humans, robots, and other artificial systems, as well as provide a foundational basis for the application of AI technologies to robotics. Additional work in AI standards development is needed across all subdomains of AI.” National Science and Technology Council, “The National and Artificial Intelligence Research and Development Strategic Plan,” 32.

¹⁰⁶ Joint Chiefs of Staff, *JCRAS*, 13.

the extent as those already developed by the IEEE.¹⁰⁷ Because of this, the DoD is heavily reliant upon Senior Leader level reviews to make a determination on the appropriateness of developing autonomous weapons systems.

If a Service wanted to develop an autonomous weapons system¹⁰⁸ they would be required to conduct a senior leader level review in accordance with the procedures published in Enclosure 3 of DoDD 300.09. Since this review has yet to be initiated, it is unknown how long the process itself will take and what additional hurdles will arise as a result. Prior to the review board, a preliminary legal review must be conducted to ascertain if the system will meet the standards in DoDD 2311.01E to ensure that it would comply with the DoD Law of War Program.¹⁰⁹ This type of review will become increasingly complicated as some US Foreign Military Sales countries are developing bans¹¹⁰ on the development of autonomous weapons systems and in 2017 a broad group

¹⁰⁷ The IEEE Standards Association has already developed some standards for AI and autonomous systems and is currently developing an entire family of standards for that field that not only addresses system architecture but also transparency, ethics, reliability. Kathy Pretz, “Three New IEEE Standards for Making Autonomous and Intelligent Systems Safer,” The Institute, 2 February 2018, accessed 30 March 2018, <http://theinstitute.ieee.org/resources/standards/three-new-ieee-standards-for-making-autonomous-and-intelligent-systems-safer>.

¹⁰⁸ An example from the USN of what exactly this means for a Service: “In coordination with, and adherence to broader DOD policy, develop doctrine to specifically introduce and advance the use of lethal autonomous weapons systems (LAWS). Clarify the conditions under which LAWS use is authorized at each level of command from the Naval Component Commander in support of a Joint Force Commander, down to the lowest ranking Sailors and Marines.” Department of the Navy, *Strategic Roadmap for Unmanned Systems*, A-8.

¹⁰⁹ John’s Hopkins Applied Physics Laboratory. “NSAD-R-16-045,” 4-28.

¹¹⁰ Potember, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, 4.

of IT leaders from around the world submitted an open letter to the UN calling on them to ban the development of lethal autonomous weapons.¹¹¹

An outright ban on autonomous weapons systems is unfeasible because so many systems currently in operation already contain components that operate with relative autonomy by employ narrow AI.¹¹² Because of this, policy for autonomous systems should account for modularity in capability design so that limitations could be imposed focused on specific components versus banning entire systems. Functional modularity is discussed in the JCRAS¹¹³ but DoDD 3000.09 is solely focusing on the role of humans in increasingly autonomous weapons delivery, not on weapons systems and their components.

There are additional hurdles for non-lethal autonomous weapons systems that could make them more difficult to develop than autonomous weapons systems:

If an NLW [non-lethal autonomous weapons systems] is developed with autonomous functions, it would need to comply with Directive 3000.03E, Instruction 3200.19, and Directive 3000.09. Review for compliance with these

¹¹¹ Future of Life Institute, “An Open Letter to the United Nations Convention on Certain Conventional Weapons,” 21 August 2017, accessed 15 January 2018, <https://futureoflife.org/autonomous-weapons-open-letter-2017/>.

¹¹² “The key to incorporating autonomous and semi-autonomous weapon systems into American defense planning is to ensure that U.S. Government entities are always acting in accordance with international humanitarian law, taking appropriate steps to control proliferation, and working with partners and Allies to develop standards related to the development and use of such weapon systems. The United States has actively participated in ongoing international discussion on Lethal Autonomous Weapon Systems, and anticipates continued robust international discussion of these potential weapon systems. Agencies across the U.S. Government are working to develop a single, government-wide policy, consistent with international humanitarian law, on autonomous and semi-autonomous weapons.” Executive Office of the President. *Preparing for the Future of Artificial Intelligence*, 3.

¹¹³ Joint Chiefs of Staff, *JCRAS*, 16.

policies is in addition to a legal review for compliance with domestic and international law. Thus, Instruction 3200.19 in particular imposes an additional procedure [Human Effects Review Board] which may inhibit the ability to expedite the deployment and development of certain technologies. This may be important to the development of future capabilities because of the desire for capability deployment to keep pace with technology development.¹¹⁴

A tertiary issue is how the Services categorize autonomous systems making it difficult to identify the best procurement model:

DoDI 5000.02 provides models of procurement processes based on whether the capability is hardware-intensive, software-intensive, or an information system, among other categories. Additionally, absent extenuating circumstances, RAS development will have to take into account the regular acquisition timeline, which could impact competitiveness. While RAS development and procurement could potentially bypass certain steps of the process, such as operator safety because there is no operator physically present, such steps would still need to comply with all relevant statutes and consider the tradeoffs between deploying earlier and risking malfunction.¹¹⁵

Acquisition hurdles are addressed in depth later in this chapter but the issue of functional trade space¹¹⁶ raises legal and policy concerns. The extent to which human decision making and intervention are required for autonomous and semi-autonomous weapons systems is based on the stipulation in DoDD 3000.09 to design systems to “allow commanders and operators to exercise appropriate levels of human judgment over the use of force.”¹¹⁷ The level of human oversight, time required to intervene in the

¹¹⁴ John’s Hopkins Applied Physics Laboratory. “NSAD-R-16-045,” 4-29.

¹¹⁵ Ibid., 4-30.

¹¹⁶ See Defense Science Board, *Task Force Report: The Role of Autonomy in DoD Systems*, 27-30 for an in-depth discussion of trade space.

¹¹⁷ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, 2.

event of system failure, and consequences of the unwillingness or inability for human intervention¹¹⁸ are left to the discretion of the command and control authorities.¹¹⁹

Figure 15 provides an overview of the current state of human-machine collaboration. Humans are optimized to perform cognitive and physical work inside of the blue ellipse, work outside is optimized (or only capable of being performed) by machines.¹²⁰ Updating policy to include machine capabilities could allow the DoD to achieve faster, more precise operations, reduce risk and complexity for humans, and conduct operations in environments that were previously beyond human ability.

¹¹⁸ “Another important aspect of the policy is that the distance between a human decision to initiate lethal force and the actual use of force is not defined; rather it is a gray area where there is room for interpretation consistent with commander intentions. This point deserves to be underscored, as many questions related to use of autonomous and semi-autonomous weapons center on the time lapse between the decision by a human to engage a target and actual engagement. The Directive defers to commander intent to determine an acceptable distance in time.” John’s Hopkins Applied Physics Laboratory, “NSAD-R-16-045,” 2-5.

¹¹⁹ “The U.S. priority has been to reiterate that all weapon systems, autonomous or otherwise, must adhere to international humanitarian law, including the principles of distinction and proportionality. For this reason, the United States has consistently noted the importance of the weapons review process in the development and adoption of new weapon systems”. Executive Office of the President, *Preparing for the Future of Artificial Intelligence*, 38.

¹²⁰ “Presently, human cognition is perceived to be superior to autonomous technologies in situations that are complex, ambiguous, and dynamic. We know human beings are very talented at making decisions in closed systems with repeatable data and feedback, including complex games like chess. But our decision-making and cognitive processes can be skewed negatively or produce irrational decisions because of bias, attribution, optimism, framing, and anchoring influences.” F. G. Hoffman, “Exploring War’s Character and Nature: Will War’s Nature Change in the Seventh Military Revolution?” *Parameters* 47, no. 4 (Winter 2017-18): 22.

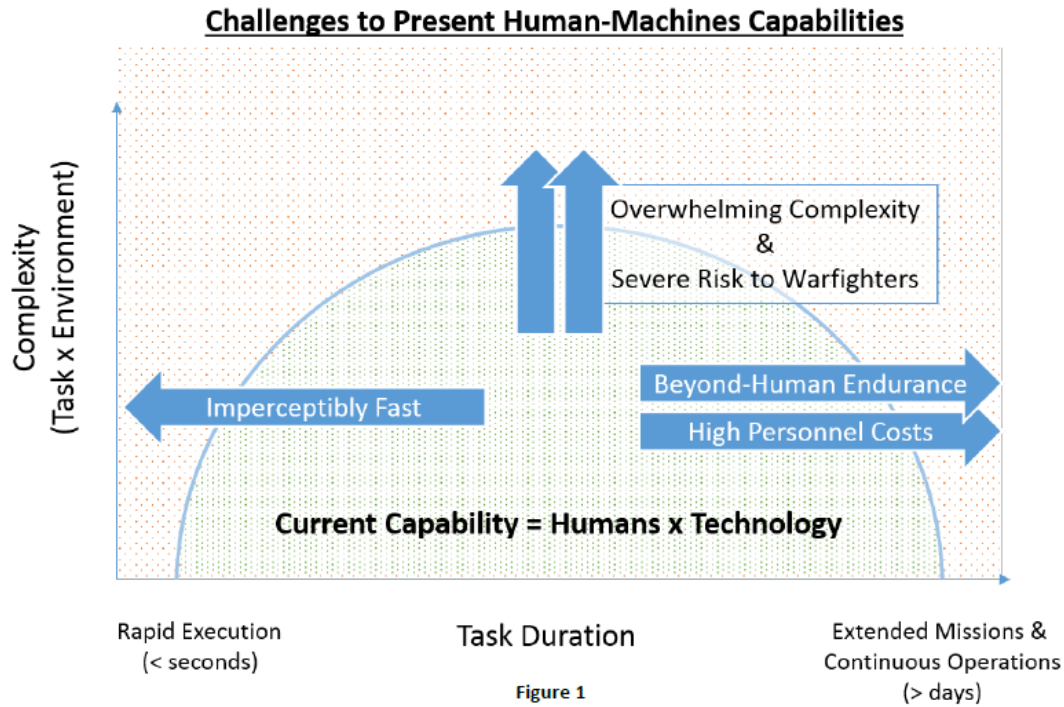


Figure 15. Human versus Machine Optimization Areas

Source: Department of Defense, Research and Engineering, *Technical Assessment: Autonomy* (Washington, DC: Office of Technical Intelligence, February 2015), 5.

Human-machine collaboration should be the resident factor in policy construction.¹²¹ When designing policy, the degree of autonomy granted to RAS to perform a task or goal supporting mission accomplishment should be considered from the perspective of command and control.¹²² JP 1-02 defines Command and Control as

¹²¹ “The greatest advantages of autonomy will come from eliminating the need for mundane tasks and augmenting human decision-making, not replacing it.” Hoffman, “Exploring War’s Character and Nature,” 31.

¹²² “As long as humans are responsible for directing war, for writing code, and for fielding and maintaining machines, warfare will remain an instrument of policy and the province of warriors. Those warriors may have machine augmentation, delegate decisions to cyber assistants, and operate more remotely; but they will be directing the fight.” Hoffman, “Exploring War’s Character and Nature,” 22.

“the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.” It follows that “the level of control used will depend on the nature of the operation or task, the risk or priority of its success, and the associated comfort level of the commander.”¹²³ For RAS “the essence of autonomy is . . . how to retain effective human control over the machine’s behavior and the risks—both the probability and consequences—associated with a loss of control.”¹²⁴ Autonomy as applied to RAS is “the condition or quality of being self-governing to achieve an assigned task based on the system’s own situational awareness, . . . planning, and decision-making . . . [and it] can be tailored for a specific mission, level of risk, and degree of human-machine teaming.”¹²⁵ Figure 16 shows an example of how the USAF envisions delegating autonomy to machines during specific missions as part of human-machine collaboration.

¹²³ Joint Chiefs of Staff, Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Government Printing Office, March 2013), V-14.

¹²⁴ Paul Scharre, “Autonomous Weapons and Operational Risk” (Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016), 3.

¹²⁵ Joint Chiefs of Staff, *JCRAS*, 3.

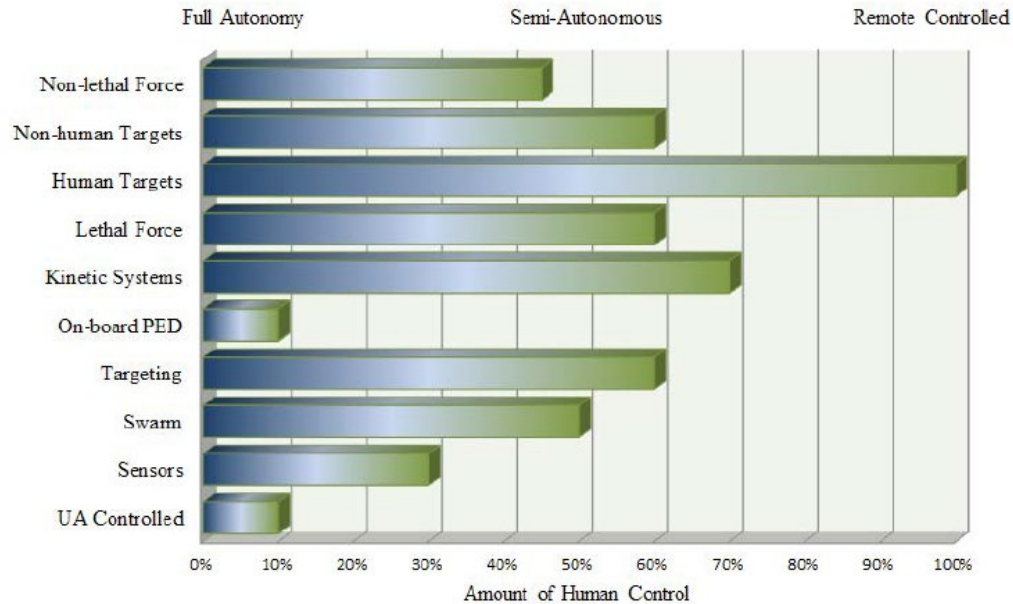


Figure 16. USAF Vision of Human-Machine Collaboration for UAS

Source: United States Air Force, *Small Unmanned Aircraft Systems Flight Plan 2016-2036: Bridging the Gap Between Tactical and Strategic* (Washington, DC: Government Printing Office, April 2016), 16. Note: USAF example of sliding scale for autonomy that delineates human level of control over machines by function.

The abilities to predict behavior and undertake corrective actions are critical to maintaining effective control. Controls for RAS should be developed similar to those for humans based on skills, roles, timelines, and capabilities so that they can operate as predictable teammates with humans ultimately responsible for mission accomplishment. Policy should define the roles and tasks that machines can perform in support of cognitive and physical human-machine collaboration while allowing Commanders and operators the ability to develop flexible controls to mitigate risk.

In summary, misinterpretation or misunderstanding of the relatively ambiguous and complex DoD policy regarding the autonomous and semi-autonomous systems leaves both the public and the DoD confused. The lack of defined roles for humans and

machines in lethal engagements raises trade space concerns for capability developers. The overarching contention on defining autonomy and the tenuousness of the Senior Leader Review process makes it unappetizing for the Services and industry to develop autonomous weapons systems in an era of decreasing government R&D funding.¹²⁶

Gap 2: Doctrine

As discussed in the literature review, the DoD does not have a published definition for autonomy or a conceptual framework resident with a taxonomy that describes the interaction between humans and machines.¹²⁷ The concepts and terms that are used by the Services are not the same as those used within the private sector, issuances or directives, or Joint operating concepts. Because of this disparity and resulting gap, the author's analysis focuses on why the DoD should adopt the definition and concept of autonomous functioning in a system in policy and guidance to the Services.

The DoD and Services currently use various terms to define human-machine collaboration. These range from “loop” based terms to flexible autonomy, supervised autonomy, and levels of automation. These terms arise because of a lack of understanding within the DoD of what AI is and how it enables autonomy. Figure 17 shows a basic

¹²⁶ “Recent analysis suggests that the socially optimal level of R&D investment—the amount that would produce the greatest rate of economic growth—is two to four times greater than actual spending” Furman, “Is This Time Different? The Opportunities and Challenges of Artificial Intelligence,” 10.

¹²⁷ The DoD dictionary does contain an entry for “autonomous operations”: In air defense, the mode of operation assumed by a unit after it has lost all communications with higher echelons forcing the unit commander to assume full responsibility for control of weapons and engagement of hostile targets. Department of Defense, *Dictionary of Military and Associated Terms*, 24.

overview of how systems utilize AI within a complex system like the “internet of things”.

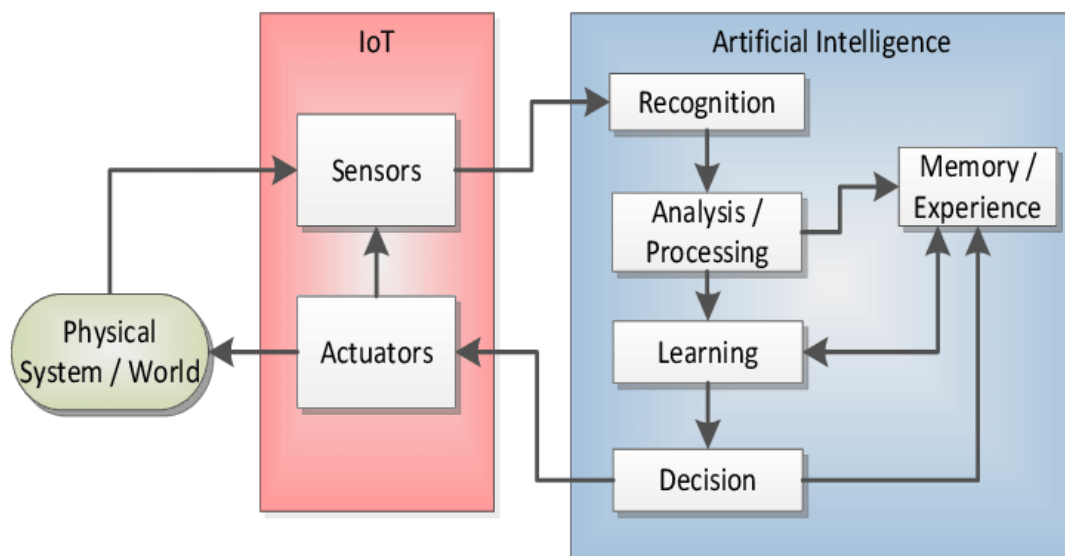


Figure 17. Basic Overview of AI Functions within a System

Source: Jovan Ivković and Jelena Ivković, “Analysis of the Performance of the New Generation of 32-bit Microcontrollers for IoT and Big Data Application” (7th International Conference on Information Society and Technology, Kopaonik, Serbia, 2017), accessed 29 March 2018, https://www.researchgate.net/figure/An-expanded-concept-of-autonomous-AI-enabled-IoT-CPS-system-based-on-the-new-ARM_fig2_316173015.

To support further analysis of how AI enables autonomy let us re-examine the difference between automation and autonomy. A simple way to understand the difference is that automation is the ability to predict how systems function based on rules. Autonomy is how a system functions based on goals, outcome should be predictable but how the system achieves goals may not be. Good definitions for these terms can be found in the DoD Research and Engineering Autonomy Community of

Interest Test and Evaluation, Verification and Validation Working Group which established the following definitions in 2011:

Automation: The system functions with no/little human operator involvement; however, the system performance is limited to the specific actions it has been designed to do. Typically these are well-defined tasks that have predetermined responses (i.e., simple rule-based responses).

Autonomy: The system has a set of intelligence-based capabilities that allows it to respond to situations that were not pre-programmed or anticipated (i.e., decision-based responses) prior to system deployment. Autonomous systems have a degree of self-government and self-directed behavior (with the human's proxy for decisions).¹²⁸

Since the terms automation and autonomy are often used interchangeably or without consideration of their innate differences it becomes difficult to understand when a system transitions from being automated to being autonomous. To provide context, the development of algorithms in the 1970s followed by the advent of deep learning enabled machine perception. Machine learning led to the development of narrow AI which supported cognition and robotic action in very specifically defined tasks. Artificial general intelligence (AGI) is still being developed to enable machine perception, cognition, and action in ways that replicate human intellect. Narrow AI currently enables machine autonomy in specific domains within specific skill sets. A recent bill introduced to Congress differentiates between general and narrow AI as follows:

Artificial General Intelligence. A notional future artificial intelligence system that exhibits apparently intelligent behavior at least as advanced as a person across the range of cognitive, emotional, and social behaviors.

¹²⁸ Department of Defense Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group, *Technology Investment Strategy 2015 to 2018* (Washington, DC: Department of Defense, May 2015), 5.

Narrow Artificial Intelligence. An artificial intelligence system that addresses specific application areas such as playing strategic games, language translation, self-driving vehicles, and image recognition.¹²⁹

Figure 18 is a visual representation of how AI enables autonomy. There are various definitions for the terms contained in this diagram, abbreviated definitions different from the ones previously presented are used here for simplicity.

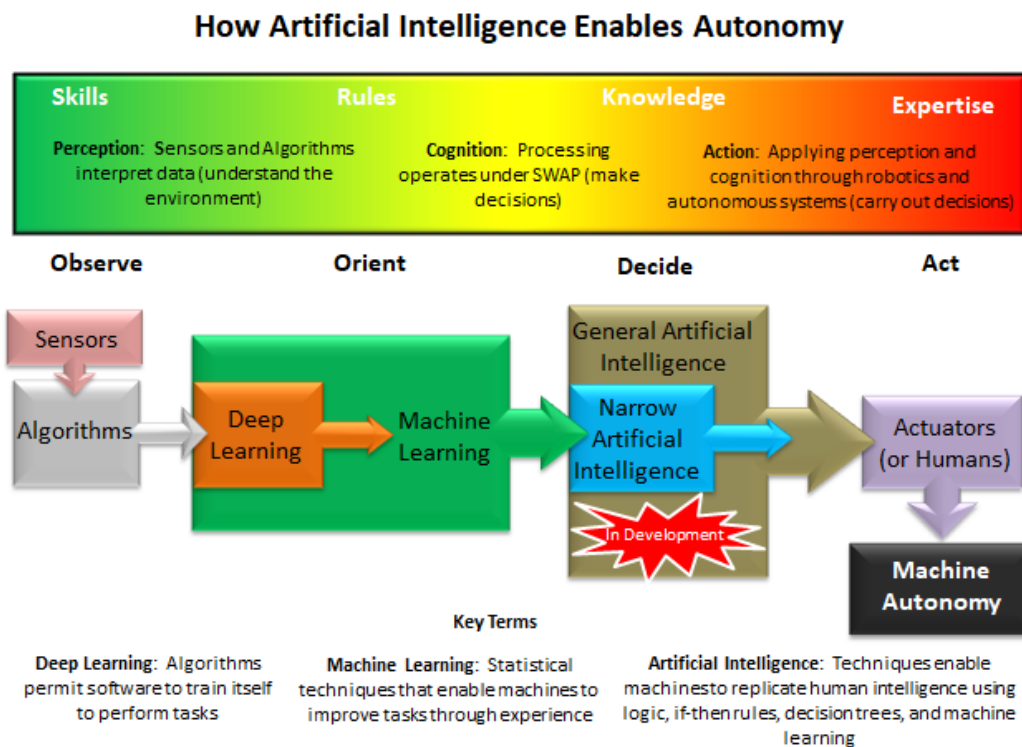


Figure 18. How Artificial Intelligence Enables Autonomy

Source: Created by author. Diagram construction was based on general knowledge and accepted terms from the private sector. Of note, this is one basic example of how AI enables autonomy, there is a vast variety of different combinations of neural networks, learning techniques, and models that could enable autonomy. The author recommends reading “Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD” produced by the MITRE Corporation in January 2017 for further DoD specific information on this topic.

¹²⁹ U.S. Congress, House, Future of Artificial Intelligence Act of 2017, 115th Cong., 1st Sess., H.R. 4625, 2017, accessed 15 March 2018, <https://www.congress.gov/bill/115th-congress/house-bill/4625/text>, 3-5.

While the aspects of perception, cognition, and action are used to describe the increasing steps toward autonomy in the Figure 18, there are many additional terms resident within a taxonomy for autonomy. In 2016, the DoD DSB conducted a summer study on autonomy that updated the work from the 2012 review of autonomous systems based on rapidly increasing development of AI. This update included descriptions and graphic examples of “human in-the-loop” and “human on-the-loop”, concepts widely used within the private sector and espoused by the Services in their concepts (not defined in these terms in DoDD 3000.09 or the JCRAS). The loop concept is based on an updated view of Boyd’s observe, orient, decide, act loop in which sense, think, decide, act, and team functions are ascribed to humans or machines depending on mission variables.¹³⁰ Figure 19 shows a graphic depiction of this concept which is basically defined using the terms “semi-autonomous, human supervised, and autonomous weapons system” in DoDD 3000.09.

¹³⁰ Defense Science Board, *Summer Study on Autonomy*, 9, 19.

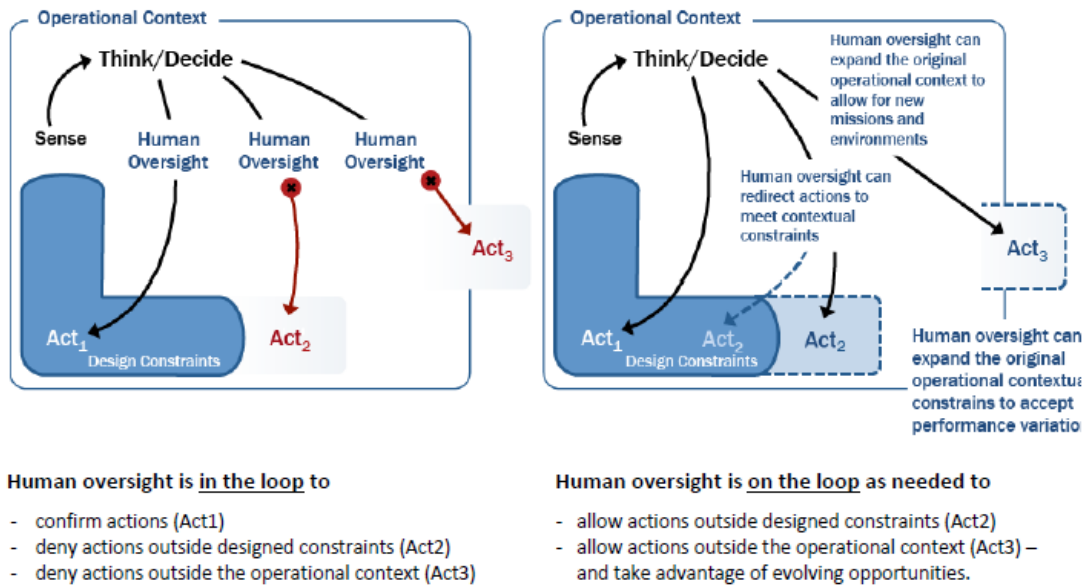


Figure 19. Human-in-the-Loop versus Human-on-the-Loop

Source: Defense Science Board, *Summer Study on Autonomy* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, June 2016), 19.

The primary policy document within the DoD that defines terminology related to autonomous systems is DoDD 3000.09.¹³¹ Taken in the context of figure 19, the definitions from DoDD 3000.09 for semi-autonomous weapons systems would be human in-the-loop, human supervised autonomous weapons systems would be human on-the-loop, and autonomous weapons systems would be human out-of-the-loop.

¹³¹ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, 13-14.

Table 7. Comparing Terminology

Semi-Autonomous <i>"Human <u>in</u> the Loop"</i>	Human-Supervised <i>"Human <u>on</u> the Loop"</i>	Autonomous <i>"Human <u>out</u> of the Loop"</i>
A weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator. Includes "fire and forget" munitions	An autonomous weapon system that is designed to provide human operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur	A weapon system that, once activated, can select and engage targets without further intervention by a human operator.

Source: Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies* (Arlington, VA: Center for Naval Analyses, January 2017), 146.

Each of the Service's future operating concept documents use "loop" terms versus those used in DoDD 3000.09. The JCRAS does not use either set of terms instead using "flexible autonomy". The lack of consistently used terminology makes it difficult to define human-machine collaboration within policy.

A thorough analysis of policy and concepts leads to the conclusion that the DoD is pursuing a policy of "Centaur teaming". The concept of "Centaur teaming" is an alternate view of human-machine collaboration different from the frameworks discussed above. Autonomy expert Paul Scharre explains that rather than try to engineer out human error through minimizing human input, autonomous capabilities should be designed based around the humans:¹³²

¹³² Sydney J. Freedberg, "Artificial Stupidity: When Artificial Intelligence + Human = Disaster,," *Breaking Defense*, 2 June 2017, 3, accessed 15 December 2017, <https://breakingdefense.com/2017/06/artificial-stupidity-when-artificial-intel-human-disaster/>.

Human decision-making and automation are not mutually exclusive, however. “Centaur” human-machine teaming cognitive architectures can leverage the predictability, reliability, and speed of automation while retaining the robustness and flexibility of human intelligence. Whenever possible, human-machine teaming will be preferred.¹³³

Scharre envisions autonomy as having multiple dimensions that offer options for how humans physically and cognitively interact with machines. He describes the three roles that humans currently perform as part of a semi-autonomous weapons system with the supposition that while it may be easy to automate the human out of the essential operator role it will be far more difficult for machines to assume the other roles based on trust.

The human as essential operator: The weapon system cannot accurately and effectively complete engagements without the human operator.

The human as moral agent: The human operator makes value-based judgments about whether the use of force is appropriate—for example, whether the military necessity of destroying a particular target in a particular situation outweighs the potential collateral damage.

The human as fail-safe: The human operator has the ability to intervene and alter or halt the weapon system’s operation if the weapon begins to fail or if circumstances change such that the engagement is no longer appropriate.¹³⁴

Narrow AI does not generally support machine capability to assume the roles of moral agent and fail safe but the development of AGI would. The question remains if robotically augmenting humans versus designing more intelligent machines is inherently a win-lose conflict that will result in humans being engineered off of the battlefield. Paul Scharre does not think it is an “either-or” conflict but rather that system design will evolve based around the strengths of both man and machine: “No—humans vs.

¹³³ Scharre, “Autonomous Weapons and Operational Risk,” 6.

¹³⁴ Ibid., 41.

machines is a false choice. The best systems will combine human and machine intelligence to create hybrid cognitive architectures that leverage the advantages of each.”¹³⁵

The problem is more than philosophical. The predominate engineering stance in the past has been to automate as much as possible and minimize human interaction to increase system reliability.¹³⁶ This reduces ambiguity in the design space by making machines more predictable but it also results over and under reliance on machines leading to lack of trust in the system when they fail to operate as advertised:¹³⁷

Most engineers and computer scientists have little to no training in human interaction with complex systems and don’t know how to address the inherent variability that accompanies all human performance. Thus, they desire a set of rules and criteria that reduce the ambiguity in the design space, which for them typically means reducing the role of humans or at least constraining human behavior.¹³⁸

Automation based development has resulted in autonomy generally being described in a series of ordinal levels which increasingly focus on engineering physical

¹³⁵ Ibid., 39.

¹³⁶ Cummings, “Man vs. Machine or Man + Machine,” 62.

¹³⁷ “Because autonomous systems in many cases do not have real-time human supervision, maintaining *effective control* over the system has two components: (1) The ability of the human operator to accurately predict the autonomous system’s behavior in the environment in which it is being used. This includes its limitations and the conditions under which it will fail. This allows the human operator to employ the autonomous system only in situations where it will perform appropriately. (2) The ability of the human operator to undertake corrective action if/when the autonomous system fails to behave in accordance with the human operator’s intentions.” Scharre, “Autonomous Weapons and Operational Risk,” 8.

¹³⁸ Mary (Missy) Cummings, “Man vs. Machine or Man + Machine,” *IEEE Intelligent Systems* 29, no. 5 (September/October 2014): 62, accessed 26 February 2018, www.computer.org/intelligent.

and cognitive work away from humans so that they can focus on tasks requiring expertise, ethical decision making, morality, and social interaction. The DoD views increasing automation as a way to reduce risk and achieve overmatch in complex environments. The DoD should also consider the perspective of “how can humans and machines work together to achieve goals resulting in enhanced perception, cognition, and action to achieve overmatch?” Using the framework of autonomous functioning within a system, the DoD could then define physical and cognitive work and roles for humans and machines in ways that retain human expertise and complement the strengths of both sides.¹³⁹ The DoD can create highly autonomous systems today that perform certain tasks as well as or better than humans alone could but it is nowhere near replicating systems that can broadly observe, think, decide, and act in a way similar to how humans adapt to changes in the environment.¹⁴⁰ For this reason, the DoD should not look at limiting the development of autonomous systems which may actually be smarter, faster, and simply better at physical and cognitive work than humans, but rather it should define capabilities and policy in terms that support human-machine augmentation and collaboration.¹⁴¹

¹³⁹ “Enhancement of co-robot capabilities: Exploit the advantages of both humans and machines for better and faster human decision making; help humans perform better in combat; and employ innovative cooperative operations between manned and unmanned platforms.” The Networking and Information Technology Research and Development Program, “Supplement to the President’s Budget for Fiscal Year 2018,” 59.

¹⁴⁰ “The role of educated humans will begin to concentrate on the higher cognitive tasks of processes such as mission analysis, operational planning, and assessments.” Hoffman, “Exploring War’s Character and Nature,” 22.

¹⁴¹ “Artificial intelligence and computer support are not necessary to remove human judgment at any or all levels of warfare decisions, but may be used simply to

Gap 3: Leadership

DoD leadership is responsible for developing a culture that understands, trusts, and accepts machine ability to augment, enable, and team with humans to accomplish missions. The ability for machines to effectively communicate requirements, anticipate responses, cross check work, and intervene if required should be planned and assessed in the same way that human teams interact today. Trust between team members is the foundation of teamwork:

The issue of trust is core to DoD's success in broader adoption of autonomy. On the one hand, an autonomous system must be designed to operate in a trustworthy fashion with respect to the missions for which it was designed. On the other hand, an autonomous system must be designed so that humans (and/or machines) can straightforwardly determine whether, once it has been deployed, it is operating reliably and within its envelope of competence—and, if not, that appropriate action can be taken.¹⁴²

The DoD must begin to cultivate trust in RAS through a cultural change.

Avenues that DoD could pursue include:

1. Conceptualize support for Centaur teams through DOTMLPF-P to create a culture of trust in RAS
2. Redefine Soldiers worth and identity based on mission accomplishment rather than what they fly, drive, and operate
3. Conduct a study to confirm the effectiveness of RAS particularly the assumptions of increasing reliability, predictability, flexibility, and robustness

improve the efficacy of human judgement. Such technology could be used to eliminate wasted human cognitive capacity on mundane tasks . . . Thus, decision-making in the age of autonomy will rely upon human-machine teaming.” Hoffman, “Exploring War’s Character and Nature,” 27.

¹⁴² Defense Science Board, *Summer Study on Autonomy*, 1

of human-machine collaboration. The DoD should also develop metrics to measure the performance of RAS beyond simply tracking the failure rate of systems and components.

Many people view autonomy as a threat to their jobs based on economic data in government reports or mistrust it because they don't understand it and think systems are unpredictable. "For autonomous systems, the goal should not be to establish certainty of the system's behavior in all situations, but to build trust that it will act reasonably, will have certain limits on inappropriate behavior, and will fail relatively predictably."¹⁴³ Training and leadership education must address both the challenges and capabilities that Centaur teams bring to the fight within the context that every military specialty will become enabled or augmented by RAS over the coming decades. Rather than designing machines to function independently and replace humans on the battlefield, the DoD should focus on developing machines that can operate interdependently with humans to achieve goals through teamwork.¹⁴⁴

Gap 4: Material

Addressing Acquisition Challenges

Analyzing how the DoD will "deliver performance at the speed of relevance"¹⁴⁵ while modernizing, innovating, and growing the force, it is obvious that funding will

¹⁴³ Department of Defense, Research and Engineering, *Technical Assessment: Autonomy* (Washington, DC: Office of Technical Intelligence, February 2015), 19.

¹⁴⁴ Bradshaw et al., "The Seven Deadly Myths of Autonomous Systems," 8.

¹⁴⁵ Department of Defense, "Remarks by Secretary Mattis on the National Defense Strategy," 10.

determine capabilities and constraints. Unlike the developmental periods for previous offset strategies, overarching funding for the DoD today is relatively constrained making it nearly impossible for the DoD to simultaneously achieve all of these lines of effort. As shown in figure 20 the DoD current and projected budget remains near historic lows as a historic percentage of GDP.

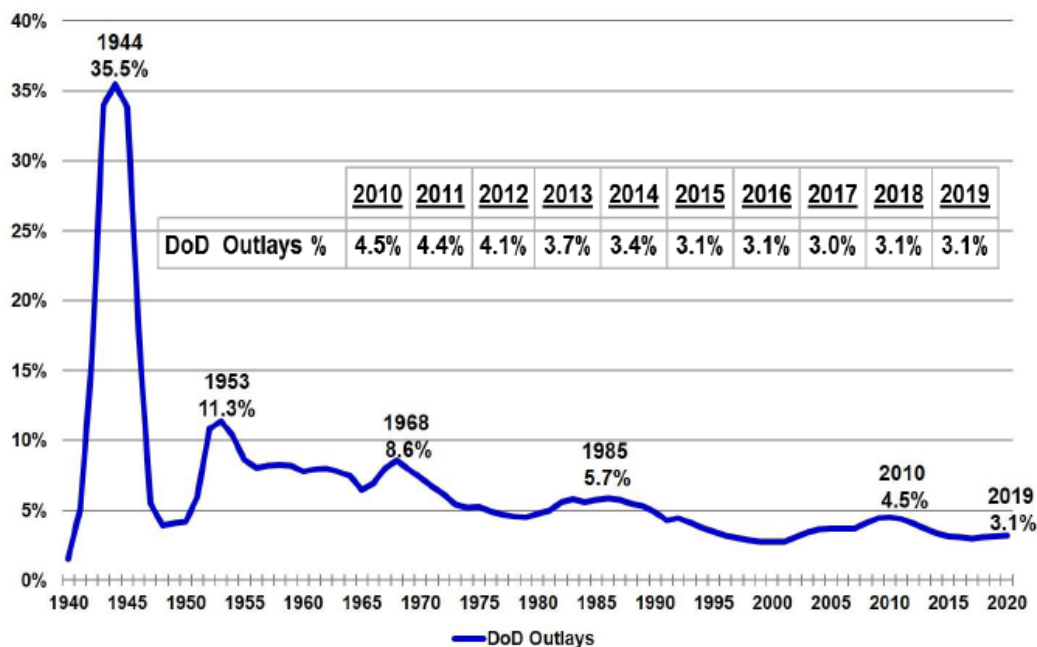


Figure 20. Defense Outlays versus Gross Domestic Product FY 1940–FY 2023

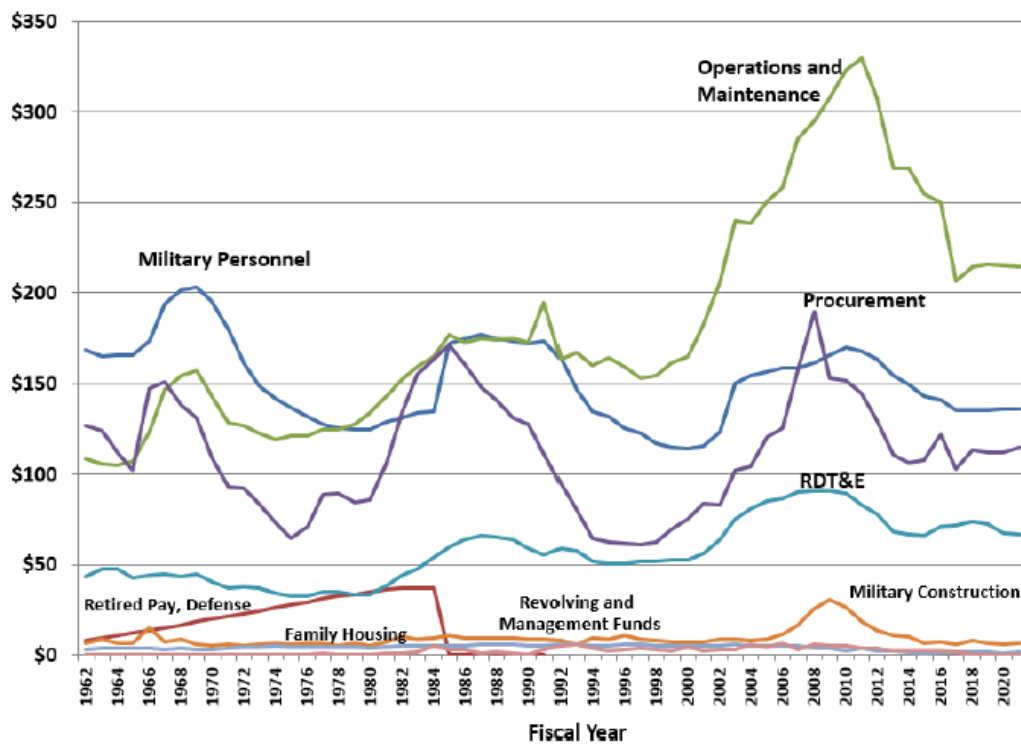
Source: “The President’s FY 2019 budget request is for \$686.1 billion. This budget represents 5 percent real growth over the initial FY 2018 President’s Budget and 10 percent real growth over the current Continuing Resolution (CR). While reversing a 7-year decline, defense spending remains near historical lows as a share of the U.S. economy.” Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*, February 2018, 1-2, accessed 26 March 2018, <https://www.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf>.

A historical overview of the DoD budget by category is presented in figure 21. While this chart does not take into account the recent budgetary increase authorized under the FY 2018 National Defense Authorization Act,¹⁴⁶ the historic precedent for spending on acquisition and Research, Development, Testing and Evaluation (RDT&E) during the development of the first and second offset strategies provides a precedent for how much the DoD may allocate to acquisition during the current period.¹⁴⁷ Declining funding for procurement and RDT&E since 2010 has created significant modernization hurdles as well as technology gaps.

¹⁴⁶ Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*, February 2018, A-2, accessed 26 March 2018, <https://www.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf>.

¹⁴⁷ “Just as it took well over a decade to fled the “assault breaker” technology envisioned in the mid-1970s, the GSS network would not attain an initial operational capability until the mid-2020s, at best, but only if focused R&D begins now and the Pentagon, White House, and Capitol Hill stay the course over at least the next decade. Given the finite and likely declining resources for defense, the nation can neither afford to continue the current “business as usual” approach to power projection, nor plan on having the resources and time to rectify the many operational and strategic problems with the current path once they manifest” – Martinage, Robert. *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability*. Center for Strategic and Budgetary Assessments (2014), Vii-VIII

Figure 1-4. DoD Funding by Budget Accounts: Historical and PB 2017 (FY 1962–FY 2021)
BY17\$, B

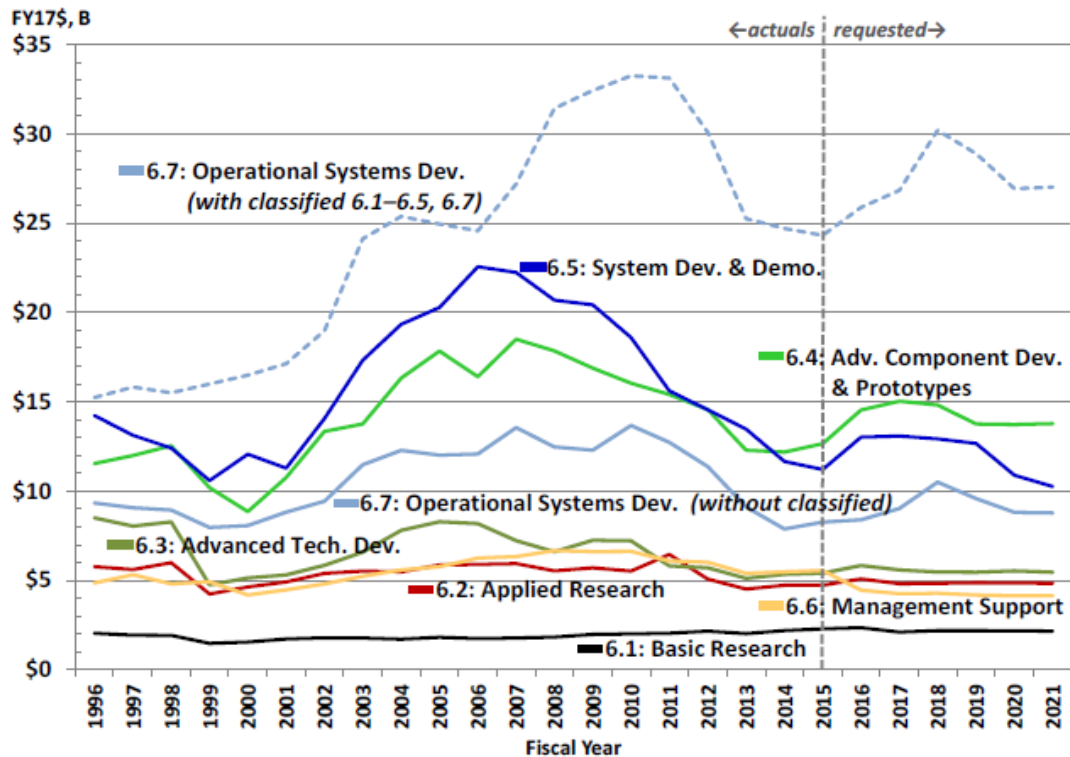


NOTE: OCO is shown in fiscal year actual budgets up through FY 2017. Budget amounts are adjusted for inflation and reported in billions of CY 2017 dollars (CY17\$B).

Figure 21. Historical DoD Budget by Category

Source: Under Secretary of Defense, Acquisition, Technology, and Logistics, *Performance of the Defense Acquisition System: 2016 Annual Report* (Washington, DC: Department of Defense, 2016), 13.

The overarching RDT&E funding decrease that began in 2008 is depicted in figure 22 broken out by field. While research for classified programs is expected to increase, funding for all other fields are expected to decline. The FY 2018 and 2019 DoD budgets increase overall funding for RDT&E but not proportionally nor at the expense of current capabilities as discussed below.



NOTE: Levels before FY 2016 are actual appropriations as reported in DoD Comptroller R1 exhibits; their totals closely match the RDT&E totals in the Comptroller's Green Book (USD(C), 2016c). OCO is shown in FY budgets up to FY 2017. Budget amounts are adjusted for inflation and reported in billions of FY 2017 dollars (FY17\$B). The blue dashed line reflects the published total 6.7 budget, which includes total classified BA 6.1–6.5 and 6.7. The solid line is BA 6.7 minus published totals for classified programs included in BA 6.7 reports (i.e., without the distorting effects of the classified totals).

Figure 22. Recent and Projected RDT&E Funding as of PB 2017

Source: Under Secretary of Defense, Acquisition, Technology, and Logistics, *Performance of the Defense Acquisition System: 2016 Annual Report* (Washington, DC: Department of Defense, 2016), 5. “Here the science and technology BAs (6.1–6.3) are relatively flat or returned to their pre-2001 levels. Accounts for Advanced Component Development and Prototypes (BA 6.4) and Operational Systems Development (BA 6.7, for existing systems) are projected to come down from their peak but remain higher than the levels in the 1990s. The System Development and Demonstration (BA 6.5) budget for new systems in the DoD’s product “pipeline” is projected to decline to its lowest level in this time period. While BA 6.4 and 6.7 levels are not coming down as far, the low levels of BA 6.5 funding reinforce the DoD’s concerns that we risk losing technological superiority in multiple operational domains.”

As shown in figure 23 the DoD is challenged to balance its need to fund current readiness with future capability needs.¹⁴⁸ As with past offset strategies, a mix of high and low end capabilities will be required to provide responsive and scalable deterrence supporting power projection in multiple theaters.¹⁴⁹ This requires the DoD to balance maintaining its current state of readiness and modernize existing equipment while increasing funding for the development of future concepts.

¹⁴⁸ During Eisenhower’s “First Look” between 1954-1957 USAF appropriations increased to 47 percent of the DoD budget while the USN, USMC and USA shrank dramatically (the Army budget was reduced by 40 percent by 1964). “Between 1954-1961 military expenditures as a percentage of the federal budget fell from 66 to 49 percent.” Under Secretary of Defense, Acquisition, Technology, and Logistics, *Performance of the Defense Acquisition System: 2016 Annual Report* (Washington, DC: Department of Defense, 2016), 11-12.

¹⁴⁹ “Given the political and diplomatic challenges associated with those initiatives, however, DoD will likely also need to reduce force structure and scale back modernization plans for legacy forces that contribute primarily to operations in low-to-medium threat environments. While that necessarily means accepting increased risk for some contingencies, it is imperative to rectify the current imbalance between forces able to operate in permissive and non-permissive environments.” Robert Martinage, “Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability” (Research, Center for Strategic and Budgetary Assessments, Washington, DC, 2014), 69.

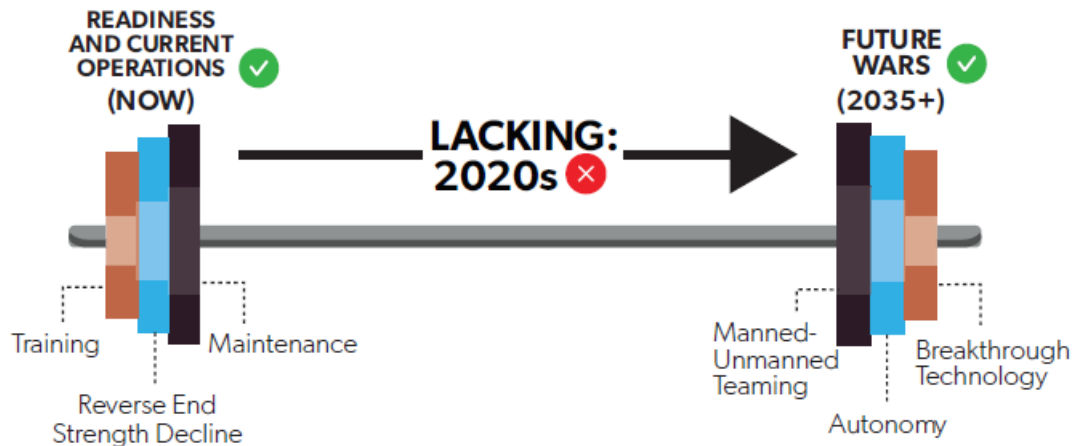


Figure 23. Building Blocks of Future Capability

Source: Mackenzie T. Eaglen, “Repair and Rebuild: Balancing New Military Spending for a Three Theater Strategy” (Research, American Enterprise Institute, Washington, DC, October 2017), 7.

Based on the FY 2019 budget request, it does not appear that the DoD is willing to exchange current capability for future requirements development. The entire DoD budget for S&T is less than the cost of four Virginia Class submarines; while the DoD total budget increased 5 percent from FY 2018, the S&T budget only increased .5 percent as shown in table 8.¹⁵⁰

¹⁵⁰ The FY 2019 DoD budget prices the cost of two Virginia Class submarines at \$7.4 billion dollars, FY 2019 DoD budget, Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*, 3-3.

Table 8. DoD S&T Budget including Base and OCO

Figure 3.4. Science & Technology Program Base and OCO budget (\$ in billions)

Program	FY 2017 Enacted	FY 2018 Request*	FY 2019 Request**	FY18–FY19 Change
Basic Research (6.1)	2.2	2.2	2.3	0.1
Applied Research (6.2)	5.1	5.0	5.1	0.1
Adv Tech Dev (6.3)	6.1	6.0	6.3	0.3
Total S&T	13.4	13.2	13.7	0.5

*FY 2018 reflects the President's Budget request +\$17.0 million Emergency Amendment: Missile Defeat and Defense Enhancements Appropriations Act of 2018 (Division B, Public Law 115-96); and includes \$25.0 million OCO funds within the Defense-Wide S&T

**FY 2019 reflects the President's Budget request, includes \$38.6 million of OCO funds within the Defense-Wide S&T

Source: Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*, February 2018, 3-12, accessed 26 March 2018, <https://www.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf>. Note: The FY 2019 DoD budget prices the cost of two Virginia Class submarines at \$7.4 billion dollars, FY 2019 DoD budget.

The decision to allocate funding away from S&T and RDT&E is not endemic to the DoD alone. Budget cuts and changed strategic priorities have resulted in all Federal Agencies dramatically reducing their R&D budgets over the last few years as shown in figure 24.

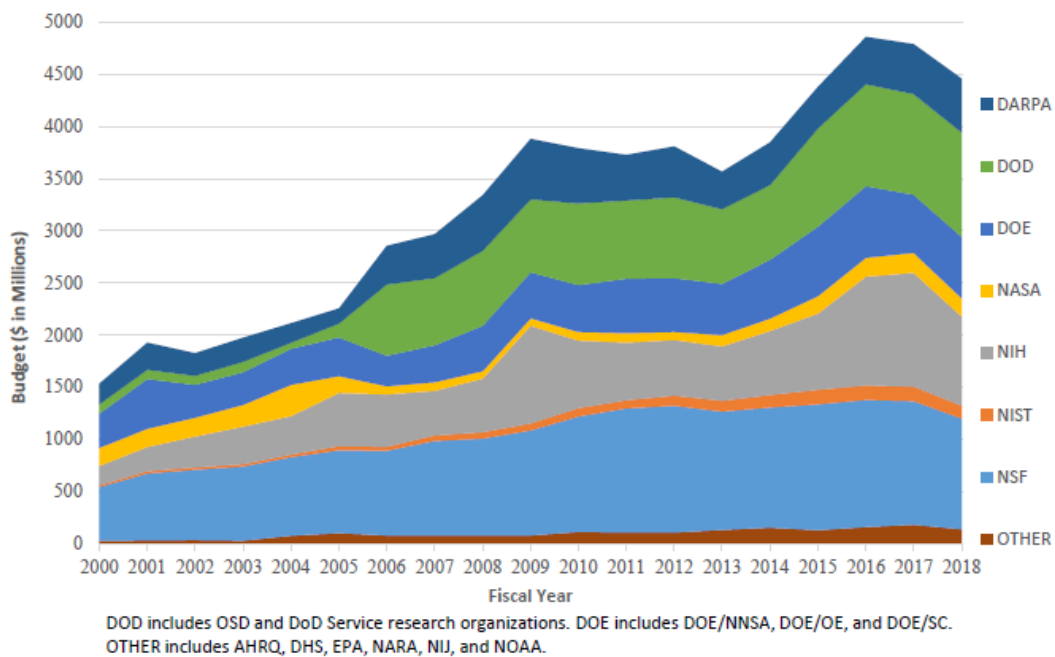


Figure 24. NITRD Budget Trends 2000-2018 by Agency

Source: Executive Office of the President, *Preparing for the Future of Artificial Intelligence* (Washington, DC: The White House, October 2016), 10.

The lack of overarching government emphasis on S&T and R&D stems from the NSS intent for the NSIB to generally fund and lead development. “There are multiple Silicon Valley and Chinese companies who each spend more annually on AI R&D than the entire United States government does on R&D for all of mathematics and computer science combined.”¹⁵¹ The NSS addresses the need to promote and protect the US NSIB but as shown in figure 24 overarching government support for this area is declining in comparison to how peer competitors are growing actively and purposefully growing their NSIBs:

¹⁵¹ Allen and Chan, “Artificial Intelligence and National Security,” 52.

Protecting the NSIB requires a domestic and international response beyond the scope of any individual company, industry, university, or government agency. The landscape of innovation does not divide neatly into sectors. Technologies that are part of most weapon systems often originate in diverse businesses as well as in universities and colleges. Losing our innovation and technological edge would have far-reaching negative implications for American prosperity and power.¹⁵²

The NSS states the intent to leverage the NSIB for technology development and funding in an effort to “lead in research, technology, invention, and innovation”:

Leverage Private Capital and Expertise to Build and Innovate: The U.S. Government will use private sector technical expertise and R&D capabilities more effectively. Private industry owns many of the technologies that the government relies upon for critical national security missions. The Department of Defense and other agencies will establish strategic partnerships with U.S. companies to help align private sector R&D resources to priority national security applications.¹⁵³

There are multiple reasons besides funding constraints for the DoD to work more closely with the private sector. For example, “technologies that are part of most weapon systems often originate in diverse businesses as well as in universities and colleges.”¹⁵⁴ There are however many bureaucratic hurdles to these types of strategic partnerships between government and the private sector. The NSS addresses the overarching issue as follows with notable guidance on experimentation, prototyping, and commercial-off-the-shelf (COTS) solutions:

We must eliminate bureaucratic impediments to innovation and embrace less expensive and time-intensive commercial off-the-shelf solutions. Departments and agencies must work with industry to experiment, prototype, and rapidly field new capabilities that can be easily upgraded as new technologies come online. . .

¹⁵² Office of the President of the United States, *The National Security Strategy of the United States of America*, 21.

¹⁵³ Ibid., 20.

¹⁵⁴ Ibid., 21.

. The United States will pursue new approaches to acquisition to make better deals on behalf of the American people that avoid cost overruns, eliminate bloated bureaucracies, and stop unnecessary delays so that we can put the right equipment into the hands of our forces. We must harness innovative technologies that are being developed outside of the traditional defense industrial base.¹⁵⁵

The specific direction in strategic guidance to utilize COTS is a result of the technology gap that was created through lack of government funding for S&T and R&D during counterinsurgency focused operations. The last decade of war in Iraq and Afghanistan resulted in the overuse of the RAP to field items as quickly as possible to forces resulting in sub-optimal system performance and an overreliance on contractors and commercial items. While some systems became programs of record, the rapid nature of the fielding resulted in long term issues with training, sustainment, and operations that have yet to be addressed today.¹⁵⁶ The DoD is now focusing on the inherent vulnerabilities associated with commercial items while simultaneously finding that it must rely on them within the near term. Commercial items are often the only option available to meet requirements due to component manufacture regulations, proprietary systems, and foreign market takeover of certain components.

The 2016 Performance Review of the DAS explains limitations and anticipated performance of commercial items and systems:

Commercial items. COTS and NDI usually (or even “only”) work for defense systems when the requirements, usage, and environments match exactly. This results in fairly low appropriateness at the system level (where functions, requirements, and “-ilities” often differ) but increasing appropriateness at part levels.

¹⁵⁵ Office of the President of the United States, *The National Security Strategy of the United States of America*, 29.

¹⁵⁶ Lewis, *Insights for the Third Offset*, 15.

Limitations of rapidly acquired systems. Because rapidly acquired systems are based on readily available and often commercial components, they share many of the COTS/NDI issues above. Also, they are often difficult and costly to sustain in the long term, difficult to convert to a regular program of record, and are often effective against only a narrow range of threats.¹⁵⁷

The suitability and reliability issues mentioned above are further compounded by obsolescence¹⁵⁸ and software development and integration specifically for IT.¹⁵⁹ With COTS, IT is all too often obsolete before the equipment is even fielded to the end user and supply chains are vulnerable to security threats (specifically cyber). Between proprietary limitations from “vendor lock” and the inability to upgrade or replace components that pose security risks, acquisition professionals are unable to adequately address security concerns. This is further compounded by the length of the various processes within the DAS which hinder the ability of Program Executive Offices to conduct “agile” acquisition to address security concerns as they arise. In the 2016 “Performance of the DAS” report, PEO’s raised concerns with many factors hampering agile acquisition including the length of the requirements, funding, and cycles,

¹⁵⁷ Under Secretary of Defense, Acquisition, Technology, and Logistics, *Performance of the Defense Acquisition System: 2016 Annual Report* (Washington, DC: Department of Defense, 2016), 117.

¹⁵⁸ “For some longer programs, upgrades may even be required before initial fielding. Replacements, lifetime buys, and upgrades must be built into strategies, budgets, and staffing plans throughout the life cycle, but some statutory fiscal rules can limit flexibility and options that save money in the end.” Under Secretary of Defense, Acquisition, Technology, and Logistics, *Performance of the Defense Acquisition System: 2016 Annual Report*, 117.

¹⁵⁹ The DoD continues to find that giving prime contractors responsibility for major software block upgrades is risky

disincentives for pursuing risk in acquisition, and component upgrades based on changing technology and threat.¹⁶⁰

The concerns expressed by the PEOs are directly related to the way that requirements are generated and tested. The development of measurable, testable, requirements based on the functional components within a system-of-systems is critical to retaining US technological advantage. The Standard “V” diagram in figure 25 shows the programmatic development cycle currently used within the DAS. This is not a viable model for developing and testing requirements for AI and autonomy because: “The addition of autonomy will require that much of the effort traditionally reserved for final DT and OT of a new system must be shifted to the left, with the majority of the T&E activities taking place before the completed system is assembled at test ranges for final system level DT and OT.”¹⁶¹

¹⁶⁰ Under Secretary of Defense, Acquisition, Technology, and Logistics, *Performance of the Defense Acquisition System: 2016 Annual Report*, 118.

¹⁶¹ Department of Defense, Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group *Technology Investment Strategy 2015 to 2018*, 8.

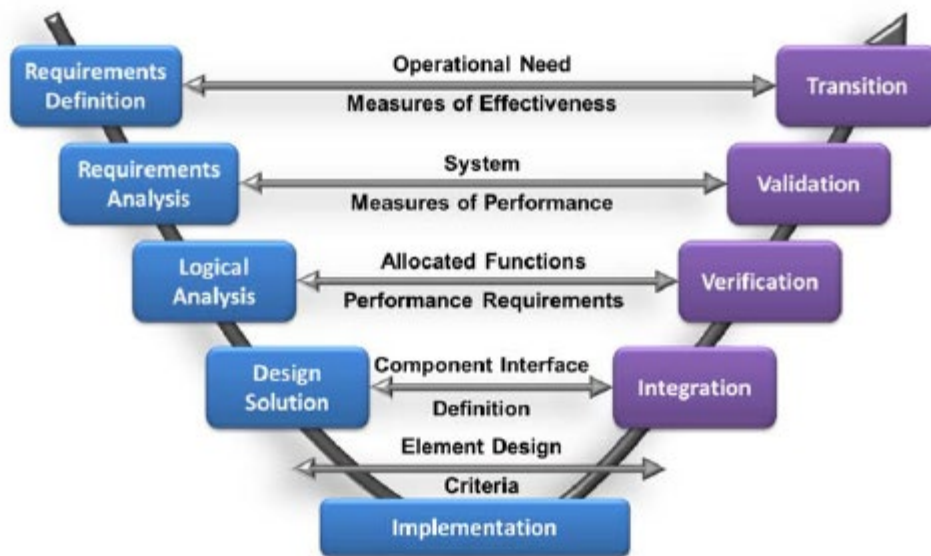


Figure 25. Standard V Development and Testing Model

Source: Department of Defense Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group, *Technology Investment Strategy 2015 to 2018* (Washington, DC: Department of Defense, May 2015), 8

Because the DoD is limited in its venues to officially convey emerging requirements to the private sector before they are validated through a requirements analysis process such as a Joint Requirements Oversight Council (JROC), they lose valuable front side development time working with the S&T and R&D community. Requirements also tend to be written be for total systems as opposed to modular components of systems which makes it difficult to conduct T&E and validation and verification (V&V) in the early portion of development as recommend by DoD's Research and Engineering Autonomy Community of Interest Test and Evaluation, Verification and Validation Working Group. The process of requirements validation, testing, and evaluation as conducted within the JCIDS normally take several years or

more resulting in users defaulting to the use of RAP to procure COTS that provide similar capabilities at a faster fielding pace with limited requirements for T&E.

Many of the requirements specifically those that come through the RAP are not technology independent. They tend to be generated in response a vendor solicitation or tech demo that purports the capability of a certain COTS system. Commercial vendors purposefully select retired military officers who are well connected to military leaders in order to conduct these solicitations and tech demos. This makes it relatively easy for the defense industry to gain access to the military users who can in turn generate requirements. Both the vendor representative and the military user may have limited technical understanding of the actual system but if the cost is low enough or the system meets a unique urgent need for the unit additional procurement avenues become possible. Items acquired through methods or organizations designed to rapidly field equipment can present the highest degree of security risk since they often contain low cost components from foreign vendors, have not gone through rigorous IT compliance procedures, and may transmit data in nefarious manners to parties outside of the DoD.

To address these issues, the DoD is acting on the bureaucratic reform guidance contained in the NSS and the NDS. The Office of the Under Secretary for Defense for Acquisition, Technology and Logistics is being restructured to include a new Under Secretary of Defense for Research and Engineering and a Under Secretary of Defense for Acquisition and Sustainment.¹⁶² Organization and regulatory restructuring is

¹⁶² Tony Bertuca, “Lord: DOD Crafting New Modernization Strategy to Guide Cutting-Edge Tech Investments,” Breaking Defense, 2 December 2017, 2, accessed 7 December 2017, <https://insidedefense.com/inside-pentagon/lord-dod-crafting-new-modernization-strategy-guide-cutting-edge-tech-investments>.

attempting to reduce the time between validating a requirement and awarding a contract by as much as 50 percent further reducing programmatic costs and accelerating fielding timelines.¹⁶³ Additional avenues such as the “Commercial Solutions Opening (CSO) process piloted by the DIUx . . . enables the DoD to rapidly acquire promising innovative commercial technologies” using non-standard contracting tools.¹⁶⁴

Developing requirements for autonomy and AI based on the definition of autonomous functioning within a system would allow capability developers to share understanding with the private sector. Standardizing terminology and developing a taxonomy that describes the spectrum of autonomy would support the development of measurable, testable Key Performance Parameters and Key System Attributes. The ability to convey these requirements to the private sector during capability development and conduct concurrent testing, validation, and verification prior to purchase could streamline acquisition and reduce overall programmatic costs. In the words of Ellen Lord, the Under Secretary of Defense for Acquisition and Sustainment:

The private sector can be a key source for technology and capability development where overlapping needs exist, as it is developing a range of technologies relevant to autonomy for commercial applications. It also often develops technology at lower cost and with faster design cycles, which can provide benefits if DoD can identify and leverage these opportunities.¹⁶⁵

¹⁶³ U.S. Congress, Senate, “Testimony Statement of The Honorable Ellen M. Lord Under Secretary of Defense Acquisition, Technology and Logistics Before the Committee on Armed Services United States Senate, 1st Sess., 115th Cong., December 7, 2017, 4.

¹⁶⁴ Ibid., 4.

¹⁶⁵ Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 9.

Innovation versus Adaptation: Changing Culture to become “Fast Followers”

For the majority of US history, the government has been the main force funding and driving innovation.¹⁶⁶ With smart technology becoming increasingly affordable to the global consumer population, there has been a paradigm shift over the last few years. “Technology R&D is now driven by the commercial sector . . . the DOD R&D budget is increasingly dwarfed [by the commercial sector]. . . . In terms of both time and resource considerations, DOD can’t compete.”¹⁶⁷ Within this context, AI has been touted as the new “arms race” but according to the new Undersecretary for Defense for Research and Engineering Mike Griffin, America is problematically “not yet in it. America’s adversaries . . . understand very well the possible utility of machine learning. I think it’s time we did as well.”¹⁶⁸

This new IT “arms race” favors countries in which government and industry cooperatively develop technology in unconstrained environments. This is resulting in peer competitors contesting the DoD’s operations in every domain.¹⁶⁹ Because high end

¹⁶⁶ “While the private sector accounts for roughly two-thirds of all spending on R&D, it is important to keep in mind that it largely invests in applied research while the Federal government provides 60 percent of the funding for basic research. . . . In the past, government-funded research has been the catalyst for many of the AI technologies that we know today” Furman, “Is This Time Different? The Opportunities and Challenges of Artificial Intelligence,” 10.

¹⁶⁷ Lewis, *Insights for the Third Offset*, 10-1.1

¹⁶⁸ Matt Stroud, “The Pentagon is Getting Serious About AI Weapons,” The Verge, 12 April 2018, accessed 16 April 2018, <https://www.theverge.com/2018/4/12/17229150/pentagon-project-maven-ai-google-war-military>.

¹⁶⁹ “The security environment is also affected by *rapid technological advancements and the changing character of war*. The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and

military capabilities are no longer limited to states that could traditionally afford the R&D to develop them, there is increasing competition “to see [who] can quickly and effectively harness commercial developments into military capabilities. Such competition rewards the state that can become the most effective fast follower.”¹⁷⁰

To compete in an era where commercial development outpaces traditional government acquisition ability, the DoD should consider changing its overarching IT acquisition strategy from that of a first mover to a fast follower. The business world broadly categorizes companies based on their ability to either innovate (first mover) or replicate (fast follower) technology or business practices. In short:

“First movers” (where an organization innovates and fields a new product) and . . . “fast followers” (where an organization refines ideas from elsewhere and quickly adapts them). Though there are some notable examples of first movers achieving long-term success (e.g., Coca Cola, Hoover), the data show that long term success in business is more likely from a fast-follower approach than a first mover approach. This trend is stronger in an environment characterized by rapid innovation.¹⁷¹

Being a fast follower is more than simply being able to replicate an ability pioneered by someone else. It takes a similar degree of expertise, a willingness to change culture to accept innovation, and most of all the ability to learn lessons through

moving at accelerating speed. New technologies include advanced computing, “big data” analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future. New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed.” Department of Defense, “Remarks by Secretary Mattis on the National Defense Strategy,” 3.

¹⁷⁰ Lewis, *Insights for the Third Offset*, 12.

¹⁷¹ Ibid.

the observation of others. Fast followers are able to “stand on the shoulders of giants” and allocate limited resources and time to points that produce exponential value. They posture their organizational structure, regulations, and even training to support the adoption of innovation. This ability to rapidly exploit and capitalize on the work of others is founded in the ability to both work in concert with those developing the capabilities and “to identify gaps and develop ways to integrate solutions to rapidly realize benefits.”¹⁷²

The Center for Naval Analyses recently wrote a report that recommends ways in which the DoD could become a fast follower of IT:

1. Build DOD technical expertise. Cultivate technical expertise on autonomy and AI in the military services capable of identifying specific technical requirements needed for achieving military capabilities.
2. Prioritize military R&D resources, leveraging a fast-follower approach. Instead of trying to cover all aspects of autonomy and AI, prioritize R&D resources to areas of the highest importance, or to areas not receiving attention in the commercial sector.
3. Monitor and integrate specific commercial developments. DOD technical expertise should track targeted autonomy and AI developments in the commercial sector, looking for ways to rapidly integrate those developments into military systems.¹⁷³

These recommendations are echoed in similar words in a variety of technical reports, concepts and roadmaps, funding strategies, and analysis papers from think tanks. Almost every article and press release today highlights DoD Senior leadership re-stating over and over again the intent from the NSS and NDS that the government and private sector work closely to share knowledge, streamline capability development, and decrease programmatic costs and fielding timelines. To achieve the Defense Objective

¹⁷² Lewis, *Insights for the Third Offset*, 13.

¹⁷³ *Ibid.*, V.

of “continuously delivering performance with affordability and speed as we change Departmental mindset, culture, and management systems”, the DoD should learn lessons from the past.¹⁷⁴

The development of armor technology during the Interwar period is an excellent historical example of the fast followership success. As with autonomy and AI today, there was intense debate as armies attempted to innovate and modernize with constrained budgets.¹⁷⁵ The modernization of militaries based on the development of mechanized and motorized technology was hotly contested in France, Great Britain, and the United States as an excessive expenditure that was politically and economically unsupportable during a time of recession. The militaries themselves were opposed to mechanization within specialties that culturally identified their mission with horses such as the Cavalry.¹⁷⁶

The 1919 Treaty of Versailles forbade Germany from possessing tanks and other large weapons but paradoxically this proved to be an advantage to Germany as it allowed them a relatively clean slate to develop new technology untethered by

¹⁷⁴ Department of Defense, “Remarks by Secretary Mattis on the National Defense Strategy,” 4,

¹⁷⁵ CPT Jonathan M. House, “Toward Combined Arms Warfare: A Survey of 20th Century Tactics, Doctrine, and Organization” (Research Survey Number 2, Combat Studies Institute, Fort Leavenworth, KS, August 1984), 45.

¹⁷⁶ “In the UK, Alfred Duff Cooper, Secretary of State for War, announced in the House of Commons in 1935 that asking the Cavalry to give up their horses for trucks “was like asking a great musical performer to throw away his violin and devote himself in the future to the gramophone.” Williamson Murray, “Armored Warfare: The British, French, and German Experiences,” in *Military Innovation in the Interwar Period*, eds. Williamson R. Murray and Allan R. Millett (Cambridge: Cambridge University Press, 1996), 28.

antiquated technology as opposed to Allied militaries.¹⁷⁷ “Planners could study concepts and then develop the equipment to make those concepts reality. Doctrine led technological development . . . where field trials had to be conducted, the Germans used mock-ups, or tested equipment and concepts in secret within the Soviet Union.”¹⁷⁸

The German military sent observers to Great Britain and the Soviet Union during the Interwar period specifically to learn lessons on the development of tanks.¹⁷⁹ German observers did not focus on simply learning lessons about materiel innovation, they took back lessons about doctrine and tactics as well. Based on their observations, the German military approached armor from a “combined arms framework in which infantry and artillery would extend the tank’s potential. This larger framework was crucial to the Germans deadly effectiveness on War II battlefields.”¹⁸⁰ The holistic DOTMLPF-P

¹⁷⁷ House, “Toward Combined Arms Warfare,” 52.

¹⁷⁸ Ibid.

¹⁷⁹ “The Germans watched British experiments with armor well into the 1935; as late as 1934 General Ludwig Beck, chief of the general staff, introduced an extensive report of that year’s maneuvers that circulated throughout the army. Guderian . . . admitted in his memoirs that the Germans had translated the current British field manual on the employment of armored fighting vehicles and used it as the basic primer for developing armored warfare. But the most important single factor in German innovation was the fact that they possessed a coherent doctrine based on a thorough and honest reading of the evidence. Moreover, they had considerable knowledge of what others had tried as they began their massive rearmament program in 1933, As the army’s doctrinal manual underlined, “when closely tied to the infantry, the tanks are deprived of their inherent speed”—at a time when the Germans possessed not a single tank on German territory” Murray, “Armored Warfare,” 41.

¹⁸⁰ Murray, “Armored Warfare,” 40.

approach to armor adoption supported the overarching concept of “Blitzkrieg” operations that defined Germany’s success from 1939 to 1942.¹⁸¹

The DoD can learn several lessons from German armor development that are applicable to the development and integration of AI and autonomy today. These lessons are summarized in a quote from the NDS:

Evolve innovative operational concepts. Modernization is not defined solely by hardware; it requires change in the ways we organize and employ forces. We must anticipate the implications of new technologies on the battlefield, rigorously define the military problems anticipated in future conflict, and foster a culture of experimentation and calculated risk-taking. We must anticipate how competitors and adversaries will employ new operational concepts and technologies to attempt to defeat us, while developing operational concepts to sharpen our competitive advantages and enhance our lethality.¹⁸²

In light of this, the technology gap between the first movers in the commercial sector¹⁸³ and the DoD can be mitigated through applying fast follower techniques such as the partnership that characterized the development of the US aerospace industry.

¹⁸¹ Murray, “Armored Warfare,” 46.

¹⁸² Department of Defense, “Remarks by Secretary Mattis on the National Defense Strategy,” 7.

¹⁸³ Ways to bridge this gap and incentivize industry while providing recompense to the government such as technology transfer are being discussed by the Office of Management and Budget. As defined by CAP goal 14 tech transfer will “improve the transition of federally funded innovations from the laboratory to the marketplace by reducing the administrative and regulatory burdens for technology transfer and increasing private sector investment in later-stage R&D; develop and implement more effective partnering models and technology transfer mechanisms for Federal agencies; and enhance the effectiveness of technology transfer by improving the methods for evaluating the ROI and economic and national security impacts of federally funded R&D, and using that information to focus efforts on approaches proven to work.” Performance.gov, “Improve Transfer of Federally-Funded Technologies from Lab-to-Market,” accessed 23 April 2018, https://www.performance.gov/CAP/CAP_goal_14.html.

“The U.S. government has always played a very active role in the aerospace market: providing R&D support, acting as an anchor customer, and developing regulations and standards to enforce use of safety-enhancing technologies and procedures.”¹⁸⁴ During WWI and through the initial stages of WWII there was little difference between military and commercial aviation technology and significant overlap with sectors such as automobile production.¹⁸⁵ As strategic bombing evolved into nuclear deterrence “aerospace technology and operations became one of the primary activities of the U.S. military and government. Aerospace technology became nearly synonymous with modern national power.”¹⁸⁶ Technology transfer for aerospace components helped lead other US industries to the forefront of digital systems development resulting in continued US dominance of air and space.¹⁸⁷ While the US did not always lead the aerospace arms race, “there was such a significant overlap between civilian and military aerospace technology in the first four decades after the invention of the airplane [that shared success resulted] in the commercial sphere. After WWII, the United States emerged as the clear winner in building commercial aircraft for the rapidly

¹⁸⁴ Allen and Chan, “Artificial Intelligence and National Security,” 85.

¹⁸⁵ Ibid., 84.

¹⁸⁶ Ibid., 87.

¹⁸⁷ “The United States encouraged the commercialization of military aerospace technologies. For instance, the digital computer industry received significant early support from defense organizations who needed computer chips for their guided missile avionics. This commercialization allowed producers to expand to new markets outside of aerospace, which in turn allowed them to reach even greater economies of scale and reduce costs for aerospace customers.” Allen and Chan, “Artificial Intelligence and National Security,” 88.

growing market in air transportation.”¹⁸⁸ The global dominance of the US aerospace industry enables the US military to maintain relative air and space superiority through restricted access to aerospace technology, classification of enabling technology, and export restrictions.¹⁸⁹

Similar to the partnership used to develop aerospace technology, the DoD should work with the private sector to identify overlapping research areas, use commercial solutions when feasible, and fund and protect breakthrough technology. In areas where it makes sense to be “fast followers” and integrate existing commercial technology such as big data and cloud computing, the DoD should develop courses of action to rapidly acquire commercial technology.¹⁹⁰ In areas of shared interest where the private sector can develop capabilities with fewer constraints or more efficiently, the DoD should increase collaboration.¹⁹¹

¹⁸⁸ Allen and Chan, “Artificial Intelligence and National Security,” 89.

¹⁸⁹ Ibid., 44.

¹⁹⁰ An analysis of venture capital data shows that over 100 private companies are working in data analysis areas relevant to DoD needs, and these have attracted almost \$900 million in private investment from 2010-2014. For cyber defense, private companies founded between 2010-2014 have received more than \$200 million in private investment. Given the overlaps in these application areas, these data suggest that there is enough private sector investment in order to develop technologies of substantial interest to DoD. Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 9.

¹⁹¹ “One area that has substantial overlap across the categories of performance, risk, and cost is human-machine interaction technology. Despite different missions and operational environments, DoD and commercial needs for human-machine interaction technology are similar because both are seeking relatively intuitive mechanisms for interaction.” Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 11.

When deciding which areas the DoD should be a “first mover” versus “fast follower” the DoD should consider the type of technology being developed as depicted in figure 26. Acquisition tends to focus around sustaining and incremental innovations because the DoD “is partial to a product or process, and it simply wants to improve upon a good thing usually to advance efficiencies . . . [or a] product or process [is] challenged by an adversary and the organization must evolve in order to preserve its effectiveness.”¹⁹² Disruptive and breakthrough innovations however “target new markets in their design, and when adopted and implemented, have a greater likelihood of reshaping the environment. These types of innovation tend to be more proactive in nature and seek to shift the balance of power in favor of those who possess the innovation.”¹⁹³

¹⁹² Ernest W. Wong and Nicholas M. Sambaluk, “Disruptive Innovations to Help Protect against Future Threats” (IEEE International Conference on Cyber Conflict, July 6, 2016), 2.

¹⁹³ Over the past century, the U.S. has become enamored with breakthrough innovations, especially as each offset strategy has provided resounding success in allowing its smaller conventional forces to match, and even surpass, its adversaries’ larger conventional military forces with cutting-edge technology and ground-breaking research. However, breakthrough innovations are expensive to research, are technologically sophisticated, and are very difficult to achieve. While the likelihood of achieving immediate success and widespread adoption of disruptive innovations are also low, the fact that they attempt to offset an adversary’s strength with systems already in place make them generally more economical and less technologically daunting propositions. Wong and Sambaluk, “Disruptive Innovations to Help Protect against Future Threats,” 2, 4.

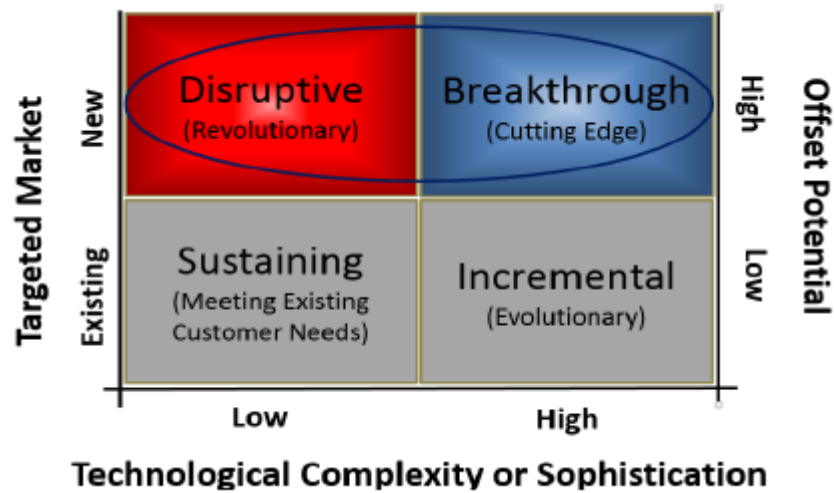


Figure 26. The Four Types of Innovation

Source: Ernest W. Wong and Nicholas M. Sambaluk, “Disruptive Innovations to Help Protect against Future Threats” (IEEE International Conference on Cyber Conflict, July 6, 2016), 2. “Each type of innovation is defined by two key factors. The first factor is the innovation’s target market, whether it be an existing one that appeals directly to existing customers and current needs, or a new market where there may not be a clearly identifiable customer or well-defined requirement at that point in time. The second factor that helps to draw distinctions between the different types of innovations is the level of technological complexity or sophistication required to bring the innovation to fruition.”

Consider breakthrough innovation as “first mover” technology and disruptive innovation as “fast follower” technology. Breakthrough technology is risky and expensive to develop because it relies on complex ideas and cutting edge technology whereas “disruptive innovations generally are cheaper to produce and do not require the level of sophisticated R&D that breakthrough innovations need. . . . Within an

environment of constrained resources, it logically follows that disruptive innovations ought to play a key role in U.S. DoD research efforts.”¹⁹⁴

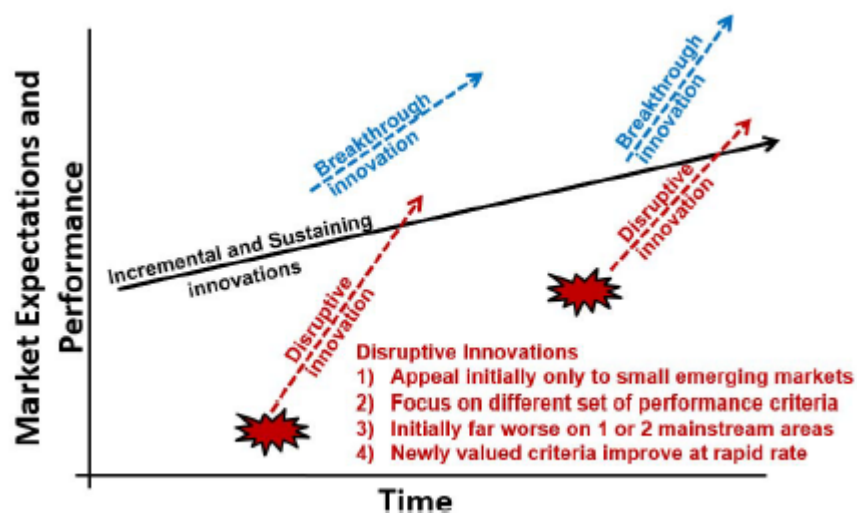


Figure 27. Comparing Breakthrough and Disruptive Innovations

Source: Ernest W. Wong and Nicholas M. Sambaluk, “Disruptive Innovations to Help Protect against Future Threats” (IEEE International Conference on Cyber Conflict, July 6, 2016), 3.

History presents a case for disruptive innovation when the agency backing it is willing to conduct experimentation.

In the American Revolutionary War, the outnumbered and ill-equipped American irregulars repelled the British Regulars with constant skirmishes and hit-and-run tactics. After World War I, battleships which had served the U.S. Navy’s leading capital ship lost their role to the disruptive innovation of carriers and the extended reach that their on-board aircraft provided. During World War II, operational research scientists were able to determine that the survivability of transport ships increased significantly when travelling in convoys; the use of

¹⁹⁴ Wong and Sambaluk, “Disruptive Innovations to Help Protect against Future Threats,” 3.

statistical analysis helped to disrupt the Nazi U-boats' control of the sea lines of communications.¹⁹⁵

The DoD could effectively save time and money by allowing the private sector to be the “first mover” developing breakthrough technology for areas that are not critically “defense unique” and fast following “disruptive innovations”. A further way to capitalize on a fast follower approach for disruptive innovations is the ability to “acquire then require” by experimenting, prototyping, testing, and evaluating prior to purchasing technology as opposed to the current “require then acquire.”¹⁹⁶ The Special Operations Community has used this practice to accelerate small batch fielding with great success. The Navy is already exploring the use of prototyping to develop small batch limited lifecycle products that operate under a concept of adapt or fail. The ability to rapidly develop, test, and improve these products allows them to iteratively evolve and change based on threat and IT upgrading.¹⁹⁷

To tie these strategies into present day examples, let's examine two cases of how sub-components of the DoD are currently using “fast follower” and “acquire then require” techniques to exploit the private sector's experiences developing AI and autonomy. The first is US Transportation Command's (USTRANSCOM)

¹⁹⁵ Wong and Sambaluk “Disruptive Innovations to Help Protect against Future Threats,” 3.

¹⁹⁶ Department of the Navy, *Strategic Roadmap for Unmanned Systems*, A-4.

¹⁹⁷ For further details refer to the Secretary of the Navy's Naval Innovation Advisory Council “Lean Startup Approach to Unmanned Systems” project charts looking to offer a methodology for rapid disruptive dual-use technology insertion through small batch capability development. Accessed 28 March 2018, <http://www.secnav.navy.mil/innovation/Pages/Home.aspx>.

groundbreaking cloud computing migration effort for its 72 logistics systems.¹⁹⁸

USTRANSCOM requested DIUx support in developing the migration strategy specifically focused on receiving assistance from over 20 commercial vendors with the engineering and integration involved in moving its first wave of migrations.

USTRANSCOM also established a “cloud center of excellence” by recruiting personal with AI knowledge and skills and it updated its mission statement and vision to reflect the how increasing automation provides enhanced performance to its customers. This type of partnership in which DIUx links the DoD to breakthrough technology developers and integrators of AI within the private sector could lay the foundation for overarching DoD cloud migration as outlined in the September 2017 memorandum entitled “Accelerating enterprise cloud adoption” from Deputy Secretary of Defense Shanahan.

The memo notably states that:

(1) technologies in areas like data infrastructure and management, cybersecurity, and machine learning are changing the character of war; (2) commercial companies are pioneering technologies in these areas; and (3) the pace of innovation is extremely rapid. The Secretary is determined to prevent any potential adversary of the United States from surprising us or overtaking our military advantage. In that regard, I am directing aggressive steps to establish a culture of experimentation, adaptation, and risk-taking; to ensure we are employing emerging technologies to meet warfighter needs; and to increase speed and agility in technology development and procurement. While technological modernization has many dimensions, I believe accelerating the Department of Defense's (DoD's) adoption of cloud computing technologies is critical to maintaining our military's technological advantage.¹⁹⁹

The memo discusses a general way ahead for migrating all levels of DoD data into the cloud as part of two phased approach. The memo was followed up by an official

¹⁹⁸ <https://federalnewsradio.com/defense-main/2017/11/with-help-from-diux-transcom-on-track-to-conduct-dods-first-large-scale-cloud-migration/> first accessed 11 may 18

¹⁹⁹ https://1yxsm73j7aop3quc9y5ifaw3-wpengine.netdna-ssl.com/wp-content/uploads/2017/11/091317_Shanahan_Cloud_Memo.pdf first accessed 11 may 2018, page 1

request for information to industry from the newly establish DoD Cloud Executive Steering Group (CESG). The RFI states that the:

DoD is seeking targeted industry input on how to best approach and structure the planned solicitation to acquire a modern enterprise cloud services solution that can support unclassified, secret, and top secret information in CONUS and OCONUS environments. This effort is being done in an aggressive, yet rigorous manner to ensure the Department realizes the operational advantages of cloud infrastructure and platform services as quickly as possible. The Department recognizes the value of technical voices from industry and encourages those voices to be at the forefront in responding to this Request for Information (RFI).²⁰⁰

The RFI asks potential vendors and others who use cloud technology to provide lessons learned as well as information on a variety of topics so that the CESG can begin to shape an acquisition and integration strategy to rapidly integrate AI. This type of nuanced approach based on early conveyance of emerging requirements, inclusion of industry partners, and willingness to accept risk with existing commercial technology where feasible supports the type of rapid fielding for critical capabilities that the DoD requires²⁰¹. USTRANSCOM's iterative movement toward the cloud and the resulting strategic guidance from the Deputy Secretary of Defense serve as excellent examples of how an integrated DOTMLPF-P approach to fast followership can succeed when leadership understands and purports the capabilities of RAS to their organizations.²⁰²

²⁰⁰

https://www.fbo.gov/?s=opportunity&mode=form&id=6fe635bc817ad6913c405d25ec5a34b5&tab=core&_cview=1 first accessed 11 may 2018

²⁰¹ <https://www.fedscoop.com/protest-transcom-will-move-classified-data-aws-cloud/> "TRANSCOM is what the Defense Information Services Agency refers to as a "pathfinder for other DOD agencies to migrate to a CS2S environment," meaning it will serve as a proof of concept for other agencies with similar needs" first accessed 11 may 2018

²⁰² <https://federalnewsradio.com/defense-main/2017/11/with-help-from-diux-transcom-on-track-to-conduct-dods-first-large-scale-cloud-migration/> "This has been championed by Gen. McDew [USTRANSCOM Commander], and also across the staff," Riester said. "It's let us look at the art of

A second example of how the DoD can expedite the development of breakthrough technology to inform or achieve its own requirements is by capitalizing on developing relationships with the commercial sector such as the newly minted cooperative research and development agreement established between the Army and Uber.²⁰³ Uber and US Army Research, Development, and Engineering Command, Army Research Laboratory (RDECOM ARL) agreed to jointly fund and collaborate on R&D of future rotor technology in support of Uber's autonomous "Uber Air" and the Army's Future Vertical Lift (FVL) programs. As part of the overarching partnership between Uber and NASA to create the technology necessary to fly autonomous air taxis within the National Airspace System (NAS)²⁰⁴, the Army and Uber will focus on the development of a new co-rotational axis rotor system and NASA and Uber will focus on upgrading the current airspace structure to integrate autonomous aircraft.²⁰⁵ This partnership also extends to academic institutions who are assisting in developing the AI integration that is necessary to enable the type of autonomy required for both air taxis and airspace management to achieve Uber Air. While the commercial sector may achieve the initial breakthrough technology for both autonomous aircraft and complex airspace management, the DoD will be the ultimate beneficiary if they remain involved

the possible when we're moving to the cloud. And as we started to educate and bring more of our workforce along, it's helped them realize the benefits and some of the things that can help and improve their jobs, from a security standpoint, building in assurance to their applications, guaranteeing their customer and the warfighter that they're going to be able to carry out the mission."

²⁰³ <https://www.army.mil/article/204882/> first accessed 11 May 2018

²⁰⁴ Uber and NASA actually have two separate agreements. See <https://utm.arc.nasa.gov/index.shtml> for information on Unmanned Aircraft Systems (UAS) Traffic Management (TM) and see <https://www.nasa.gov/press-release/nasa-uber-to-explore-safety-efficiency-of-future-urban-airspace> for information on Urban Air Mobility (UAM) first accessed 11 May 2018

²⁰⁵ <http://www.complex.com/life/2018/05/uber-plans-to-join-with-nasa-and-us-army-to-develop-aviation-rideshare-network-uber-air> first accessed 11 May 2018

throughout the development process. Joint development with industry focused around experimentation and prototyping will allow the DoD to iteratively integrate lessons learned and modularly modernize existing programs while informing future concepts. In a time of budget constraints and rapidly developing technology, these types of partnerships are critical to maintaining the DoD's ability to develop requirements into relevant material that at a lower cost and faster pace than is possible through JCIDS.

In summary, the DAS is not agile enough to develop IT via the JCIDS process which results in user demand for COTS via the RAP. Because the DoD is unable to develop requirements on pace with the commercial sector, it has become overly reliant on commercial technology which is often propriety in nature and contains inherent security risks. The DoD should consider alternative methods or changes to the DAS in order to rapidly develop, validate, and test requirements in collaboration with the private sector. The DoD could benefit from the S&T and R&D done within the private sector if it prioritizes funding and acquisition of different types of materiel based on the criticality of the need for government developmental lead.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

As the technology of AI continues to develop, practitioners must ensure that AI-enabled systems are governable; that they are open, transparent, and understandable; that they can work effectively with people; and that their operation will remain consistent with human values and aspirations.

— Executive Office of the President,
Preparing for the Future of Artificial Intelligence

This section is divided into recommendations for policy, doctrine, leadership and materiel. Conclusions focus on information that can be inferred from the literature review in chapter 2 and the analysis in chapter 4. Recommendations highlight specific areas of analysis for further research and propose actions that the DoD could take in the near term to improve RAS development, acquisition, and integration.

Conclusions

While the DoD currently maintains a qualitative and quantitative RAS advantage over peer competitors, it is poised to lose that advantage if it does not find a way to both modernize the current military and innovate to ensure the success of the future force. The DoD is particularly at risk of peer competitors gaining parity and contesting operations in domains where RAS employment is unable to be countered by conventional US military forces such as the information environment. The DoD also must prepare to fight against AI enabled robotic adversaries on a conventional battlefield who may possess qualitative advantages of tempo and reach over US forces as well as a quantitative numerical superiority. Based on the AI dominance strategies published by Russia and China, the US military must rapidly generate DOTMLPF-P solutions to both

deter and overmatch these countries ability to project power in all domains. To do this, the DoD must re-frame the way it develops, acquires, and integrates RAS specifically in regards to policy, doctrine, leadership, and materiel.

Recommendations

Autonomy can provide the DoD tremendous value by enhancing the performance of military systems, decreasing risk to U.S. warfighters, and generating cost savings. DoD R&D efforts should focus on developing systems to operate in complex, adversarial environments and leveraging commercial technology for information analysis, cyber defense, and cost-saving applications. To support these technology development efforts, DoD should develop policy and conduct research and experimentation to support open architectures, interoperability, resilience, CONOPS development, and TEV&V to ensure that U.S. systems maximize capability and flexibility, while minimizing risk and cost. If successful, developments in these areas will enable DoD to overcome challenges posed by the security environment, paving the way for continued U.S. military superiority.²⁰⁶

Recommendations and mitigations for the gaps discussed in the introduction follow and are defined in terms of policy, doctrine, leadership, and materiel.

The author has four main recommendations for how the DoD can maintain a competitive RAS advantage over peer competitors.

1. The concept of autonomous functioning within a system should be the foundation for framing DoD policy. Policy should define roles to be retained by humans and cognitive, physical and operational tasks that can be allocated to machines.
2. The DoD should develop doctrine that describes AI and autonomy and publish a standardized taxonomy that describes human-machine collaboration in terms

²⁰⁶ Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 21.

of required capabilities. The concept of autonomous functioning within a system should be the foundation for the framework and taxonomy.

3. DoD leadership must provide clear intent on the roles that humans will retain and tasks that machines can do within the cognitive, physical, and operational domains. They must develop a culture that builds trust in human-machine teams and focuses on developing technology that augments and enables humans rather than engineering humans “out-of-the-loop”. A holistic study of the performance of DoD RAS should be conducted to confirm the assumptions of increasing reliability, predictability, flexibility, and robustness of human-machine collaboration. The DoD should also develop metrics to measure the performance of RAS beyond simply tracking the failure rate of systems and components.
4. The DoD should prioritize funding of breakthrough technology that is critical to its core competencies especially in areas where insufficient private sector investment exists. The DoD should assume a “fast follower” strategy for IT (specifically RAS) in areas where there is significant overlap with the private sector that would support cost savings and increase force generation. Fast Followership must be applied across the entire DOTMLPF-P spectrum to accelerate the DoD out of its current COTS centric acquisition strategy into a more collaborative approach to requirements generation and testing.

Recommendations specific to each of these points are discussed below. The author’s proposed conceptual framework and taxonomy are referenced throughout this section as figures 28 and 29 as presented below. The author recommends that the DoD

adopt the conceptual framework and taxonomy presented in figures 28 and 29 as a standardized format to develop policy, doctrine, and material. The author also recommends that DoD leadership use this framework to describe the required capabilities for human-machine collaboration.

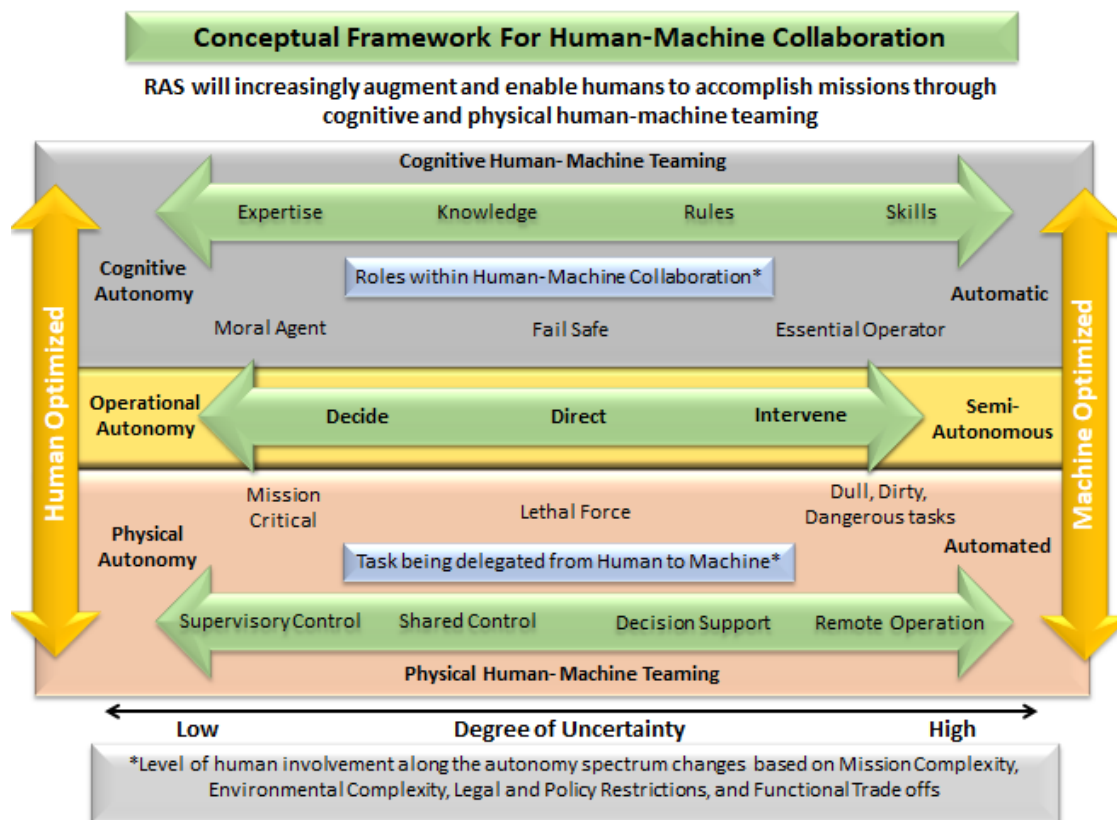


Figure 28. Conceptual Framework and Taxonomy for Human Machine Collaboration

Source: Concept developed by the author based on research and concepts developed by Mary (Missy) Cummings, “Artificial Intelligence and the Future of Warfare” (Research Paper, Chatham House, The Royal Institute of International Affairs, January 2017); Mary (Missy) Cummings, “Man vs. Machine or Man + Machine,” *IEEE Intelligent Systems* 29, no. 5 (September/October 2014): 62-69, accessed 26 February 2018, www.computer.org/intelligent; Jenay M. Beer, Arthur D. Fisk, and Wendy A. Rogers, “Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction,” *Journal of Human-Robot Interaction* 3, no. 2 (2014); and Paul Scharre, “Autonomous Weapons and Operational Risk” (Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016).

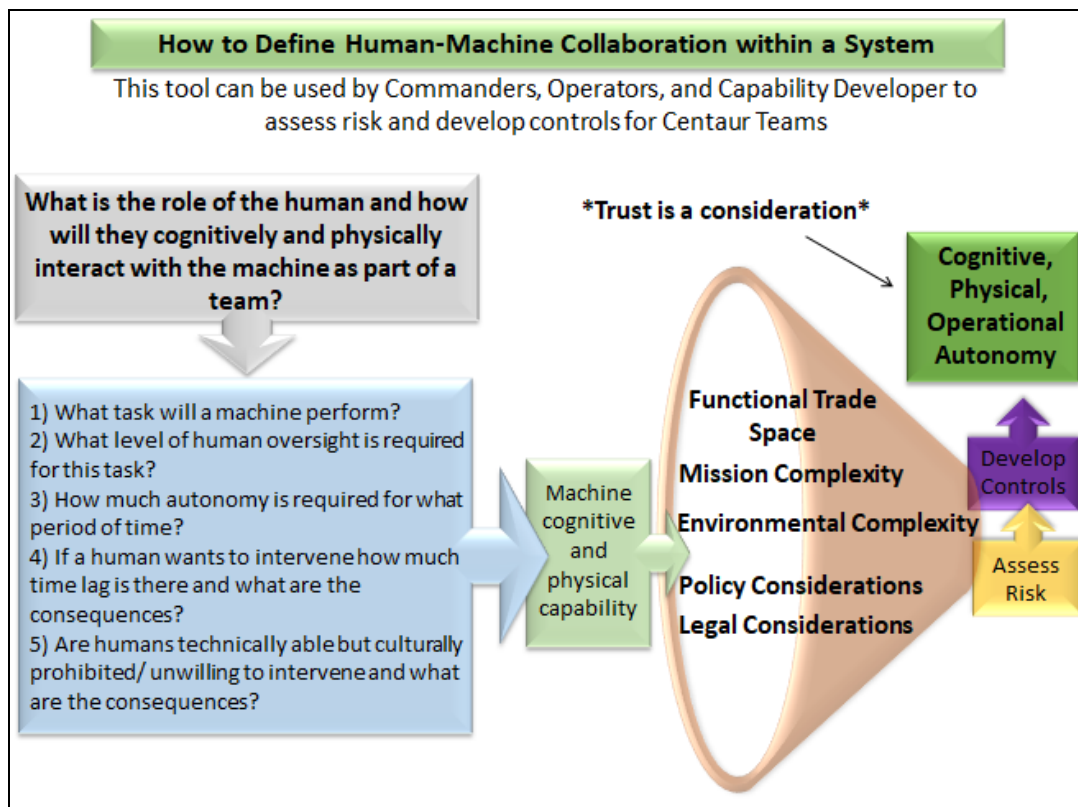


Figure 29. Conceptual Framework and Taxonomy for Human Machine Collaboration

Source: Concept developed by the author based on research and concepts developed by Mary (Missy) Cummings, “Artificial Intelligence and the Future of Warfare” (Research Paper, Chatham House, The Royal Institute of International Affairs, January 2017); Mary (Missy) Cummings, “Man vs. Machine or Man + Machine,” *IEEE Intelligent Systems* 29, no. 5 (September/October 2014): 62-69, accessed 26 February 2018, www.computer.org/intelligent; Jenay M. Beer, Arthur D. Fisk, and Wendy A. Rogers, “Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction,” *Journal of Human-Robot Interaction* 3, no. 2 (2014); and Paul Scharre, “Autonomous Weapons and Operational Risk” (Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016).

Recommendations for Policy and Doctrine

The document “Preparing for the Future of AI” developed by the National Science and Technology Committee on Technology for the Executive Office of the President states that “the Administration is engaged in active, ongoing interagency

discussions to work toward a government-wide policy on autonomous weapons consistent with shared human values, national security interests, and international and domestic obligations.”²⁰⁷ It lists a variety of recommendations for further research and action the most important of which is that “The U.S. Government should complete the development of a single, government-wide policy, consistent with international humanitarian law, on autonomous and semi-autonomous weapons.”²⁰⁸

The lack of a holistic government wide policy and roadmap to developing AI as opposed to the Chinese and Russian strategic plans discussed in chapter 4 directly impacts the DoD’s ability retain its asymmetric RAS advantage. The existence of a whole of government approach to autonomy and AI would support Federal R&D funding of critical capabilities and would facilitates collaboration between the NSIB and Federal Agencies like the DoD. As recently stated by the Vice Chief of Staff of the Air Force GEN Stephen W. Wilson, “I think it’s going to take all of us working together across academia, across the industry, across the departments, across all the national labs . . . and bringing them together in this competition with AI because that’s, in fact, what China’s doing.”²⁰⁹

Regardless of the policy gap the US government level, the current DoD issuances that pertain to autonomy and AI should be updated based on the concept of autonomous functioning within a system. The proposed framework and taxonomy in

²⁰⁷ Executive Office of the President, *Preparing for the Future of Artificial Intelligence*, 38.

²⁰⁸ Ibid.

²⁰⁹ Stroud, “The Pentagon is Getting Serious About AI Weapons.”

figures 28 and 29 substantially expands what currently exists in policy and doctrine to include not just the roles of human but also the machines particularly addressing the aspect of human-machine collaboration. Additionally, issuances should be updated with the definitions for the following terms as proposed in the glossary of this research: Artificial Intelligence, Artificial General Intelligence, Augmentation, Automation, Autonomous functioning with a system, Autonomy, Centaur Teaming, Cognitive Autonomy, Decision Support, Disruptive Innovation, Distributed System, Human-Machine Collaboration, Narrow Artificial Intelligence, Operational Autonomy, Physical Autonomy, Remote Operation, Shared Control, Supervisory Control, and Team. It is recommended that the DoD either refrain from using or better define misleading terms such as unmanned, “loop” based terms, autonomous system, semi-autonomous system, flexible autonomy, and supervised autonomy.

Recommendations for Leadership

DoD leadership should advocate for RAS adoption in three main ways. First, leaders must prioritize modernization of current capabilities based on an open architecture system to ensure that future concepts do not become reliant on commercial technology. Second, leaders must provide clear and unambiguous intent on what roles will be retained by humans and what tasks machines can do within the cognitive, physical, and operational domains. Specific to this, they must provide intent on the development of human-machine collaborative teams designed to enable, augment and team with humans. Third, leaders must embrace RAS with the understanding that machines can augment and enable humans to achieve beyond human cognitive, physical, and operational capabilities. Leaders are responsible for building a culture of trust within

the DoD to integrate RAS with the understanding that maintaining the military's paradigm status is based on the need adopt rapid and sweeping moves toward automation.

To provide the groundwork for how the DoD could benefit from increasing automation, DoD leadership should request two studies:

1. An overarching assessment of the DoD to determine how AI and automation could support cost savings and reduce risk across the force.

2. The DoD should request a study to assess the performance of current RAS.

The study should validate or deny the assumptions of increasing reliability, predictability, flexibility, and robustness of human-machine collaboration over traditionally “manned” systems. The analytics of such a study should both corroborate the need for RAS in future concepts and increase trust within the DoD for RAS.

Trust between humans and machines is the foundational component of cultural change because “The Joint Force requires the ability to operate along the spectrum of operations with teams of humans and/or machines.”²¹⁰ Regardless of cultural or personal aversion to automation and autonomy, leaders must be cognizant that the terms they use to describe RAS will largely determine the amount of training that Soldiers invest in current RAS technology and the degree to which they trust their systems.

²¹⁰ Joint Chiefs of Staff, *JCRAS*, 14.

Recommendations for Acquisition

The ability to become “fast followers” of IT will largely determine the DoD’s ability to regain a competitive RAS advantage.²¹¹ The future of RAS development will largely be based on collaboration with the private sector, the DoD’s ability to reform the DAS to support rapid modernization and acquisition specifically for IT, and emergence of requirements for modular components versus entire COTS systems. As stated by Secretary of Defense Mattis AI has “got to be better integrated by the Department of Defense, because I see many of the greatest advances out here on the West Coast in private industry.”²¹²

The Office of Technical Intelligence document “DoD Research and Engineering: Technical Assessment for Autonomy” lists multiple recommendations that merit mention in this research. They fall into five broad categories to be further discussed below:

1. Broaden participation in the DOD acquisition process by lowering the barriers to entry for non-traditional industry partners
2. Increase risk tolerance
3. Accelerate the acquisition processes to pace the accelerating threats and evolving technology of today’s global environment

²¹¹ “Unlike the past, where government research drove technological development, global commercial interests will drive the direction and the tempo of advancements in RAS. The Joint Force must be able to identify innovations in unique RAS technology, adapt and incorporate appropriate military requirements, and rapidly field to the force” Joint Chiefs of Staff, *JCRAS*, 16.

²¹² Tom Simonite, “Defense Secretary James Mattis Envis Silicon Valley AI Ascent,” *Wired*, 11 August 2017, accessed 16 April 2018, <https://www.wired.com/story/james-mattis-artificial-intelligence-diux>.

4. Impose common standards and modular design to reduce costs, improve interoperability within and across domains, and broaden the vendor base
5. Allow for an iterative process in the development of requirements, informed by early fleet experimentation, prototyping, and demonstrations²¹³

Key to achieving all of these points is collaboration with the private sector within the guidance from the NSS and the NDS. Specifically, “the DoD should aim to leverage the private sector to solve lower complexity problems where significant near-term savings and advancements can be realized and conserve R&D investment for other, defense-unique areas.”²¹⁴ The DoD should conduct an assessment of what areas are “defense-unique” and which they can assume risk through “acquire then require” or “fast follower” techniques. An initial assessment is that:

The private sector will be well positioned to support DoD needs in terms of cost reduction, information analysis, and cyber defense, but DoD will need focused investments to develop systems to operate in complex, adversarial environments. However, just because private sector investment will develop relevant technologies does not mean that DoD will benefit. The Office of the Secretary of Defense and the Services will need to enact concerted efforts to identify, evaluate, acquire, and tailor commercial technologies.²¹⁵

The DoD must prioritize funding for the development of critical capabilities that are unique to its needs and find ways to leverage lessons learned from testing and experimentation with commercial technology within the private sector. The DoD should remain a “first mover” for breakthrough innovations with defense unique requirements,

²¹³ Department of the Navy, *Strategic Roadmap for Unmanned Systems*, 36.

²¹⁴ Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 24.

²¹⁵ *Ibid.*, 13.

a “fast follower” for areas where they are unable to innovate at the same pace as the commercial sector but collaboration is possible, and adopt an “acquire then require” approach to areas that particularly support the DoD’s ability to purchase and then improve through iterative prototyping. The author recommends further research to determine viability of changes to the DAS to institute both “acquire then require” and “fast followership” of IT. The DoD should also weight its investment portfolio in favor of narrow AI over AGI: “DoD’s portfolio in AGI should be modest and recognize that it is not currently a rapidly advancing area of AI. The field of human augmentation via AI is much more promising and deserves significant DoD support.”²¹⁶

To support effective collaboration with the private sector across all of these areas, the DoD must reform the DAS to support early and frequent discussion of requirements specifically developed around the concept of autonomous functioning with a system.²¹⁷ This type of approach is specifically recommended in the JCRAS and defined in CRC 5 within that document: “The Joint Force requires the ability to develop

²¹⁶ Potember, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, 56.

²¹⁷ “The main obstacle to introducing modularity into the force is reliance on proprietary hardware and software that are tethered to the original manufacturer. This creates legal complications involving intellectual property and practical challenges involving design that impose high costs for platform modifications. To mitigate these challenges, DoD should require an open architecture for systems, which is a series of protocols that define how different aspects of the system interface and communicate with each other from a hardware and software point of view. Adopting an open architecture would mean that any developer could create new modules – perception, cognition, or action – and integrate them relatively quickly into existing systems, including with parts from other designers – to develop new or upgraded systems. This would decrease upgrade and development costs and timelines.” Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 16.

modular systems supported by open architectures enabling cross-service and partner-nation interchangeability whenever feasible.”²¹⁸

Changing to modular requirements as stipulated in the NDS and JCRAS would also support the type of T&E and validation and verification recommended by the DoD’s Research and Engineering Autonomy Community of Interest Test and Evaluation, Verification and Validation Working Group.²¹⁹ This group proposes the following change to the standard “V” process discussed in chapter 4 of this research as a way begin to address the testing, validation, and verification of requirements that accounts for autonomy.

²¹⁸ Joint Chiefs of Staff, *JCRAS*, 15.

²¹⁹ “Testing and evaluating future highly autonomous systems will require an increased emphasis on setting verifiable requirements, developing system models traceable to requirements to guide design activities, and verifying and validating merging subsystems and products throughout the development process” Department of Defense, Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group *Technology Investment Strategy 2015 to 2018*, 8.

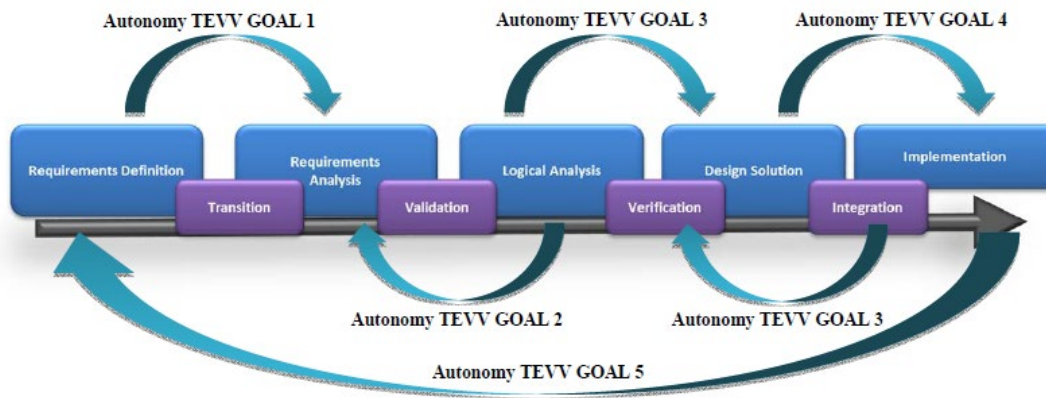


Figure 30. Proposed Changes to the Standard V Model

Source: Department of Defense, Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group *Technology Investment Strategy 2015 to 2018* (Washington, DC: Department of Defense, May 2015), 9.

The DoD Research and Engineering document “Technical Assessment for Autonomy” agrees with need for changed metrics and process.²²⁰ The JCRAS also discusses the need to clearly articulate requirements and goals through collaborative development with the private sector. CRC 7 states that “The Joint Force requires the ability to identify and articulate clearly RAS operational requirements, technology development goals, and acquisition requirements to industry, academia, and the military Science and Technology (S&T) community.”²²¹

²²⁰ “Recommendation 13: Take advantage of opportunities to leverage commercial R&D in autonomy to reduce costs, particularly in logistics, maintenance, and information analysis. . . . Given their potential sophistication, autonomous systems will also require the development of new metrics, standards, and methodologies for TEV&V” Department of Defense, Research and Engineering, *Technical Assessment: Autonomy*, 16.

²²¹ Joint Chiefs of Staff, *JCRAS*, 16.

A final point pertains to the need for the DoD to develop a whole of agency approach to developing and integrating RAS. “AI, both commercially derived and DoD-specific, will be integral to most future DoD systems and platforms. To be a “smart buyer” and to support its unique development needs, DoD needs to maintain a strong portfolio of [AI] research, and a cadre of knowledgeable program officers, widely across the most rapidly advancing areas.”²²² Leadership is ultimately responsible to transition the DoD culturally and operationally as the character of war changes. The DoD must make this transition in a united manner if they wish to retain a competitive RAS advantage over peer competitors. Interoperability, integration, and interdependence between the Services is critical to the success of future concepts in which thinking, acting agents other than humans will have increasing operational autonomy to execute missions. “A comprehensive joint approach will enhance the interoperability of systems, while avoiding duplication of capability and excessive costs, thus ensuring the Joint Force’s ability to realize the full potential of cross-domain RAS employment for operational effectiveness.”²²³

²²² Potember, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, 55.

²²³ Joint Chiefs of Staff, *JCRAS*, 19.

GLOSSARY

Artificial General Intelligence. An artificial intelligence system [agent] that exhibits goal based behavior at least as advanced as a human across the range of cognitive, social and physical behaviors.²²⁴

Artificial Intelligence. Systems capable of perception, cognition, and action that seek to approximate human knowledge and expertise. Specific capabilities include learning, reasoning, rationality, planning, communicating, decision-making, self-direction, and adaptation. Cognitive architectures and neural networks provide the foundation for machine intelligence.²²⁵

Augmentation. An informational, electromechanical, or pharmaceutical system that enhances human physical or cognitive capability and acts as an extension to the human operator.²²⁶

Automation. A system that functions with limited human involvement. System performance is restricted to specific actions by design. Typically these are well-defined tasks that have predetermined responses based on specific inputs, rules, and outputs.²²⁷

Autonomous functioning in a system. The ability of a system, platform, or software to complete a task without human intervention, using behaviors resulting from the action of computer programming with the external environment. Tasks or functions executed by a platform, or distributed between a platform and other parts of a system, may be performed using a variety of behaviors which may include reasoning and problem solving, adaptation to unexpected situations, self-direction, and learning. Which functions are autonomous – and the extent to which human operators can direct, control or cancel functions – is determined by system design function trade-offs, mission complexity, external operating environment conditions, and legal or policy constraints. This can be contrasted with automated functions, which (although they require no human intervention) operate using a fixed set of inputs, rules, and outputs, the behavior of which is

²²⁴ Author Proposed Definition.

²²⁵ Author Proposed Definition.

²²⁶ John's Hopkins Applied Physics Laboratory. "NSAD-R-16-045," 5-8.

²²⁷ Derived from Department of Defense, Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group. *Technology Investment Strategy 2015 to 2018*, 2.

determined and largely predictable. Automatic functions do not permit the dynamic adaptation of inputs, rules, or outputs.²²⁸

Autonomous weapons system: A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.²²⁹

Autonomy. A state in which a system possesses sufficient self-direction capabilities to be authorized to operate with limited or no human oversight during mission performance. The system may be highly automated or have cognitive and physical capabilities that support goal based reasoning and action.²³⁰

Centaur teaming. Cognitive architectures that can leverage the predictability, reliability, and speed of automation while retaining the robustness and flexibility of human intelligence.²³¹

Cognitive Autonomy. The degree of self-direction with which systems are authorized to conduct conscious intellectual activity such as decision making, reasoning, problem solving, and learning with limited or no human oversight during mission performance. This ability is largely based on the presence of artificial intelligence.²³²

Decision Support. The degree of physical autonomy in which the system perceives the environment and develop task plans. The human monitors the system and environment and is responsible for selecting and directing the system in the implementation of the task plan. The human intervenes if the machine requests assistance or the level of task complexity increases beyond machine capability.²³³

Disruptive Innovation. Technology that targets new markets through design to reshape the operational environment and shift the balance of power in favor of those who

²²⁸ Williams and Scharre, *Autonomous Systems*, 56-57.

²²⁹ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, 13.

²³⁰ Author proposed definition.

²³¹ Scharre, “Autonomous Weapons and Operational Risk,” 5.

²³² Author proposed definition.

²³³ Author proposed definition.

possess these innovations. This type of technology is generally less risky and costly to develop than breakthrough technology.²³⁴

Distributed system. A number of independent agents linked by a network that appear to its users as a single coherent system.²³⁵

Flexible autonomy. The ability to adjust the level of human control over RAS. When deciding the level of control, the commander will consider system capabilities and limitations, mission risk and complexity, and characteristics of the operating environment. The commander may employ a specific RAS with greater human control in some situations but employ the same RAS with greater autonomy in other circumstances (i.e., contested environments with degraded or denied communications).²³⁶

Human in-the-loop. The machine stops and waits for human approval before continuing after each task is completed. The human operator is assumed able to monitor the environment and the machine's actions, and gives a "go ahead" to the machine once it has been confirmed that the machine's performance is adequate and consistent with operational mission requirements.²³⁷

Human-Machine Collaboration. Agents have a cognitive understanding of each other's capabilities, can monitor progress towards goals, and engage in human-like teamwork. Trust between agents is fundamental to achieving goals.²³⁸

Human on-the-loop. Once activated, the machine performs a task under human supervision, and will continue performing the task until the human operator intervenes to halt its operation. However, in practice, there will always be a time delay between when a malfunction or failure occurs and when the operator exerts whatever "control" is necessary to adjust the machine's behavior. For example, it may take some time for the human operator to simply "recognize" (and/or understand the reasons for) a malfunction, and there may be some delay in

²³⁴ Definition derived from Wong and Sambaluk, "Disruptive Innovations to Help Protect against Future Threats."

²³⁵ John's Hopkins Applied Physics Laboratory. "NSAD-R-16-045," 5-8.

²³⁶ Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, 7.

²³⁷ Ilachinski, *AI, Robots, and Swarms*, 147.

²³⁸ Derived from Defense Science Board, *Task Force Report: The Role of Autonomy in DoD Systems*, 50.

deciding on what commands are appropriate to send to the machine to correct its behavior.²³⁹

Human out-of-the-loop. Once activated, the machine performs its tasks without any assistance on the part of the human operator, who neither supervises the operation nor has an ability to intervene in the event of a system failure.²⁴⁰

Human-supervised autonomous weapon system. An autonomous weapon system that is designed to provide human operators with the ability to intervene and terminate engagements, including in the event of a weapon system failure, before unacceptable levels of damage occur.²⁴¹

Narrow Artificial Intelligence. An artificial intelligence system [agent] that exhibits rule or goal based perception, cognition, or action for specific application areas.²⁴²

National Security Innovation Base (NSIB). The American network of knowledge, capabilities, and people including academia, National Laboratories, and the private sector that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life.²⁴³

Operational Autonomy. The degree of self-direction with which systems are authorized to accomplish missions and goals with limited or no human oversight during mission performance. Self-direction is based on the cognitive and physical capabilities of the machine as factored against mission complexity, environmental complexity, legal considerations, policy considerations, functional trade space, and risk. Authorization of self-direction is contingent on human trust in machine ability.²⁴⁴

Physical Autonomy. The degree of self-direction with which systems are authorized to conduct tasks or physical work with limited or no human oversight during mission performance. This ability is largely based on automation resulting from

²³⁹ Ilachinski, *AI, Robots, and Swarms*, 148.

²⁴⁰ *Ibid.*, 151.

²⁴¹ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, 14.

²⁴² Author proposed definition.

²⁴³ Office of the President of the United States, *The National Security Strategy of the United States of America*, 21.

²⁴⁴ Author proposed definition.

rule based behavior. Artificial intelligence can be integrated into systems to achieve goal based behavior.²⁴⁵

Remote Operation. The degree of physical autonomy in which the system enables or augments humans to act. The human is responsible for perception and cognition aided by information provided by sensors within the system. The human directs the system in action implementation and intervenes if the machine requests assistance or the level of task complexity increases beyond machine capability.²⁴⁶

Robot. A powered machine capable of executing a set of actions by direct human control, computer control, or a combination of both. It is comprised minimally of a platform, software, and a power source.²⁴⁷

Robotic and Autonomous Systems (RAS). A framework to describe systems with a robotic element, an autonomous element, or more commonly, both. As technology advances, there will be more robotic systems with autonomous capabilities as well as non-robotic autonomous systems. The term highlights the physical (robotic) and cognitive (autonomous) aspects of these systems.²⁴⁸

Semi-autonomous weapon system. A weapon system that, once activated, is intended to only engage individual targets or specific target groups that have been selected by a human operator.²⁴⁹

Shared Control. The degree of physical autonomy in which the system is authorized sufficient self-direction to perform all aspects of a task with limited human oversight during mission performance. The human monitors the system and environment and intervenes if the machine request assistance or the level of task complexity increases beyond machine capability.²⁵⁰

Supervised Autonomy. A framework which facilitates the development of human robot systems devised in a human-oriented manner to augment users in accomplishing

²⁴⁵ Author proposed definition.

²⁴⁶ Author proposed definition.

²⁴⁷ Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, A-4.

²⁴⁸ Ibid., 2.

²⁴⁹ Department of Defense, Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, 14.

²⁵⁰ Author proposed definition.

their task. The general concept is to incorporate supervisory control with a qualitative approach for the control of robots. Supervisory control does not rely on human users to perform all the basic functions of perception and action in a system. Instead, it shifts all basic autonomous functions to the physical robot agent, integrated with a set of qualitative instructions, in combination with a simple graphical user interface, and together with suitable feedback form the complete framework.²⁵¹

Supervisory Control. The degree of physical autonomy in which the system is authorized sufficient self-direction to perform all aspects of a task with limited or no human oversight during mission performance. The human monitors the system and environment and intervenes if needed.²⁵²

Team. A distinguishable set of two or more agents who interact dynamically, interdependently, and adaptively toward a common and valued goal/object/mission, who have each been assigned specific roles or functions to perform.²⁵³

Unmanned System [platform]. An electro-mechanical system [platform], with no human operator aboard, that is able to exert its power to perform designed missions. May be mobile or stationary. Includes categories of unmanned ground vehicles (UGVs), unmanned aerial vehicles (UAVs), unmanned underwater vehicles (UUVs), unmanned surface vehicles (USVs), unattended munitions (UMs), and unattended ground sensors (UGS). Missiles, rockets, and their sub-munitions, and artillery are not considered unmanned systems.²⁵⁴

²⁵¹ Gordon Cheng, and Alexander Zelinsky, “A Framework for Human-Robot Systems Development,” *Autonomous Robots* 10, no. 3 (May 2001): 251.

²⁵² Derived from Horizon Digital Economy Research Institute, “The IEEE P7003 Standard for Algorithmic Bias Consideration,” accessed 20 March 2018, <https://ec.europa.eu/jrc/communities/sites/jrccties/files/ansgarkoene-2018.pdf>.

²⁵³ John’s Hopkins Applied Physics Laboratory. “NSAD-R-16-045,” 5-8.

²⁵⁴ Hui Min Huang, ed., *Autonomy Levels for Unmanned Systems (ALFUS) Framework, Volume I: Terminology* (Gaithersburg, MD: National Institute of Standards and Technology, September 2004), 20, accessed 30 November 2017, https://www.nist.gov/sites/default/files/documents/el/isd/ks/NISTSP_1011_ver_1-1.pdf.

BIBLIOGRAPHY

- Allen, Greg, and Daniel Chan. "Artificial Intelligence and National Security." Report, Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge, MA, 2017.
- Article 36.org. "Key Elements of Meaningful Human Control." Accessed 2 April 2018. <http://www.article36.org/wp-content/uploads/2016/04/MHC-2016-FINAL.pdf>.
- Baculinao, Eric. "The U.S. No Longer Possesses Clear Military-Technical Dominance, and China is Rapidly Emerging as a Would-Be Superpower in Science and Technology." *NBC News*, 17 February 2018. Accessed 1 May 2018. <https://www.nbcnews.com/news/world/these-chinese-military-innovations-threaten-u-s-superiority-experts-say-n848596>.
- Beer, Jenay M., Arthur D. Fisk, and Wendy A. Rogers. "Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction." *Journal of Human-Robot Interaction* 3, no. 2 (2014): 74-99.
- Bendett, Samuel. "In AI, Russia is Hustling to Catch Up." *Defense One*. 4 April 2018. Accessed 9 April 2018. <http://www.defenseone.com/ideas/2018/04/russia-races-forward-ai-development/147178/>.
- . "Russia is Poised to Surprise the US in Battlefield Robotics." *Defense One*. 25 January 2018. Accessed 9 April 2018. <http://www.defenseone.com/ideas/2018/01/russia-poised-surprise-us-battlefield-robotics/145439/>.
- Bertuca, Tony. "Lord: DOD Crafting New Modernization Strategy to Guide Cutting-Edge Tech Investments." *Breaking Defense*. 2 December 2017. Accessed 7 December 2017. <https://insidedefense.com/inside-pentagon/lord-dod-crafting-new-modernization-strategy-guide-cutting-edge-tech-investments>.
- Bier, Nicole, and Patrick Madden. "Unmanned Aerial Vehicle Assessment: Russia." *Red Diamond* (January/February 2018): 8-13.
- Bradshaw, Jeffrey M., Robert Hoffman, Matthew Johnson, and David Woods. "The Seven Deadly Myths of Autonomous Systems." *Human Centered Computing* (May-June 2013): 2-9.
- Bughin, Jacques, Eric Hazan, Sree Ramaswamy, Michael Chui, Tera Allas, Peter Dahlström, Nicolaus Henke, and Monica Trench. "Artificial Intelligence the Next Digital Frontier?" Discussion Paper, McKinsey Global Institute, June 2017.
- Chairman of the Joint Chiefs of Staff. *Capabilities-Based Assessment (CBA) User's Guide, Version 3: Force Structure, Resources, and Assessments Directorate (JCS J-8)*. Washington, DC: Government Printing Office, March 2009.

- Chase, Michael S. *China's Conception of Strategic Deterrence also Includes Deterrence in the Space and Information Domains*. Santa Monica, CA: RAND Corporation, 2018. Accessed 1 May 2018. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT489/RAND_CT489.pdf.
- Cheng, Gordon, and Alexander Zelinsky. "A Framework for Human-Robot Systems Development." *Autonomous Robots* 10, no. 3 (May 2001): 251-266.
- . "Supervised Autonomy: A Paradigm for Tele-Operating Mobile Robots." Research School of Information Sciences and Engineering, The Australian National University, Canberra, Australia, 2001.
- Clough, Bruce T. *Metrics, Schmetrics! How the Heck do you Determine a UAV's Autonomy Anyway?*, Wright Patterson AFB: Government Printing Office, August 2002.
- Creemers, Rogier; Graham Webster, Paul Tsai; Paul Triolo; and Elsa Kania. Translated. "A Next Generation Artificial Intelligence Development Plan." New America Cybersecurity Initiative, 2017. Accessed 29 March 2018. <https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf>.
- Cummings, Mary (Missy). "Artificial Intelligence and the Future of Warfare." Research Paper, Chatham House, The Royal Institute of International Affairs, January 2017.
- . "Informing Autonomous System Design Through the Lens of Skill-, Rule-, and Knowledge-Based Behaviors." *Journal of Cognitive Engineering and Decision Making* (October 2017): 58-61.
- . "Man vs. Machine or Man + Machine." *IEEE Intelligent Systems* 29, no. 5 (September/October 2014): 62-69. Accessed 26 February 2018. www.computer.org/intelligent.
- Defense Science Board. *Summer Study on Autonomy*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, June 2016.
- . *Task Force Report: The Role of Autonomy in DoD Systems*. Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, June 2012.
- Department of Defense. Department of Defense Directive 3000.09, *Autonomy in Weapons Systems*, Change 1. Washington, DC: Department of Defense, 8 May 2017.
- . Department of Defense Directive 5100.01, *Functions of the Department of Defense and its Major Components*. Washington, DC: Department of Defense, 21 December 2010.

- . Department of Defense Instruction 8100.04, *DoD Unified Capabilities (UC)*. Washington, DC: Department of Defense, 9 December 2010.
- . Department of Defense Instruction 8330.01, *Interoperability of Information Technology (IT), Including National Security Systems (NSS)*. Washington, DC: Department of Defense, 21 May 2014.
- . Department of Defense Instruction 8500.01, *Cybersecurity*. Washington, DC: Department of Defense, 14 March 2014.
- . *Dictionary of Military and Associated Terms*. Washington, DC: Department of Defense, February 2018.
- . “Remarks by Secretary Mattis on the National Defense Strategy.” News Transcript, January 19, 2018. Accessed 22 January 2018. <https://www.defense.gov/News/Transcripts/Transcript-View/Article/1420042/remarks-by-secretary-mattis-on-the-national-defense-strategy/>.
- . *Unmanned Systems Integrated Roadmap FY 2013-2038*, Washington, DC: Department of Defense, 2013.
- . *White Paper: Evolution of Department of Defense Directive 5100.01 “Functions of the Department of Defense and Its Major Components”*. Accessed 15 December 2017. http://dcmo.defense.gov/Portals/47/Documents/PDSD/DoDD5100.01_WhitePaper.pdf.
- Department of Defense, Foreword by Hon. Robert O. Work, 32nd Deputy Secretary of Defense. “Artificial Intelligence, Big Data, and Cloud Taxonomy.” Govini. Accessed 30 March 2018. http://www.govini.com/research-form/?post_title=DoD+ARTIFICIAL+INTELLIGENCE%2C+BIG+DATA+AND+CLOUD+TAXONOMY&post_link_redirect=http%3A%2F%2Fwww.govini.com%2Fresearch-item%2Fdod-artificial-intelligence-and-big-data-taxonomy%2F&post_id=4026
- Department of Defense, Research and Engineering. *Technical Assessment: Autonomy*, Washington, DC: Office of Technical Intelligence, February 2015.
- Department of Defense, Research and Engineering, Autonomy Community of Interest (COI) Test and Evaluation, Verification and Validation (TEVV) Working Group. *Technology Investment Strategy 2015 to 2018*. Washington, DC: Department of Defense, May 2015.
- Department of the Navy. *Strategic Roadmap for Unmanned Systems*. Washington, DC: Department of the Navy, 7 March 2018.
- Durst, Phillip J., and Wendell Gray. *Levels of Autonomy and Autonomous System Performance Assessment for Intelligent Unmanned Systems*. Vicksburg, MS: United States Army Engineer Research and Development Center, April 2014.

- Eaglen, Mackenzie T. "Repair and Rebuild: Balancing New Military Spending for a Three Theater Strategy." Research, American Enterprise Institute, Washington, DC, October 2017.
- Executive Office of the President. *Preparing for the Future of Artificial Intelligence*. Washington, DC: The White House, October 2016.
- Freedberg, Sydney J. "Artificial Stupidity: Fumbling the Handoff from AI to Human Control." *Breaking Defense*, June 5 2017. Accessed 15 December 2017. <https://breakingdefense.com/2017/06/artificial-stupidity-fumbling-the-handoff/>.
- . "Artificial Stupidity: When Artificial Intelligence + Human = Disaster." *Breaking Defense*, 2 June 2017. Accessed 15 December 2017. <https://breakingdefense.com/2017/06/artificial-stupidity-when-artificial-intel-human-disaster/>.
- Furman, Jason. "Is This Time Different? The Opportunities and Challenges of Artificial Intelligence." Remarks, AI Now: The Social and Economic Implications of Artificial Intelligence Technologies in the Near Term, New York University, New York, 7 July 2016.
- Future of Life Institute. "An Open Letter to the United Nations Convention on Certain Conventional Weapons." 21 August 2017. Accessed 15 January 2018. <https://futureoflife.org/autonomous-weapons-open-letter-2017/>.
- GLOBSEC NATO Adaptation Initiative Steering Committee. *One Alliance: The Future Tasks of the Adapted Alliance*. Slovak Republic: NATO, November 2017.
- Grant, Bob. "White House Science Office in Flux." *The Scientist*. 3 July 2017. Accessed 23 April 2018, <https://www.the-scientist.com/?articles.view/articleNo/49787/title/White-House-Science-Office-in-Flux/>.
- Harper, John. "Pentagon Struggling to Take Advantage of Artificial Intelligence." *National Defense Magazine*, August 21 2017.
- Herrmann, Jon. "Common Standards Are Vital for Innovation in the NDAA." *Real Clear Defense*, September 26 2017.
- Hoffman, F. G. "Exploring War's Character and Nature: Will War's Nature Change in the Seventh Military Revolution?" *Parameters* 47, no. 4 (Winter 2017-18): 19-31.
- Horizon Digital Economy Research Institute. "The IEEE P7003 Standard for Algorithmic Bias Consideration." Accessed 20 March 2018. <https://ec.europa.eu/jrc/communities/sites/jrccties/files/ansgarkoene-2018.pdf>.
- Horowitz, Michael C., and Paul Scharre. "An Introduction into Autonomy in Weapons Systems," Working Paper, Center for a New American Security, Washington, DC, February 2015.

- . *Meaningful Human Control in Weapons Systems: A Primer*, Working Paper, Center for a New American Security, Washington, DC, March 2015.
- House, Jonathan M., CPT. “Toward Combined Arms Warfare: A Survey of 20th Century Tactics, Doctrine, and Organization.” Research Survey Number 2, Combat Studies Institute, Fort Leavenworth, KS, August 1984.
- Hui Min Huang, ed. *Autonomy Levels for Unmanned Systems (ALFUS) Framework, Volume I: Terminology*. Gaithersburg, MD: National Institute of Standards and Technology, September 2004. Accessed 30 November 2017. https://www.nist.gov/sites/default/files/documents/el/isd/ks/NISTSP_1011_ver_1-1.pdf.
- . “Autonomy Levels for Unmanned Systems (ALFUS).” Accessed 2 October 2017. <https://www.nist.gov/sites/default/files/documents/el/isd/ks/ALFUS-BG.pdf>.
- Ilachinski, Andrew. *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies*. Arlington, VA: Center for Naval Analyses, January 2017.
- Ivković, Jovan, and Jelena Ivković. “Analysis of the Performance of the New Generation of 32-bit Microcontrollers for IoT and Big Data Application.” 7th International Conference on Information Society and Technology, Kopaonik, Serbia, 2017. Accessed 29 March 2018. https://www.researchgate.net/figure/An-expanded-concept-of-autonomous-AI-enabled-IoT-CPS-system-based-on-the-new-ARM_fig2_316173015.
- John’s Hopkins Applied Physics Laboratory. “NSAD-R-16-045: Joint Concept for Robotic and Autonomous Systems (JCRAS) Baseline Assessment Report Version 2.0.” Briefing prepared for the Joint Staff as an enclosure to task JSJB3, December 2016.
- Joint Chiefs of Staff. *Joint Concept for Robotic and Autonomous Systems (JCRAS)*. Washington, DC: Joint Chiefs of Staff, October 2016.
- . Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Government Printing Office, March 2013.
- Knox, Macgregor, and Williamson Murray, *The Dynamics of Military Revolution 1300-2050*. Cambridge: Cambridge University Press, 2001.
- Lage, Dyndal, Gjert, COL, LtCol Tor Arne Bernsten, and Assistant Professor Sigrid Redse-Johansen. “Autonomous Military Drones: No Longer Science Fiction.” *NATO Review* (August 2017). Accessed 30 September 2017. <http://www.nato.int/docu/review/2017/Also-in-2017/autonomous-military-drones-no-longer-science-fiction/EN/index.htm>.
- Lee, Kai-Fu, and Paul Triolo. “China’s Artificial Intelligence Revolution: Understanding Beijing’s Structural Advantages.” Sinovation Ventures, December 2017.

- Accessed 22 March 2018.
https://www.eurasiagroup.net/files/upload/China_Embraces_AI.pdf.
- Lewis, Larry. *Insights for the Third Offset: Addressing the challenges of autonomy and AI in Military Operations*. Arlington, VA: Center for Naval Analyses, September 2017.
- Manea, Octavian. "The Role of Offset Strategies in Restoring Conventional Deterrence." *Small Wars Journal* (4 January 2018): 6-9. Accessed 22 January 2018.
<http://smallwarsjournal.com/jrnl/art/the-role-of-offset-strategies-in-restoringconventional-deterrence>.
- Martinage, Robert. "Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability." Research, Center for Strategic and Budgetary Assessments, Washington, DC, 2014.
- Maze, Rick, and Gina Cavallaro. "Battling Bureaucracy: The Way Forward Requires Modernizing the Modernization Process." *Army Magazine* (AUSA), 22 February 2018.
- Murray, Williamson. "Armored Warfare: The British, French, and German Experiences." In *Military Innovation in the Interwar Period*, edited by Williamson R. Murray and Allan R. Millett, 6-49. Cambridge: Cambridge University Press, 1996.
- National Research Council. *Autonomous Vehicles in Support of Naval Operations*. Washington, DC: The National Academies Press, 2005.
- National Science and Technology Council. "The National and Artificial Intelligence Research and Development Strategic Plan." *Networking and Information Technology Research and Development Subcommittee*, October 2016.
- Naval Innovation Advisory Council. "Lean Startup Approach to Unmanned Systems." Accessed 28 March 2018. <http://www.secnv.navy.mil/innovation/Pages/Home.aspx>.
- Office of the President of the United States. *The National Security Strategy of the United States of America*. Washington, DC: The White House, December 2017.
- Office of the Under Secretary of Defense (Comptroller) Chief Financial Officer. *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request*. February 2018. Accessed 26 March 2018.
<https://www.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf>.
- Pavluk, Joshua, and August Cole. "From Strategy to Execution: Accelerating the Third Offset." *War on the Rocks*, 9 June 2016. Accessed 20 September 2017.
<https://warontherocks.com/2016/06/from-strategy-to-execution-accelerating-the-third-offset/>.

- Pellerin, Cheryl. "Deputy Secretary: The Third Offset Strategy Bolsters America's Deterrence." DOD News, Defense Media Activity, October 31 2016. Accessed 27 November 2017.
<https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/>.
- Polyakova, Alina, and Spencer P. Boyer. "The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition." Paper, Brookings-Robert Bosch Foundation Transatlantic Initiative, March 2018.
- Potember, Richard. *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*. McLean, VA: MITRE Corporation, 2017.
- Pretz, Kathy. "Three New IEEE Standards for Making Autonomous and Intelligent Systems Safer." The Institute. 2 February 2018. Accessed 30 March 2018.
<http://theinstitute.ieee.org/resources/standards/three-new-ieee-standards-for-making-autonomous-and-intelligent-systems-safer>.
- Roberts, Colin. "Killer Robots: Moral Concerns vs Military Advantages." *The National Interest*, 3 November 2016. Accessed 20 December 2017.
<http://nationalinterest.org/blog/the-buzz/killer-robots-moral-concerns-vs-military-advantages-18277>.
- Scharre, Paul. "Autonomous Weapons and Operational Risk." Center for a New American Security Ethical Autonomy Project, Washington, DC, February 2016.
- Simonite, Tom. "Defense Secretary James Mattis Envis Silicon Valley AI Ascent." *Wired*, 11 August 2017. Accessed 16 April 2018. <https://www.wired.com/story/james-mattis-artificial-intelligence-diux>.
- Smith, Stan, COL. "Pilot or not: Future Vertical Lift needs an aviator in the cockpit." *AUSA*, August 21 2017. Accessed 20 September 2017. www.AUSA.org.
- Stone, Peter, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyan Krishnan, Ece Kamar, Sarit Kraus, Kevin Leyton-Brown, David Parkes, William Press, AnnaLee Saxenian, Julie Shah, Milind Tambe, and Astro Teller. "Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence." Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA, September 2016. Accessed 13 February 2018. <http://ai100.stanford.edu/2016-report>.
- Stroud, Matt. "The Pentagon is Getting Serious About AI Weapons." *The Verge*, 12 April 2018. Accessed 16 April 2018. <https://www.theverge.com/2018/4/12/17229150/pentagon-project-maven-ai-google-war-military>.
- Sullivan, Ian, Matthew Santaspiro, and Luke Shabro. "Mad Scientist Conference: Visualizing Multi-Domain Battle 2030-2050." Conference Sponsors: US Army Training and Doctrine Command and Georgetown University Center for Strategic Studies, 25-26 July 2017.

- The Networking and Information Technology Research and Development Program. *Supplement to the President's Budget for Fiscal Year 2018*. Washington, DC: The White House, October 2017.
- The OECD Science. "Technology and Industry Scoreboard 2017." Accessed 30 April 2018. https://read.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-scoreboard-2017_9789264268821-en#page15.
- Under Secretary of Defense, Acquisition, Technology, and Logistics. *Performance of the Defense Acquisition System: 2016 Annual Report*. Washington, DC: Department of Defense, 2016.
- United States Air Force. *RPA Vector: Vision and Enabling Concepts 2013-2038*. Washington, DC: Government Printing Office, February 2014.
- . *Small Unmanned Aircraft Systems Flight Plan 2016-2036: Bridging the Gap Between Tactical and Strategic*. Washington, DC: Government Printing Office, April 2016.
- United States Air Force Office of the Chief Scientist. *Autonomous Horizons: System Autonomy in the Air Force – A Path to the Future, Vol I: Human-Autonomy Teaming*. Washington, DC: Government Printing Office, June 2015.
- United States Army. *Robotic and Autonomous Systems Strategy*., Fort Eustis, VA: Government Printing Office, March 2017.
- . TRADOC Pamphlet 525-7-15, *The United States Army Concept Capability Plan for Army Aviation Operations 2015-2024*, FT. Eustis, VA: Government Printing Office, September 2008.
- U.S. Congress. House. Future of Artificial Intelligence Act of 2017. 115th Cong., 1st Sess., H.R. 4625, 2017. Accessed 15 March 2018. <https://www.congress.gov/bill/115th-congress/house-bill/4625/text>
- U.S. Congress. Senate. "Testimony Statement of The Honorable Ellen M. Lord Under Secretary of Defense Acquisition, Technology and Logistics Before the Committee on Armed Services United States Senate, 1st Sess., 115th Cong. December 7, 2017.
- Walton, Timothy A. "Securing the Third Offset Strategy: Priorities for the Next Secretary of Defense." *Joint Forces Quarterly* 82 (3rd Quarter July 2016): 6-15. Accessed 15 November 2017. <http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-82/Article/793224/securing-the-third-offset-strategy-priorities-for-the-next-secretary-of-defense/>.
- Wang, Yue. "Will the Future of Artificial Intelligence Look Chinese?" *Forbes*, 6 November 2017. Accessed 2 February 2018. <https://www.forbes.com/sites/ywang/2017/11/06/will-the-future-of-artificial-intelligence-look-chinese/#306dac847fdc>.

- Williams, Andrew P., and Paul Scharre, eds. *Autonomous Systems: Issues for Defence Policymakers*. NATO Communications and Information Agency. Accessed 20 September 2017. <http://www.act.nato.int/>.
- Wong, Ernest W., and Nicholas M. Sambaluk. "Disruptive Innovations to Help Protect against Future Threats." IEEE International Conference on Cyber Conflict, July 6, 2016.
- Work, Bob, Deputy Secretary of Defense. "The Third U.S. Offset Strategy and its Implications for Partners and Allies." Speech, Willard Hotel, Washington, DC, 28 January 2015. Accessed 31 January 2018. <https://www.defense.gov/News/Speeches/Speech-View/Article/606641/the-third-us-offset-strategy-and-its-implications-for-partners-and-allies/>.