University of Pennsylvania
ScholarlyCommons

Wharton Research Scholars

Wharton Undergraduate Research

2020

U.S. Military Innovation In The 21st Century: The Era Of The “Spin-On”

Tyler J. Knox
University of Pennsylvania

Follow this and additional works at: https://repository.upenn.edu/wharton_research_scholars

Part of the Business Law, Public Responsibility, and Ethics Commons, Defense and Security Studies Commons, Government Contracts Commons, Military and Veterans Studies Commons, Military, War, and Peace Commons, National Security Law Commons, Other Public Affairs, Public Policy and Public Administration Commons, Policy Design, Analysis, and Evaluation Commons, President/Executive Department Commons, Public Policy Commons, Science and Technology Law Commons, and the Science and Technology Policy Commons

Knox, Tyler J., "U.S. Military Innovation In The 21st Century: The Era Of The “Spin-On”" (2020). *Wharton Research Scholars*. 194.
https://repository.upenn.edu/wharton_research_scholars/194

This paper is posted at ScholarlyCommons. https://repository.upenn.edu/wharton_research_scholars/194
For more information, please contact repository@pobox.upenn.edu.

U.S. Military Innovation In The 21st Century: The Era Of The “Spin-On”

Abstract

The intersection between the U.S. military and technological innovation, a “military-innovation nexus,” has led to the genesis of key technologies, including nuclear energy, general computing, GPS, and satellite technology from World War II to the present. However, an evolving innovation context in the twenty-first century, including the leadership of the commercial sector in technology innovation and the resurgence of great power competition, has led to doubts about the ability of the Department of Defense to discover and promote the technological innovations of the future. The Third Offset Strategy was formulated in 2014 in response to these concerns: The offset strategy promulgated reforms to bring the Pentagon and the commercial sector closer together while creating alternative contracting mechanisms for streamlined procurement and prototyping. Using defense biometrics and artificial intelligence as case studies of spin-on innovations adopted by the military, this Article seeks to understand the efficacy of the reforms undertaken under the auspices of the Third Offset Strategy to improve the institutional underpinnings of the U.S. innovation system for national security. I argue that the Third Offset Strategy has allowed the Pentagon to more effectively procure, develop, and field commercial technologies in the twenty-first century, and I conclude by proposing modest recommendations for the successful acquisition of spin-on innovations.

Keywords

U.S. military, defense innovation, military innovation, spin-on, technology adoption, Department of Defense, Third Offset Strategy, biometrics, artificial intelligence, great power competition, procurement

Disciplines

Business Law, Public Responsibility, and Ethics | Defense and Security Studies | Government Contracts | Military and Veterans Studies | Military, War, and Peace | National Security Law | Other Public Affairs, Public Policy and Public Administration | Policy Design, Analysis, and Evaluation | President/Executive Department | Public Policy | Science and Technology Law | Science and Technology Policy

This thesis or dissertation is available at ScholarlyCommons: https://repository.upenn.edu/wharton_research_scholars/194

U.S. MILITARY INNOVATION IN THE 21ST CENTURY:

THE ERA OF THE “SPIN-ON”

By

Tyler Knox

An Undergraduate Thesis submitted in partial fulfillment of the requirements for the

WHARTON RESEARCH SCHOLARS

Faculty Advisor:

Sarah E. Light

Associate Professor, Legal Studies & Business Ethics

THE WHARTON SCHOOL, UNIVERSITY OF PENNSYLVANIA

MAY 2020

Abstract

The intersection between the U.S. military and technological innovation, a "military-innovation nexus," has led to the genesis of key technologies, including nuclear energy, general computing, GPS, and satellite technology from World War II to the present. However, an evolving innovation context in the twenty-first century, including the leadership of the commercial sector in technology innovation and the resurgence of great power competition, has led to doubts about the ability of the Department of Defense to discover and promote the technological innovations of the future. The Third Offset Strategy was formulated in 2014 in response to these concerns: The offset strategy promulgated reforms to bring the Pentagon and the commercial sector closer together while creating alternative contracting mechanisms for streamlined procurement and prototyping. Using defense biometrics and artificial intelligence as case studies of spin-on innovations adopted by the military, this Article seeks to understand the efficacy of the reforms undertaken under the auspices of the Third Offset Strategy to improve the institutional underpinnings of the U.S. innovation system for national security. I argue that the Third Offset Strategy has allowed the Pentagon to more effectively procure, develop, and field commercial technologies in the twenty-first century, and I conclude by proposing modest recommendations for the successful acquisition of spin-on innovations.

Keywords

U.S. military innovation, spin-on, technology adoption, Department of Defense, Third Offset Strategy, biometrics, artificial intelligence, great power competition, and procurement

Acknowledgements

I would like to convey my sincere thanks to Professor Sarah Light, my faculty adviser for the honors thesis. My experience serving as a Research Assistant for Professor Light during my junior year at the University of Pennsylvania was the deciding factor that convinced me to pursue this project. Indeed, her work on the Military-Environmental Complex and its link to defense innovation provided the inspiration for the research question explored herein, and my time as an RA also allowed me to build the fundamental research skills necessary to complete this Article. Professor Light's mentorship throughout this experience was invaluable, and her sharp eye has helped to make this project something I am proud of. I would also like to thank the entire community behind Wharton Research Scholars Seminar (WH299): the faculty, staff, and students who supported and inspired me along the way. Lastly, my thanks to all who lent their time to this project or provided me with encouragement and advice over the past year!

Table of Contents

INTRODUCTION

Since World War II, the U.S. military has played a critical, if often overlooked, role in facilitating technological innovation. Tasked with providing the military forces to deter war and to protect the security of the United States, the Department of Defense and its armed services have pioneered new technologies to further American warfighting capabilities and maintain a leading edge over competitor states.[1] From the birth of nuclear energy through the Manhattan Project in the 1940s to funding the construction of ENIAC, the first electronic general-purpose computer in 1946, the U.S. military has often been at the forefront of funding, facilitating, and adopting untested technologies.[2] This connection between the U.S. military and technology innovation, a "military-innovation nexus," has not been accidental. The Department of Defense is firmly embedded in the U.S. national innovation system, including historically close relationships with academic research institutions and partnerships with leading defense technology firms like Boeing and Lockheed Martin. The U.S. national innovation system for defense-related R&D and procurement thus involves the innovation ecosystem of research institutions, firms, and the armed services in a mutually-reinforcing network with the objective of meeting the Pentagon's national security technology needs.[3] However, with consumer technology firms increasingly driving the development of next-generation technologies in a renewed environment of great power competition[4], is the Pentagon still capable of discovering and promoting the technological innovations of the future? In this Article, I will explore and challenge this assumption by describing the changing twenty-first century context of military innovation, analyzing the cases of defense biometrics and artificial intelligence through the lens of the Third Offset Strategy, and proposing modest recommendations for the successful acquisition of spin-on innovations.

Whenever potential foes develop advanced military capabilities, defense leaders have pursued top-down "offset strategies" to foster innovation and secure U.S. superiority.[5] Retroactively referred to as the "First Offset," President Eisenhower set the stage for coordinated military technology innovation with his "New Look" policy in 1956. The "New Look" was a defense doctrine which articulated the use of advanced nuclear weapons to counter the numerical

[1] *See* "About The Department of Defense (DoD)." Accessed March 29, 2020. https://archive.defense.gov/about/.

[2] *See* "ENIAC at Penn Engineering." Accessed March 29, 2020. https://www.seas.upenn.edu/about/history-heritage/eniac/; Steinbock, Dan. "The Erosion of America's Defense Innovation." *American Foreign Policy Interests* 36, no. 6 (November 2, 2014): 366–74. https://doi.org/10.1080/10803920.2014.993251.

[3] Mowery, David C. 2009. "National Security and National Innovation Systems." *The Journal of Technology Transfer* 34 (5): 455-473. doi:10.1007/s10961-008-9100-4.

[4] Lynn (2014); *See* Friedman, Uri. "The New Concept Everyone in Washington Is Talking About." The Atlantic, August 6, 2019. https://www.theatlantic.com/politics/archive/2019/08/what-genesis-great-power-competition/595405/.; Mitchell, A. Wess, and Elbridge A. Colby. "The Age of Great-Power Competition." *Foreign Affairs*, April 16, 2020. https://www.foreignaffairs.com/articles/2019-12-10/age-great-power-competition.

[5] *See* Felter, Joseph. "It's Not Just The Technology: Beyond Offset Strategies." Text. Hoover Institution. Accessed March 30, 2020. https://www.hoover.org/research/its-not-just-technology-beyond-offset-strategies.

superiority of the Soviet Union's standing army.[6] By the Vietnam War, when it became apparent that the Soviet Union had reached nuclear parity with the United States, a "Second Offset" strategy was formulated around a series of promising new technologies including precision-guided missiles, the Global Positioning System (GPS), reconnaissance satellites, and stealth aircraft.[7] Investment in and adoption of these emerging technologies spurred a new period of American military superiority, demonstrated by the overwhelming U.S. victory in the 1990-1991 Gulf War.[8]

However, in the decades following the Gulf War, America's competitor states have actively invested in innovative defense technologies of their own. Russia and China sought to modernize their military capabilities after the startling ease with which the United States defeated Iraqi forces during the Gulf War.[9] They have invested in anti-satellite weapons, hypersonic missiles, and other asymmetric technologies to obviate the threat of America's conventional military strengths. For example, the aircraft carrier, a traditional symbol of U.S. military might, is threatened by Chinese innovation in anti-ship missile technology. Navy strategists believe that China has successfully developed two missiles capable of destroying American carriers: the Dongfeng-21D and the YJ-12.[10] The strategic consequence of this development is the risk that the US aircraft carriers would be rendered useless in the event of a conflict in the South China Sea, for example, due to fears that they would be successfully destroyed. At the same time, while the U.S. has been involved in counter-terrorism initiatives in Iraq and Afghanistan, the focus of the Pentagon's leaders has shifted away from long-term, disruptive innovation to technologies like surveillance drones that are applicable to countering militant insurgencies but are less useful in great power conflict.

The contextual landscape for the U.S. national innovation system has also experienced significant changes since the late twentieth century. We can trace shifts in this innovation landscape as early as the 1970s, when the development of a technology of critical importance to the Pentagon — semiconductors — was being increasingly driven by the market demands of large commercial users.[11] Why was this the case? Defense contractors found their market share of the semiconductor industry slipping from 50% in the mid-1960s to less than 10% by the late 1970s, undermining their ability to entice semiconductor firms to do military work: "We were forced to use decade-old microelectronic technology," complained one Pentagon official, "while

[6] *See* "Dwight D. Eisenhower: Foreign Affairs | Miller Center," October 4, 2016. https://millercenter.org/president/eisenhower/foreign-affairs.

[7] *See* "Who's Afraid of America?" *The Economist*. Accessed March 29, 2020. https://www.economist.com/international/2015/06/13/whos-afraid-of-america.

[8] *See* U.S. Department of Defense. "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence." Accessed March 29, 2020.

[9] Ibid

[10] *See* Broder, Jonathan. "What China's New Missiles Mean for the Future of the Aircraft Carrier." Newsweek, February 16, 2016. https://www.newsweek.com/china-dongfeng-21d-missile-us-aircraft-carrier-427063.

[11] Stowsky, Jay. "From Spin-Off to Spin-On: Redefining the Military's Role in Technology Development." UC Berkeley: *Berkeley Roundtable on the International Economy*, 1992. https://escholarship.org/uc/item/0tf8v3c7.

Atari games were using the latest."[12] Moreover, while major U.S. defense companies like Raytheon and Boeing continue to service the Pentagon's military technology needs, they are no longer the driving engines of innovation they once were. As Lynn (2014) discusses, these firms transitioned from diversified conglomerates with both defense and commercial operations to a handful of defense-only companies.[13] The transition was brought about by industry consolidation in the 1990s after the fall of the Soviet Union contributed to a precipitous decline in U.S. military spending. Today, large commercial technology firms (e.g. Alphabet, Amazon, Apple, etc.) surpass defense contractors in technology R&D spending, as consumer tech firms are pioneering next-generation innovations like artificial intelligence, 5G, and autonomous vehicles. For example, it was initially Google, and not a traditional major defense contractor, which was awarded the Project Maven contract to help the armed services use machine learning to analyze drone footage.[14] These shifts have led the Pentagon to become a net purchaser, rather than the traditional net producer, of next-generation commercial technologies.[15] In other words, the Department of Defense is co-opting civilian-developed consumer technologies for warfighting purposes. This channel is that of the "spin-on," which Stowsky (1992) defines as the diffusion of technology from the civilian to the defense sector.[16]

Faced with the advancing capabilities of "competitor states" and a changing innovation context, American war planners and policymakers are now asking an essential question: Is the United States facing a crisis of innovation? Beginning under Secretary of Defense Chuck Hagel, both Congress and the Department of Defense have pursued institutional and policy reforms to improve the military's tech innovation capabilities. Initially formulated around the ethos of a "Third Offset Strategy*" in 2014, reforms emphasized building relationships with the commercial sector while lowering barriers to doing business.[17] For example, the Defense Innovation Unit (DIU) was founded in 2015 as an investing arm for the Pentagon in potentially strategic emerging spin-on technologies, designed to facilitate partnerships with commercial tech starts in Silicon Valley and other hubs like Austin and Boston.[18] Moreover, statutory authority to accelerate contracting and provide alternative ways to engage with potential commercial partners

[12] Julian, Ken, "Defense Program Pushes Microchip Frontiers," *High Technology*, May 1985, pp. 49-56

[13] *See* William J. III Lynn, "The End of the Military-Industrial Complex: How the Pentagon Is Adapting to Globalization," Foreign Affairs 93, no. 6 (November/December 2014): 104-[vi]

[14] Statt, Nick. "Google Reportedly Leaving Project Maven Military AI Program after 2019." The Verge, June 1, 2018. https://www.theverge.com/2018/6/1/17418406/google-maven-drone-imagery-ai-contract-expire.

[15] Ibid; *See* Director of Defense Research & Engineering. *2008 Department of Defense Research and Engineering: Strategic Basic Research Plan*. U.S. Department of Defense: Office of Defense Research and Engineering, 2008. p.3.

[16] Stowsky (1992)

[17] *Origins of the Third Offset Strategy attributed to the Defense Innovation Initiative announced by Secretary of Defense Chuck Hagel at the 2014 Reagan Defense Forum; *See* Manea, Octavian. "The Third Offset Strategy in Historical Context." Small Wars Journal, 2015. https://smallwarsjournal.com/jrnl/art/the-third-offset-strategy-in-historical-context.
U.S. Department of Defense. "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence."

[18] *See* Hempel, Jessi. "DoD Head Ashton Carter Enlists Silicon Valley to Transform the Military." *Wired*, November 18, 2015. https://www.wired.com/2015/11/secretary-of-defense-ashton-carter/.

was expanded, such as the Other Transaction Authority (OTA) and Commercial Solutions Opening (CSO).[19]

Recent academic literature (Light, 2014; Gholz, 2014) has focused on the role that the Department of Defense can play in mitigating climate change through an innovation strategy. This "Military-Environmental Complex" is founded on the alignment of U.S. national security priorities and environmental policy.[20] Reducing energy demand and encouraging the development of renewable sources are critical to the U.S. warfighting mission.[21] Acknowledging the harmony between these objectives and the preservation of the environment, Light (2014) proposes how the Military-Environmental Complex has the potential to promote innovative green technologies and processes aligned with U.S. national security while providing large-scale commercial support for existing technologies. For example, the Strategic Environmental Research and Development Program (SERDP) is the Department of Defense's environmental science and technology program. The DoD, in partnership with the Department of Energy and the Environmental Protection Agency, invests in basic and applied research for solutions to its environmental challenges. In this context, innovation is arguably both spin-off and spin-on. SERDP funds novel solutions to environmental challenges facing the DoD, which can then be co-opted for civilian applications, but the program also invites contractors to modify (or adapt) existing technologies and processes developed for the commercial economy to national security purposes.[22]

Ultimately, both the "crisis of U.S. military innovation" and the thesis on the "Military-Environmental Complex" motivated the research question that will be explored in this Article, as both must wrestle with the question of whether the Pentagon is still capable of discovering and promoting the technological innovations of the future. I am interested in exploring and challenging this assumption by understanding the changing twenty-first century context of technological innovation. This Article will seek to examine the institutional and policy reforms undertaken under the auspices of the Third Offset Strategy to determine their impact on the ability of the U.S. national innovation system to identify and facilitate the development of novel technologies. Stakeholders — such as the CEO of the National Security Technology Accelerator and a collection of former acquisition officials — have begun to question the efficacy of some of these reforms, including concerns over the Pentagon's focus on tech firms in Silicon Valley and a new "commercialization valley of death" being created by new transaction authorities

[19] *See* Procurement Innovation Resource Center. "Commercial Solutions Opening Guide." GSA.org. U.S. General Services Administration, June 1, 2018. https://www.gsa.gov/cdnstatic/PIRC CSO Guide 62518.pdf.

[20] Light, Sarah E. "The Military-Environmental Complex." Boston College Law Review, May 2014. https://lawdigitalcommons.bc.edu/bclr/vol55/iss3/5.

[21] Brosig, Max, Parker Frawley, Andrew Hill, Molly Jahn, Michael Marsicek, Aubrey Paris, Matthew Rose, Amar Shambaljamts, and Nicole Thomas. "Implications of Climate Change for the U.S. Army." *U.S. Army War College*, July 2019., 52.

[22] *See* Strategic Environmental Research and Development Program. "About SERDP and ESTCP." Accessed March 29, 2020. https://www.serdp-estcp.org/About-SERDP-and-ESTCP.

preventing the fielding of technologies for warfighting after their initial prototyping.[23] Using the conceptual framework of the U.S. national innovation system for defense-related R&D and procurement, I will analyze the successful development, procurement, and fielding of automated biometrics during the War on Terror and explore the Pentagon's pursuit of artificial intelligence for warfighting using a case study methodology.

Research Significance

Understanding the efficacy of the Third Offset Strategy and recent reforms undertaken to improve the institutional underpinnings of the U.S. innovation system for national security is of critical importance to both Congressional policymakers and stakeholders at the Department of Defense responsible for maintaining and promoting military innovation. The Senate Committee on the Armed Forces and the House Armed Services Committee are the principal legislative bodies with jurisdiction over the Department of Defense and the military branches. These committees are responsible for spearheading recent changes in procurement and contracting (e.g. Other Transaction Authority, Commercial Solutions Opening procedure) to more rapidly acquire new technologies for military applications. However, no systematic analysis or research has yet been performed to gauge the impact of these new procedures for defense contracting.

Similarly, existing literature (Christiansson, 2017; Freeman et. al., 2015) remains only inchoate on new Pentagon institutions for "spin-on" innovation, such as the Defense Innovation Unit, which transitioned from an experimental program to a permanent status in 2017. Understanding the effectiveness of DIU and other new units will better inform sound policymaking on U.S. military innovation while gauging the success of existing tactics to better respond to the 21st century innovation context. In a greater sense, both the Department of Defense and Congress are concerned with maintaining U.S. military technology superiority over competitor states like China and Russia, which have been rapidly building up their own asymmetric capabilities. My research will be useful toward a greater understanding of this "crisis of innovation," guiding policy efforts toward maintaining the United States' advantage in military innovation.

Less immediately, the ecosystem of firms constituting the national innovation system also stand to benefit from further reforms to improve the efficiency and ease of DoD procurement, contracting, and investment. There could be an expanded window of opportunity for small businesses and tech startups outside of the traditional Silicon Valley hub to work with the Pentagon, for example. Moreover, a national innovation system more responsive to the twenty-

[23] *See* Gray, Gary, William Riski, and George Schleh. "Accelerating DoD Systems Fielding While Avoiding a New 'Valley of Death'." Federal News Network, July 31, 2019. https://federalnewsnetwork.com/commentary/2019/07/accelerating-dod-systems-fielding-while-avoiding-a-new-valley-of-death/.; Greef, Tim. "The Pentagon Is Losing the Innovation Battle. Here's How to Turn It Around." Defense One, April 30, 2018. https://www.defenseone.com/ideas/2018/04/pentagon-losing-innovation-battle-heres-how-turn-it-around/147821/?oref=d1-related-articl.

first century innovation context could better drive civilian adoption of traditional “spin-off” innovations promoted and funded by the Department of Defense. Lastly, arguments being made for a “Military-Environmental Complex” are founded upon the historical role the Pentagon has played in promoting technological innovations like the internet and GPS; my research will provide a theoretical grounding for these arguments in a 21st century innovation context rather than in the Cold War-era from which these technologies initially sprung.

I. LITERATURE REVIEW

This Article proceeds in six Parts. Part I provides the theoretical framework for this Article. It elaborates on prior literature written on military innovation and presents the concept of the U.S. national innovation system for defense-related R&D and procurement. Part II is an overview of the Third Offset Strategy and recent reforms undertaken to improve defense-related technology acquisition, including new units like the Defense Innovation Unit and contracting vehicles (e.g. Other Transaction Authority). Part III discusses the case study methodology that will be used for this Article, including the rationale behind it for conducting research in the social sciences. Part IV is devoted to the first case, defense biometrics, and charts its historical development as a spin-on innovation during the Global War on Terror. Lessons are drawn with implications for military innovation generally and the Third Offset Strategy. This analysis is then brought forward to the second case — artificial intelligence (AI) — which is discussed in Part V. This Part discusses the Pentagon’s mission to bring AI capabilities to the armed services, defining AI and charting the course of its procurement thus far. Lastly, Part VI concludes the Article with insights gleaned from the stories of defense biometrics and artificial intelligence, and it offers recommendations on how to best proceed with the Third Offset Strategy, especially as it relates to artificial intelligence, the next great technology frontier. These recommendations focus on the dynamics of the spin-on process after contracting: The importance of a guiding framework or ideology for the translation of a new innovation to warfighting, rapid prototyping in a “natural experiment” setting, organizational dynamics promoting experimentation and creativity, and awareness of non-institutional factors like military ethics which can impede technology development.

1.2 The U.S. National Innovation System: A Conceptual Framework

The U.S. military has historically played an important role in identifying, funding, and facilitating the adoption of new technologies. Mowery (2009, 2010) surveys the U.S. national innovation system for defense-related R&D innovation and investment, identifying key industry sectors which the Department of Defense promoted during and after the Cold War.[24] To begin, the “national system of innovation” (NSI) framework for analyzing innovation performance and policy has been a part of the scholarship for analyzing innovation performance and policy for

[24] Mowery (2009)

over 20 years since the first articulation of the concept in Freeman (1987).[25] National innovation systems are defined as the institutions, policies, and actors that affect the creation of knowledge, the innovation processes that translate research into applications (commercial or non-market), and the processes that influence the adoption of innovations.[26] Thus, the alignment between the U.S. national innovation system and national security focuses on the role the Department of Defense has played in the U.S. national innovation system and the policies underlying it. Mowery (2009, 2010)'s framework of a national system for U.S. military innovation, and the potential for both policy-driven and institutional change, will provide the theoretical basis of this Article.

Mowery and Rosenberg (1993)'s paper on the U.S. national innovation system began a discussion of the role of defense spending on R&D and procurement. A later study, Mowery (2009, 2010), discusses three channels from which public investments in defense-related R&D and procurement impact the innovative performance of either industrial sectors or the economy as a whole. The first is most tied to the "R" of R&D; investments in basic and applied research can both support the discovery of new scientific and engineering knowledge and the development of the institutional constituents of national innovation systems (e.g. university-based research). The second channel is the "spin-off" of defense-related innovations for civilian applications (e.g. GPS, the early internet). Procurement is the third channel, where the Department of Defense plays the role of a "lead purchaser" for new technologies. Consequently, supplier firms are able to refine their cost structure and product performance and reliability while contracting with the Pentagon. It is important to note that there can be significant overlap across these three channels in real life, with the Pentagon at times pursuing multiple strategies simultaneously. For example, the U.S. semiconductor industry is often cited as an example of a heavy beneficiary of public investment in both initial R&D for technology development and then procurement upon its maturity, with the military helping to prove the market for an untried technology.[27]

1.3 The Contextual Landscape: Innovation in the 21st Century

How has the contextual landscape for the U.S. national innovation system for defense-related R&D and procurement evolved over the past several decades? One of the most significant changes has been what I will refer to as a "fourth channel." This channel is that of the "spin-on" which Alic et al. (1992), Samuels (1994), and Stowsky (1992) define as the diffusion of technology from the civilian to the defense sector. In other words, military-relevant technologies

[25] *See* Godin, Benoît. "National Innovation System: A Note on the Origins of a Concept," Project on the Intellectual History of Innovation, 2010, 8.

[26] Mowery (2009)

[27] Mowery, David C. "Chapter 29 - Military R&D and Innovation." In *Handbook of the Economics of Innovation*, edited by Bronwyn H. Hall and Nathan Rosenberg, 2:1219–56. Handbook of the Economics of Innovation, Volume 2. North-Holland, 2010. https://doi.org/10.1016/S0169-7218(10)02013-7.

are first developed and refined for commercial applications and later adapted for military-use. This is the inverse of the traditional "spin-off" approach to defense-related R&D, where technology initially developed for defense applications is re-purposed for general market use. When Stowsky (1991) conducted his study, spin-on was only just becoming a part of the defense-related R&D toolkit; it is now a fourth channel in its own right. Indeed, Mowery (2009) touches upon spin-on as "the need [of the military services] to reform both R&D and procurement programs so as to exploit advances in civilian applications more rapidly."[28] It is important to distinguish "spin-on" as its own channel from conventional materials procurement; the latter can be understood as the simple purchase of existing items from the marketplace (e.g. new military hardware, upgrades to existing equipment, weapons and ammunition, etc.) *without* its explicit adaptation for military-specific purposes.[29] Practically, the DoD and lawmakers use *procurement* to generally refer to a specific title within the annual National Defense Authorization Act (NDAA) and defense appropriations legislation, which entitles the Pentagon to make purchases appropriated by Congress.[30]

Lynn (2014) further discusses the contextual changes surrounding the U.S. national innovation system for national security, going as far as to sound "the end of the Military-Industrial Complex."[31] While the true extent of this characterization can be disputed, Lynn (2014) does precisely identify key changes in R&D dynamics that he considers to be a new, "fourth era" for the national innovation system. The "third era" the Department of Defense has now moved beyond was the era of consolidation, in which the industry shifted from diversified conglomerates with their own commercial divisions to a smaller cohort of defense-only firms. In the fourth era, U.S. defense companies (and the Department of Defense, by extension) lag far behind large commercial companies in technology R&D, becoming a net importer for the first time of next-generation commercial technology. It will be extremely difficult, if not impossible, for the major U.S. defense firms to catch up; the Pentagon's R&D budget has fallen as company-funded R&D spending at top U.S. defense firms has declined from 3.5% to 2% of sales from 2000 to 2012, compared to 8% of sales devoted to R&D at peer commercial companies.[32] Lynn (2014) also devotes attention to the imperative of globalizing the national innovation system for national security. Taken together, Lynn (2014) lays the groundwork for the contextual changes facing the national innovation system. Thus, while Lynn's "fourth era" focused on the relationships that constitute the national innovation system for defense, the aforementioned "fourth channel" of the "spin-on" describes a *specific feature* of that system which he predicts

[28] Mowery (2009) touches upon "spin-on" as being a channel worth future study in the years ahead, but he is predominantly concerned with the historical workings of the U.S. NSI for defense (pre-2000)

[29] *See* Peters, Heidi M, and Brendan W McGarry. "Defense Primer: Procurement." *Congressional Research Service,* February 7, 2020, 3.

[30] *"When Congress appropriates money, it provides budget authority—the authority to enter into obligations. Obligations occur when agencies enter into contracts, submit purchase orders, employ personnel, or otherwise legally commit to spending money.": See* Ibid; Schwartz, Moshe, John F Sargent Jr, and Christopher T Mann. "Defense Acquisitions: How and Where DOD Spends Its Contracting Dollars," July 2, 2018, 29.

[31] *See* William J. III Lynn, "The End of the Military-Industrial Complex: How the Pentagon Is Adapting to Globalization," Foreign Affairs

[32] Ibid

will come to increasingly define the "fourth era of innovation:" namely, how specific commercial products and technologies are co-opted and developed for military applications.

2. The third offset strategy and technology acquisition

As previously noted, procurement is one of the three major channels identified by Mowery (2009, 2010) from which public investments in defense-related technologies flow. DoD procurement is a highly complex mechanism in which the armed services acquire the materials and technologies from the private sector to serve its warfighting mission. The Department of Defense defines the acquisition process in three stages: (1) technology development, (2) systems development, and (3) production.[33] This process has traditionally been run according to DoD Directive 5000, the major procurement rules governing how the Pentagon acquires new weapons and technologies.[34] Procurement has been the subject of much attention at both the Pentagon and among policymakers, considering notable technology acquisition failures that wasted billions in appropriated funds (e.g. Future Combat Systems, RAH-66 Comanche).[35]

Acknowledging these contextual changes, the Department of Defense has taken steps to build relationships with the commercial sector while lowering barriers to doing business. The former has often revolved around the formation of new institutions (e.g. Defense Innovation Unit, Defense Innovation Board), while the latter has focused on more efficient and rapid contracting mechanisms (e.g. Other Transaction Authority, Commercial Solutions Opening). The Pentagon's articulated strategy to respond to the 21st century innovation context and bolster American military superiority has been referred to as the Third Offset Strategy. Then-Secretary of Defense Ashton Carter conveyed the motivation behind the Third Offset in remarks made at the CSIS Conference in October 2016: "The current erosion of the U.S. technological advantage derives not from adversaries' numerical superiority or superior volumes of investment, but from the increasing global and commercial nature of the innovation environment and the increasing applicability of commercial technologies to military operations."[36] The Third Offset Strategy, then, is focused on improving the ability of the Pentagon to harness the technological advances in the commercial sector for military applications — to prepare the DoD to capture "spin-on" innovations from the private sector.

One of the key pieces of this strategy has been the Defense Innovation Unit (DIU), the Department of Defense's "scouting program" for spin-on technologies. Founded in 2015, the DIU works to identify private sector technologies that can be co-opted for challenges facing the

[33] *See* Schwartz, Moshe. "Defense Acquisitions: How DoD Acquires Weapon Systems and Recent Efforts to Reform the Process." *Congressional Research Service*, May 23, 2014, 21.

[34] *See* Freedberg, Sydney J. "Choose Your Own Acquisition Adventure: Ellen Lord." Breaking Defense. Breaking Media, December 5, 2019. https://breakingdefense.com/2019/12/choose-your-own-acquisition-adventure-ellen-lord/.

[35] *See* Demotes-Mainard, Julien. "RAH-66 Comanche-The Self-Inflicted Termination: Exploring the Dynamics of Change in Weapons Procurement." *Defense Acquisition University*, April 2012, 27.

[36] *Carter Gives Keynote Address at CSIS Conference*. CSIS Conference, 2016. https://www.youtube.com/watch?v=DsfPaFNELYI.

Defense Department. Defense Innovation Unit offices have been founded in Silicon Valley, Austin, and Boston with the goal of tapping into the projects and relationships being cultivated within the regional innovation hubs. The DIU connects the Pentagon and leading commercial firms through its 3-step "National Security Challenge" pathway. The unit begins with a demand-signal from its DoD partners, who contact the DIU with a "mission-critical challenge" their organization is facing.[37] The DIU will discuss next steps, including appointing a dedicated liaison and funding for prototype solutions. Then, the DIU and DoD partner translate their relevant challenge into an open commercial solicitation (a Commercial Solutions Opening) to receive innovative proposals, and together the DIU and its DoD liaison will award contracts for one or more prototype projects, setting the stage for eventual technology adoption.

Moreover, DoD procurement policy has undergone significant change over the past decade, as reforms behind institutional structure, contracting, etc. have begun to come into effect. In 2009, the Weapon Systems Acquisition Reform Act began the reform process for the procurement of major weapons systems. The legislation created a Pentagon office, the Office of Cost Assessment and Program Evaluation (CAPE), to analyze the cost of new programs and put more emphasis on weapons testing before production. Moreover, armed services commanders were given more say in weapons requirements, a decision expanded upon in the 2016 National Defense Authorization Act, which provided the heads of the armed services with increased control (and greater liability) for weapons programs and their requirements. Of particular importance is a major overhaul of DoD Directive 5000 from a "one-size-fits-all" acquisitions approach to an adaptive acquisition framework with six different pathways: urgent operational needs, middle tier acquisition, major capability acquisition, software acquisition, defense business systems, and acquisition of services. The middle tier acquisition pathway is also of note, allowing DoD program managers to prototype or field mature technologies in an operational environment within five years, a much more rapid procurement process.[38]

The Pentagon has sought statutory authority for accelerated contracting and alternative ways to engage with commercial partners, including the Other Transaction Authority (OTA) and Commercial Solutions Opening (CSO) procedure.[39] These mechanisms are intended for companies and organizations that are conducting research on technology which could have relevant defense applications, but do not have previous or extensive contracting history with the federal government.[40] However, OTAs are also open to traditional contractors and universities which are proposing project work in the spirit of rapid prototyping. Other Transaction Authority

[37] *See* Defense Innovation Unit. "DIU | Work with Us." Accessed April 30, 2020. https://www.diu.mil/work-with-us.

[38] *See* Freedberg, Sydney J. "Choose Your Own Acquisition Adventure: Ellen Lord."

[39] *See* Procurement Innovation Resource Center. "Commercial Solutions Opening Guide."; Miller, Jason. "OTAs Aren't the Only Answer to Satisfy DoD's Need for Procurement Speed." Federal News Network, March 28, 2019. https://federalnewsnetwork.com/acquisition-policy/2019/03/otas-arent-the-only-answer-to-satisfy-dods-need-for-procurement-speed/

[40] *See* DARPA. "Contract Management." Accessed April 30, 2020. https://www.darpa.mil/work-with-us/contract-management#OtherTransaction; Defense Acquisition University. "Other Transaction (OT) Guide | Adaptive Acquisition Framework." Accessed April 30, 2020. https://aaf.dau.edu/aaf/ot-guide/.

comes in two forms: Technology Investment Agreements (TIAs) and Other Transactions for Prototypes (OTs for Prototypes). Technology Investment Agreements are not subject to procurement regulations (e.g. Federal Acquisition Regulation), and are intended as assistance instruments used to “reduce barriers to commercial firm’s participating in defense research, to give the DoD access to the broadest possible technology and industrial base; promote new relationships among performers in both the defense and commercial sectors of that technology and industrial base; and stimulate performers to develop, use, and disseminate improved performance and contracting practices.”[41] The TIA also allows contractors to conduct their accounting using Generally Accepted Accounting Principles (GAAP), rather than the FAR or DFARS cost principles likely to be unfamiliar to a small commercial technology firm. Like TIAs, Other Transactions for Prototypes are also not subject to FAR regulations and allow contract awardees to avoid abiding by the relevant FAR cost accounting standards. The Pentagon has the authority to award OTs for Prototypes for projects where the final deliverable will be a prototype “directly relevant to enhancing the mission effectiveness of military personnel and the supporting platforms, systems, components, or materials proposed to be acquired or developed by the Department of Defense or the armed services.”[42] While these OTs offer awardees significant flexibility on negotiating contract terms and conditions, the one absolute requirement for receiving an OT for Prototyping is the involvement of a small business or nontraditional defense contractor.[43]

While the creation of new procurement pathways seems intuitive to facilitate prototyping and technology adoption, are DoD stakeholders using them? DARPA has placed the Other Transaction Authority (OTA) at the center of its latest AI campaign, the Artificial Intelligence Exploration program. Announced in July 2018, the program envisions high-risk, high-payoff projects demonstrating the feasibility of innovative AI concepts within 18 months of award, a rapid acquisition pipeline reminiscent of commercial speeds. DARPA is employing both types of OTAs: Technology Investment Agreements (TIAs) and Other Transactions for Prototypes (OTs for Prototypes). Similarly, the Defense Innovation Unit utilizes both CSOs and OTAs in its engagement with cutting-edge commercial technology companies. The unit begins with a Commercial Solutions Opening (CSO) process, a competitive solicitation of proposals for potential solutions to problems facing DoD partners, such as the Air Force, Navy, and JAIC. The DIU will respond to CSOs within thirty days to schedule a pitch, and chosen firms will then proceed to contracting using Other Transaction Authority, specifically OTs for Prototypes.[44]

[41] *See* DARPA. “Contract Management.”; 10 U.S.C. § 2371; Part 37 of the DoD Grant and Agreement Regulations (DoDGARs)

[42] *See* 10 U.S.C. § 2371b

[43] See DARPA. “Contract Management.”: *“A non-traditional defense contractor is defined as an entity that is not currently performing or has not performed in the last one-year period any contract for the Department of Defense that is subject to full Cost Accounting Standards (CAS) coverage.”*

[44] *See* Defense Innovation Unit. “DIU | Work with Us.”

The motivation behind granting OTA and CSO authority to acquisition units in the Pentagon — to increase flexibility for prototyping and work with non-traditional contractors — is to improve both traditional procurement and the ability of the DoD to more effectively capture spin-on innovations. Similarly, the creation of the Defense Innovation Unit and other procurement changes (e.g. DoD Directive 5000 reform, CAPE, and the 2016 NDAA) embody the spirit of the Third Offset Strategy to make the DoD more nimble in acquiring cutting-edge technologies being spearheaded by the commercial technology sector. Ultimately, the Third Offset seeks to improve the institutional underpinnings of the national innovation system for national security in order to realize the articulated promise of the Third Offset to secure American military superiority

3. METHODOLOGY

My research uses a case study methodology. Using the case study method allows me to examine the institutional and policy reforms undertaken under the auspices of the Third Offset Strategy to determine their impact on the ability of the U.S. national innovation system to identify and facilitate the development of novel technologies.

The analysis of case studies to answer research-driven questions has extensive precedent in the social sciences, particularly in legal studies. As discussed by Miller (2018), case study research involves the intensive analysis of one or several phenomena, outcomes, or processes; it is aimed at gaining as complete an understanding of the object under study as possible.[45] A case study approach is most applicable to my research considering that I will be examining the institutional and policy underpinnings of the U.S. national innovation system for national security; these underpinnings are necessarily decided by the complex legal regime dictating the Pentagon's procurement and organizational policies, as decided by Congressional and DoD policy makers. Moreover, because legal rules, forms, institutions, and norms are likely to have critical temporal and spatial dimensions, it is difficult to make broad comparisons and generalizations, necessitating a case study analysis. Indeed, because law functions through causal pathways that sometimes overlap, it is challenging to determine discrete and identifiable cause and effects (as you would be able to develop in other fields of research using something like regression analysis, for example). Lastly, Miller (2018) discusses how case studies can be useful in the event of new or low information contexts and skepticism about conventional wisdom, relevant here to both the recency of the Third Offset Strategy reforms and general consensus in Washington that the U.S. is not doing enough to maintain its innovation edge.

I have identified two case studies from which to analyze the national innovation system for defense in the twenty-first century. Both identified case studies share three similar features

[45] Miller, Lisa L. "The Use of Case Studies in Law and Social Science Research." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, October 1, 2018. https://doi.org/10.1146/annurev-lawsocsci-120814-121513.

which makes the insights largely generalizable and useful to study. First, each case study revolves around a singular “technology” or innovation. Second, this innovation will have both clear civilian implications (e.g. GPS for consumer navigation) and be relevant to the Pentagon’s national security mission. Third, to be sure that the technology is born out of the twenty-first century innovation context, case studies are temporally restricted to post-2000 and must be largely born out of the civilian tech economy (a spin-on innovation, essentially).

The first case study is that of defense biometrics.[46] The technology, which involves utilizing physiological characteristics (like a fingerprint) for identification and access control, came into use in the wars in Iraq and Afghanistan. Since 9/11, it has become a key feature of the United States’ counterinsurgency strategy. The case of defense biometrics highlights how a technology untested in military operations became a military innovation with real operational impacts (e.g. detainee management, high-value targeting). It also illuminates the challenges associated with the development, acquisition, and successful use of a new technology on the ground by warfighters. The case study of biometrics will provide key lessons for military innovation in general, and then be analyzed from the perspective of its implications for the reforms of the Third Offset Strategy.

The second case that will be examined in this Article is that of artificial intelligence. Artificial intelligence is a technology that is becoming increasingly important to the U.S. military’s great power strategy in an era of rivals fielding asymmetric strategies to deny the freedom to access (and field forces) in their respective spheres of influence. For example, in July 2017, the Chinese government released a strategy detailing its plan to dominate AI by 2030, and in September 2017, the Russian government similarly announced its intention to pursue AI technological superiority.[47] The ability of the armed services to successfully incorporate AI into warfighting is considered by defense officials and policymakers to be indicative of the future of the nation’s military superiority.

Alongside the similar case profiles — singular "technology" or innovation, civilian applications with national security implications, and a post-2000 "spin-on" innovation — of biometrics and artificial intelligence, the two sets of technologies also share an important quality: They represent the military’s quest to increase the agility at which it operates. In this new “legs race,” the innovative applications of biometrics and AI will not be used (necessarily) to augment the destructive capabilities of the armed services as in a conventional “arms race”, but to achieve the compression of time and space to field more nimble warfighters.[48] I will then apply the

[46] Defense Science Board. “Report of the Defense Science Board Task Force on Defense Biometrics.” Fort Belvoir, VA: Defense Technical Information Center, March 1, 2007. https://doi.org/10.21236/ADA465930.

[47] Sayler, Kelley M. “Artificial Intelligence and National Security.” *Congressional Research Service*, November 2019, 42.

[48] Hom, Andrew. “The New Legs Race: Critical Perspectives on Biometrics in Iraq.” ProQuest, 2008. https://search-proquest-com.proxy.library.upenn.edu/docview/225307851?pq-origsite=summon; Farrell, Raymond. “The New Legs Race.” *Military Review*, 2008. Gale Academic OneFile.

insights gleaned from defense biometrics to that of artificial intelligence, examining how the Third Offset Strategy and reforms to procurement rules either promote or undermine the Pentagon's goal to field this next-generation technology.

4. CASE I: DEFENSE BIOMETRICS

Automated biometrics was a developing consumer technology in the 1990s, with existing applications for access control and identity verification. With the advent of the Global War on Terror after 9/11, identity dominance as a guiding strategy for the federal government and the armed services led to its adoption as a defense technology in the 2000s to 2010s. Part IV defines biometrics, sketches the military application, and charts the timeline in which biometrics became an important tool used by warfighters. This Part then concludes with insights drawn for military innovation and implications for the Third Offset Strategy.

4.1 Defining biometrics

As defined by the International Standards Committee on Biometrics, *biometrics* is the "automated recognition of individuals based on their behavioral and biological characteristics."[49] The U.S. National Science and Technology Council (NSTC) Subcommittee on Biometrics provides a similar, but slightly more general definition: "A measurable biological (anatomical and physiological) and/or behavioral characteristic that can be used for automated recognition."[50] These behavioral and biological characteristics unique to an individual — also known as *biometric characteristics* — are the distinguishing, repeatable *biometric features* which can be extracted for biometric recognition.[51] Examples of biometric characteristics include face topography, facial skin texture, finger topography, iris structure, vein structure of the hand, ridge structure of the palm, retinal pattern, and handwritten signature dynamics.[52] In order to be recognized, an individual must be known or "learned" through an enrollment process, in which their biometric characteristics are recorded by the biometric system.[53] This previously enrolled biometric data can be compared to existing contextual data to a particular individual or for the verification of identity, a process known as *biometric matching*.

[49] International Organization for Standardization. "ISO/IEC 2382-37:2017." ISO.org, February 2017. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/06/66/66693.html.

[50] Defense Science Board. "Report of the Defense Science Board Task Force on Defense Biometrics"

[51] Ibid

[52] Voelz, Glenn. 2016. "Catalysts of Military Innovation: A Case Study of Defense Biometrics." *Defense Acquisition Research Journal: A Publication of the Defense Acquisition University* 23 (2): 176-201. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=114851840&site=ehost-live; Wayman, James L. "Biometrics in Identity Management Systems." *IEEE Security Privacy* 6, no. 2 (March 2008): 30–37. https://doi.org/10.1109/MSP.2008.28.

[53] Wayman (2008)

Biometrics — as defined by the use of behavioral and biological characteristics to identify individuals — has existed for centuries. The established custom of handwritten signatures for legal agreements, commercial exchange, and banking is but one example.[54] The conventional definition of biometrics, and the modern innovation, is that of *automated biometrics*; over the past forty years, a proliferation of biometric technologies have allowed users to automate the once-laborious process of verification. Biometrics have thus expanded into a variety of enterprise applications, with one of the most important being access control. Access control systems recognize individuals whose biometric characteristics are logged into the system.[55] When these users interact with an access control interface, they are granted access to the secured space. Biometrics for access control applications saw initial widespread adoption by both universities for their research laboratories and the nuclear power industry.[56] For example, San Jose State University (SJSU) has been using hand geometry readers since 1993 for controlled, secure access to its Computer and Telecommunications Center.[57] Additionally, by 2003, the entrances to more than half of U.S. nuclear power plants were equipped with biometric hand geometry systems to ensure the safety of internal power generation facilities from potential sabotage or terrorist activity.[58]

Beyond access control, biometrics can supplement existing identity verification measures and achieve secondary firm objectives. The Walt Disney Company has utilized biometric technology — finger geometry — to secure its theme park tickets since June 2005.[59] Upon entry to Disney's parks, the guest presents one fingerprint to be scanned. This fingerprint information is then recorded and matched to their park ticket, allowing Disney to ensure that all tickets can only be used by the individual who first presented it to gain entry. In this way, the Walt Disney Company essentially eliminates the potential ticket reseller market, as a guest cannot "hand off" their ten-day park ticket after two days of use because their biometrics remain tied to it.[60] The firm has received some criticism by privacy advocates (e.g. The Electronic Privacy Information Center, ACLU) for introducing biometric technology to "access roller coasters," with Disney contesting that its system does not store fingerprint images and guests can only present valid photo identification instead.[61]

[54] Zhang, David D. *Automated Biometrics: Technologies and Systems*. Springer Science & Business Media, 2013.

[55] Zhang, David D. *Automated Biometrics: Technologies and Systems*; Wayman (2008)

[56] *See* Government Accountability Office. "Information Security: Challenges in Using Biometrics." GovInfo.gov, September 9, 2003. https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-03-1137T/html/GAOREPORTS-GAO-03-1137T.htm.

[57] Wayman (2008)

[58] *See* Government Accountability Office. "Information Security: Challenges in Using Biometrics."

[59] *See* Wyld, David. "Biometrics at the Disney Gates." SecureIDNews, March 2, 2006. https://www.secureidnews.com/news-item/biometrics-at-the-disney-gates/.

[60] *See* Harmel, Karen, and Laura Spadanuta. "Disney World Scans Fingerprint Details of Park Visitors." The Boston Globe, September 3, 2006. archive.boston.com/news/nation/articles/2006/09/03/disney_world_scans_fingerprint_details_of_park_visitor*s;* Leibacher, Herb. "Disney World, Your Fingerprints, And The US Government." *World of Walt* (blog). Accessed April 5, 2020. https://www.worldofwalt.com/disney-world-fingerprints-us-government.html.

[61] *See* "Privacy Policy | FAQ | Walt Disney World Resort." Accessed April 5, 2020. https://disneyworld.disney.go.com/faq/my-disney-experience/my-magic-plus-privacy/; Harmel, Karen, and Laura Spadanuta. "Disney World Scans Fingerprint Details of Park Visitors."

4.2 The military application: Identity dominance

As previously noted, a collection of biometric characteristics can be compiled on any one individual. Taken together, their biometric data can be combined with biographical and contextual information to create a "pattern of life" profile for individual subjects.[62] Using this profile in conjunction with other biometric data and all-source intelligence, analysts can identify connections among other individuals, correlate their activities, and discern the structure of their social networks. The doctrine of identity dominance stems from this ability to "crack open" human networks through the fusion of biometric data and intelligence gathering: terrorist networks during the United States' War on Terror (2001 - ongoing).[63]

Identity dominance theory was first promulgated in the context of the Global War on Terrorism, the original impetus for the military adoption of biometric technology. In this context, identity dominance translates to the ability of U.S. authorities — from the military to the Department of Homeland Security — to link an enemy combatant or similar national security threat to their previously used identities and past activities (as they relate to terrorism and other crimes).[64] The logic proceeds as follows: The U.S. military must be able to determine whether a person encountered by a warfighter in the field is a friend or foe. The ability of the United States to make a successful determination has direct implications for the success of its mission and the safety of its personnel and allies. Warfighters cannot rely on the individual's given name and "official documents;" these materials can be forged while aliases and cover stories can be concocted at whim. If the military cannot verify an individual's identity with their name and documents, *biometric matching* is the solution to this identity conundrum. Biometric data cannot be falsified, as one cannot simply falsify their finger topography or hand vein structure with any relative ease. In this way, an individual's physiological and behavioral traits provide an indelible link to their identity or presence at a given event. Identity dominance depends on coordinating biometric systems across U.S. authorities: Homeland Security, State Department, FBI, state and local law enforcement, and the intelligence community.[65] In other words, an FBI agent investigating a person of interest in a domestic terror cell could find evidence that the same individual had been detained by Coalition forces in Iraq or Afghanistan some years prior through the registration and verification of their biometrics. On the flip side, a warfighter conducting regular biometric checks at a border crossing could identify and detain an individual who had been previously arrested in the United States (by uploading their data into the FBI's IAFIS database).[66]

[62] Voelz (2016)

[63] *See* Byman, Daniel. "Eighteen Years On: The War on Terror Comes of Age." Combating Terrorism Center at West Point, September 10, 2019. https://ctc.usma.edu/eighteen-years-war-terror-comes-age/.; Woodward, John D. "Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism:" Product Page. U.S. Army, Combined Arms Center, 2005. https://www.rand.org/pubs/reprints/RP1194.html.

[64] Wayman (2008)

[65] Ibid

[66] *See* Public Intelligence. "Identity Dominance: The U.S. Military's Biometric War in Afghanistan," April 21, 2014. https://publicintelligence.net/identity-dominance/.

4.3 A spin-on innovation: Bringing defense biometrics to warfighting

Initial biometrics development largely developed out of university lab research with subsequent translation to the commercial sector. The 1970s saw the adoption of hand geometry biometrics for a number of access control applications. For example, 1974 marked the first deployment of early biometrics technology at the University of Georgia, where hand geometry readers were used for access to its dormitory food service areas.[67] By 1985, one of the first retinal scanning systems was installed for access control purposes at the Naval Postgraduate School. Iris recognition technologies were developed in the 1980s by researchers at the University of Cambridge led by Dr. John Daugman. In the 1990s, research expanded upon the traditional biometric modalities (e.g. fingerprint, hand geometry, iris, and retina) to include the development of voice, signature, palm print, and (early) facial recognition.[68] For example, DARPA sponsored the FacE REcognition Technology (FERET) program from 1993 to 1997 in conjunction with the DoD Counterdrug Technology Development Program Office. The initiative was intended to encourage the development of facial recognition programs, and it both assessed existing prototypes and encouraged its development for commercialization as a non-defense product.[69] 1995 also saw the launch of the first commercial iris product due to a joint project between the Defense Nuclear Agency and Iriscan to create a prototype device.[70] In this way, the Department of Defense was attuned to early developments in automated biometrics, and it played an initial supporting role in supporting technological development and proof-of-concept through the first facial and iris recognition prototypes. This reflects the traditional role of the DoD in sponsoring R&D of potential defense-relevant technologies — the "first channel" of investments in basic and applied research.

Prior to 2001, biometrics was a largely new technology untested for defense purposes, with limited operational application on the battlefield itself. Prior to Iraq and Afghanistan, the Pentagon's use case for biometrics was restricted to physical access control and securing automated systems, similar to existing commercial applications at the time. The Army began a biometric development program in 1999 at the behest of Congress, which granted $10 million to conduct "[an] immediate assessment of biometrics sensors and templates ... to accomplish a more focused and effective information assurance effort."[71] At the same time, Army Chief Information Officer Lieutenant General William H. Campbell commissioned the RAND Corporation to

[67] Chaudhari, Rahul D, Ashok A Pawar, and Rakesh S Deore. "The Historical Development Of Biometric Authentication Techniques: A Recent Overview." *International Journal of Engineering Research* 2, no. 10 (2013): 8.

[68] Asha, S., and C. Chellappan. "Biometrics: An Overview of the Technology, Issues, and Applications." *International Journal of Computer Applications* 39, no. 10 (February 2012). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.736.1587&rep=rep1&type=pdf.

[69] *See* Mayhew, Stephen. "History of Biometrics." Biometric Update, February 1, 2018. https://www.biometricupdate.com/201802/history-of-biometrics-2.

[70] * Defense Nuclear Agency restructured as Defense Threat Reduction Agency; *See* Federal Bureau of Investigation. "Iris Recognition." File. Accessed April 30, 2020. https://www.fbi.gov/file-repository/about-us-cjis-fingerprints_biometrics-biometric-center-of-excellences-iris-recognition.pdf/view.

[71] *See* Public Law No: 106-79, Oct. 25, 1999

review existing commercial biometric applications and assess the sociological, legal, and ethical issues raised by military use of biometrics. The RAND study also considered the establishment of a biometrics center.[72] In July 2000, Public Law 106-246 designated the Secretary of the Army as "… the Executive Agent to lead, consolidate and coordinate all biometrics information assurance programs of the Department of Defense."[73]

The conflicts in Iraq (2001 - 2011) and Afghanistan (2001 - 2020) introduced biometrics to U.S. warfighting capabilities.[74] Military officials were confronted with the inadequacy of prevailing intelligence technologies in waging counterinsurgency operations in dense, sprawling urban environments populated by both militants and innocent civilians. As coalition forces turned to a counter-insurgency strategy after early conventional successes in both theatres, they needed to be able to attain population-level information and specific intelligence for identifying and eliminating insurgents on the field.[75] For American soldiers on the battlefield, the identity crisis was clear: How could you distinguish between an enemy "soldier" and a member of the local population? As previously noted, "identity dominance" emerged as a theory linking this struggle to the wartime needs of U.S. forces in Iraq and Afghanistan. Biometrics offered a promising solution to this identity crisis by identifying actors based not on their stated identity or documentation, but on concrete, unfalsifiable biometric characteristics. In conjunction with contextual data, warfighters could also use biometrics to root out terrorist cells and their networks.[76] It was in this context that the Pentagon came to recognize biometric identification "as a basic warfighting capability."[77] With the defense use case for biometrics in the War on Terror made clear, how would the military go about developing, procuring, and implementing the technology in its warfighting on the ground?

In August 2001, the Pentagon stood-up the Biometrics Fusion Center (BFC), a unit tasked with evaluating and integrating existing commercial biometric identification systems for military and federal agencies. While the U.S. Army held executive authority over the BFC, the unit itself was cross-functional, with officers from the other services and revolving experts from academia and the private sector to the Center to ensure effective coordination across the military. The Biometrics Fusion Center would work with interested parties in the DoD on implementing "quick-look" programs; these projects would be short-term technology and qualification programs designed to "see how biometrics work outside the lab in a small operational

[72] Woodward, John D., Katharine Watkins Webb, Elaine M. Newton, Melissa A. Bradley, and David Rubenson. *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns.* Rand Corporation, 2001.

[73] *See* Biometrics Task Force. "Annual Report FY09." Department of Defense, 2009. https://apps.dtic.mil/dtic/tr/fulltext/u2/a517637.pdf.

[74] * U.S. and Taliban currently in process of ceasing hostilities by concluding a peace treaty; if conditions are met, U.S. and NATO forces will withdraw from the country after 14 months; *See* Council on Foreign Relations. "The Iraq War." Accessed April 10, 2020. https://www.cfr.org/timeline/iraq-war.; Biswas, Soutik. "US and Taliban Sign Deal to End 18-Year Afghan War." *BBC News*, February 29, 2020, sec. Asia. https://www.bbc.com/news/world-asia-51689443.

[75] Voelz (2016); Voelz, *Rise of IWar: Identity, Information, and the Individualization of Modern Warfare*. Simon and Schuster, 2018.

[76] *See* Public Intelligence. "Identity Dominance: The U.S. Military's Biometric War in Afghanistan."

[77] Voelz, Glenn J. *Rise of IWar: Identity, Information, and the Individualization of Modern Warfare*.

environment."[78] Indeed, as Phillip Loranger, director of the Biometrics Fusion Center at the time commented, the Center's evaluation process was necessary because of the "inherent differences between commercial and government application [as] plug-and-play is the exception."[79] With the available commercial technology requiring adaptation for military specifications, the military's adoption of biometrics can be understood as a spin-on innovation, the "fourth channel." Essentially, the BFC was the "hub" for the Pentagon's initial pursuit of biometrics: It provided an institutional basis for the efforts of the armed services to explore the use case of existing commercial biometric technology for their own operational objectives and facilitated the "movement" of both the products and best practices across the services.

The first Biometric Automated Toolset (BAT) was produced by the Battle Command Battle Laboratory by the end of 2001. BAT is a multimodal (fingerprint, iris, and face) system for the collection, matching, and storage of personally identifiable biometric information. Its technical interface is a laptop with plug-in devices for facial, fingerprint and retina capture.[80] Iris recognition relied on a handheld device developed by SecuriMetrics Inc., a startup launched in 1999 in Martinez, California by CEO and Founder Greg Peterson.[81] Neurotechnology — founded as "Neurotechnologija" in 1990 in Vilnius, Lithuania — provided a fingerprint capture and identification engine for BAT's fingerprint recognition capabilities[82]. A facial recognition engine was developed by Lau Technologies[83], which allowed warfighters to take a photo and convert it to a 3D image. The firm was founded in 1990 by Joanna Lau in Littleton, Massachusetts.[84] The device was initially tested in Kosovo, where it was used to identify local workers accessing U.S. installations in the region.[85] As development proceeded from prototype to functioning system in the Balkans, the incorporation of biometrics into U.S. military operations in the Middle East became possible.

BAT was first employed by Joint Special Operations Command in Afghanistan in 2002 for the purpose of enrolling persons of interest detained in the battlefield. A year later, the device had made its way to American forces in Iraq, moving beyond enrollment to interrogation reporting and detainee management at Abu Ghraib.[86] In this way, detainee management became

[78] *See* Keaton, Henry. "Fusion Center Unites Diverse Research Groups." SIGNAL Magazine, November 4, 2004. https://www.afcea.org/content/fusion-center-unites-diverse-research-groups.

[79] Ibid

[80] *See* New Systems Training & Integration Office. "Introduction to Biometrics and Biometric Systems." Biometrics Identity Management Agency, n.d. https://www.tam.usace.army.mil/Portals/53/docs/UDC/Training/Biometrics%20101.pdf.

[81] *See* New Systems Training & Integration Office. "Introduction to Biometrics and Biometric Systems."; Crunchbase profile; https://www.businesswire.com/news/home/20060221005096/en/Viisage-Completes-Acquisition-Leading-Iris-Recognition-Company

[82] *See* Neurotechnology. "About Neurotechnology: Company Information and White Paper." Accessed April 14, 2020. https://www.neurotechnology.com/about.html#shareholders.

[83] Lau Technologies' engine is also employed by the State Department to find duplicate visa applicants, by motor vehicle divisions, by law enforcement agencies, and in other DoD initiatives.

[84] *See* National Defense Industrial Association. "Joanna Lau." Accessed April 14, 2020. https://www.ndia.org/leadership-bios/joanna-lau.

[85] Voelz, Glenn J. *Rise of IWar: Identity, Information, and the Individualization of Modern Warfare*. , https://www.tam.usace.army.mil/Portals/53/docs/UDC/Training/Biometrics%20101.pdf

[86] Voelz, Glenn J. *Rise of IWar: Identity, Information, and the Individualization of Modern Warfare*.

one of the most important applications of biometric technology in the Middle East, improving the previously-dysfunctional handling of detainees, documenting their capture, and identifying and accounting for them all.[87] The Second Battle of Fallujah in 2004 in Fallujah, Anbar Province saw the first, large-scale deployment of biometrics. The city was encircled by Coalition forces, and it was the scene of some of the fiercest urban combat in the entire war. All residents were enrolled into the BAT system to facilitate identification.[88] At the end of 2004, the successful suicide bombing attack of a US base in Mosul led to efforts to deploy biometrics for access control in US military facilities in Iraq and Afghanistan. BISA, the Biometric Identifications System for Access, is the repository for all biometric and biographical information collected from foreign nationals seeking access to a secured U.S. facility.[89] Enrolled individuals are checked against both the Pentagon's Automated Biometric System (ABIS) and the FBI's Integrated Automated Fingerprint Identification System (IAFIS). Those who pass the security checks are granted a biometric ID card.[90] In 2007, the Army's biometric capabilities were expanded with the operational use of the Handheld Interagency Identity Detection Equipment (HIIDE).[91] The handheld device, resembling a large camera, is a tactical extension of BAT, allowing for the collection of iris, fingerprint, and biographical data in the field. The device also communicates with BAT; the latter can export watchlists for on-the-spot identification to HIIDE and can import digital "portfolios" of data on subjects to be uploaded into ABIS.[92]

The biometrics value proposition was validated in April 2011, when 475 prisoners in Kandahar, Afghanistan escaped from the Sarposa prison. Coalition forces were able to apprehend 35 escapees in a matter of days through biometric identification at checkpoints, routine traffic stops, and border crossings.[93] Coalition forces have also worked closely with the Afghani justice system to train security forces and prosecutors on using biometrics as evidence to secure criminal convictions in domestic courts, a tactic which is believed to lead increased conviction records and longer sentences compared to alternative forms of evidence.[94] This has been an advantageous work-around for U.S. forces in the country, limited in their legal ability to detain "unprivileged enemy belligerents" and monitor released individuals for recidivism. Indeed, the Afghan government now employs a biometric database of its own — the Afghan Automated Biometric Identification System (AABIS) — in support of its prosecutorial initiatives for counterterrorism, an example of defense biometrics strengthening local rule of law in

[87] Voelz (2016)

[88] Voelz (2016); Voelz, Glenn J. *Rise of IWar: Identity, Information, and the Individualization of Modern Warfare*; Mansfield-Devine, Steve. "Biometrics at War: The US Military's Need for Identification and Authentication." Biometric Technology Today 2012, no. 5 (May 1, 2012): 5–8. https://doi.org/10.1016/S0969-4765(12)70091-7.

[89] *See* New Systems Training & Integration Office. "Introduction to Biometrics and Biometric Systems."

[90] *See* New Systems Training & Integration Office. "Introduction to Biometrics and Biometric Systems."; Mansfield-Devine (2012)

[91] Mansfield-Devine (2012)

[92] *See* New Systems Training & Integration Office. "Introduction to Biometrics and Biometric Systems."; Mansfield-Devine (2012)

[93] Mansfield-Devine, Steve. "Biometrics at War: The US Military's Need for Identification and Authentication." Biometric Technology Today 2012, no. 5 (May 1, 2012): 5–8. https://doi.org/10.1016/S0969-4765(12)70091-7.

[94] *See* Public Intelligence. "Identity Dominance: The U.S. Military's Biometric War in Afghanistan."

Afghanistan.[95] Lastly, biometrics have been successful in the Army's identity-based targeting of high value combatants. Biometric Identification Analysis Reports (BIAR) provided U.S. forces with biographical information, encounter history, and instructions for identifying, tracking, and targeting persons of interest, such as combatants linked to the construction and use of Improvised Explosive Devices (IEDs) against Coalition forces.[96] From 2007 to 2008 alone, approximately 1,700 insurgents were biometrically linked to existing forensic evidence associated with the manufacture of IEDs.[97]

4.4 Lessons for military innovation

Looking back at the military's two decades of experience with biometrics, it is clear that the technology has reached "operational maturity." Biometrics have become "programs of record" — established procurement programs with their own management offices — for the Army, Navy, and Marine Corps. In 2015, for example, the Navy and Marine Corps kicked off an open contract opportunity for vendors to develop "Identity Dominance System 2.0." The announcement called for expanding existing capabilities to include palm print, vascular, DNA, voice, gait, and hand geometry data collection. The proposal's "wish list" also included the ability to collect information at a greater distance, greater storage capacity, and more rapid processing.[98] By understanding the process in which biometrics were successfully procured, developed, and incorporated into the Army's warfighting, it is possible to arrive at high-level lessons relevant for the acquisition of future military innovations and assess what impact (if any) recent reforms undertaken through the Third Offset Strategy could have had for defense biometrics.

To begin, the story of defense biometrics demonstrates the importance of a clear use case for a new technology in warfighting. An evolving military context in 2001 — the Middle Eastern conflicts against complex foreign insurgencies — presented an ideal application for biometrics, a technology as-yet unknown to the Army. In the early stages of the Global War on Terror, both the growing need to identify and detain insurgents on the battlefield and the insufficiency of existing technological solutions became apparent; falsified documentation could make verifying an individual's identity exceedingly difficult. At the same time, the realm of U.S. government agencies combating foreign terrorism brought to the strategy of "identity dominance" to the fore. Biometrics presented an innovative solution to both identification deficiencies on the ground and an ability to realize identity dominance in the Global War on Terrorism, a powerful dual-use case which drove the military's early interest and commitment to biometrics as a tool for access

[95] *See* Federal Bureau of Investigation. "Mission Afghanistan: Biometrics." Story, April 29, 2011. https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.; Voelz (2016)

[96] Voelz (2016)

[97] Kieffer, Jody, and Kevin Trissell. "DOD Biometrics—Lifting the Veil of Insurgent Identity." Army AL&T, June 2010, 4.

[98] Gallagher, Sean. "Military Looks to Upgrade Its 'Tactical Biometrics' with Identity Dominance System 2." ArsTechnica, October 9, 2015.https://arstechnica.com/information-technology/2015/10/military-looks-to-upgrade-its-tactical-biometrics-with-identity-dominance-system-2/?comments=1.

control, detainee management, high-value targeting, and support for Rule of Law operations. A clear use case for a military innovation may seem to be readily apparent, but it is worth emphasizing this feature; the histories of both civilian and military technology development are littered with examples of technologies pitched as "innovative" and "groundbreaking" that ultimately went nowhere.[99] Their promise remains unrealized in many cases because they failed to solve a pressing problem facing end-users, and without the support of the ultimate constituencies, languished and failed to leave an impact. Defense biometrics, then, illuminates how a compelling use case facilitates early development, procurement, and on-the-ground implementation by aligning the interests of stakeholders.

With the articulation of a clear compelling use case, the DoD must turn to the next step in the innovation journey: obtaining the cutting-edge technological solution. The technology must either be developed internally, or rely on procurement of existing commercial technology, or some combination of these mechanisms. For a spin-on military innovation, the technology *itself* must be mature enough for defense users to imagine potential applications and to realize these applications in the field. Biometrics is an example of a technology that saw early internal development (e.g. Battle Command Battle Laboratory), especially for BAT, but predominantly relied on technology acquisition and adaptation from third-party commercial vendors to develop its biometric modalities. Taken together, defense biometrics highlights how the Pentagon was in a favorable position to benefit from the advancements (and investment) occurring in R&D and prototyping for the identification technologies. Of course, one of the consequences of co-opting an existing commercial technology for defense purposes is sacrificing a market-driving position (i.e. private end-users govern the innovation's development and standards). But still, as defense biometrics demonstrates, the Pentagon is positioned to exploit developments in the commercial sector and adapt to emerging military needs, saving institutional focus and valuable human and financial capital at the same time.[100]

Having elaborated on the significance of a clear use case and the availability of existing commercial technology for a spin-on innovation, both must be validated through prototyping. In other words, a working prototype of a defense innovation must be put out into the hands of warfighters in the field to determine if the technology in question realizes articulated needs. In the case of defense biometrics, the technology benefited from the context of the Iraq and Afghanistan Wars. Defense biometrics was a *wartime innovation*, as opposed to a technological change occurring during peacetime. Some literature — such as Rosen (1991) — consider wartime innovation to be a distinct causal pathway of change from peacetime innovation, as the

[99] *See* for examples of failed consumer product "innovations" (e.g. Google Glass, the Segway): CB Insights Research. "When Corporate Innovation Goes Bad — The 101 Biggest Product Failures Of All Time," April 7, 2020. https://www.cbinsights.com/research/corporate-innovation-product-fails/

[100] Voelz (2016)

former benefits from "the natural experiment" of the battlefield.[101] The demands of war and imperatives for success in the field lower barriers to change while the battlefield provides an opportunity to conduct a natural experiment in which "technology requirements are explicitly articulated in response to challenges posed by an actual adversary rather than a hypothetical one."[102] Usage by warfighters allows technology program leaders to acquire rapid tactical feedback, paving the way for iterative design and improvement in the technology's defense application. At the same time, operational needs become better defined, accelerating R&D, prototyping, and deployment.

The metaphor of the battlefield as a natural experiment clearly reflects that of biometrics, as the technology was put into the field in the form of BAT and then iterated and refined through the challenges of implementation in the Middle East. Phil Scarfo, VP of worldwide sales and marketing for biometrics solutions provider Lumidigm, defines the difference warfighters face in applying their technology as compared to commercial providers: "In many cases, you have one opportunity to collect the information. You can't tolerate that information being lost or of insufficient quality because [of] environmental conditions that aren't ideal… Military users don't want to have to retake or mess around with stuff that may or may not work."[103] Private technology firms like Lumidigm contracting with the Pentagon were able to optimize their solutions to the needs of soldiers on the field through the iterative feedback received from initial prototypes and design more effective technologies in response. For example, Scarfo discusses how his firm recognized the challenge of spoofing: "In military use cases, you're dealing with an uncooperative user who may go to extreme measures to fool the biometric capture system," including contaminants on fingers, sandpaper removal of surface skin, and even surgical alterations of fingerprints.[104] Lumidigm won a Small Business Innovative Research (SBIR) contract in 2006 from the U.S. Air Force Research Laboratory Information Directorate in Rome, NY to respond to this challenge.[105] The SBIR contract was granted to Lumidigm to develop fingerprint sensors that would resist efforts by uncooperative users to fool conventional readers, an example of an iterative solution to an obstacle faced by warfighters in applying existing biometric technology to their identification challenges in the field.

As noted, the Pentagon did not adopt biometrics in an institutional vacuum. The strategic shift toward counterterrorism in the wake of 9/11 encouraged parallel biometric initiatives across the federal government. In September 2001, the federal government had two operating biometric systems: one at the Federal Bureau of Investigation (FBI) and the other at U.S. Immigration and

[101] *See* Rosen, Stephen Peter. *Winning the Next War: Innovation and the Modern Military*. Cornell University Press, 1991. https://www.jstor.org/stable/10.7591/j.ctv2n7k6j.

[102] Voelz (2016)

[103] Mansfield-Devine (2012)

[104] Ibid

[105] *See* Military & Aerospace Electronics. "Briefs | Lumidigm Wins Air Force SBIR Contract for Fingerprint Sensors," February 1, 2005. https://www.militaryaerospace.com/home/article/16708210/briefs.

Naturalization Service (INS).[106] At the same time, the State Department, intelligence agencies, and the Army had smaller research projects and pilot studies under way; these projects would become tied to the mandates of their respective agencies in waging the War on Terror.[107] Of the operational biometric systems in 2001, the FBI's was the most robust. The agency had collected, preserved, classified, and exchanged fingerprint records with other Federal, state, and local law enforcement agencies since 1924. In 1999, the Agency made the pioneering decision to *automate* this process, launching the Integrated Automated Fingerprint Identification System (IAFIS) in 1999.[108] IAFIS introduced large-scale biometrics to the federal government, an example of a successful biometrics system for identity verification for law enforcement purposes. In this way, the Pentagon benefitted from the institutional ecosystem: Parallel biometric initiatives established favorable cross-links, opportunities for knowledge-sharing, and also proof-of-concept for what biometrics could look like: A *military* IAFIS, enrolled with the biometrics of detained insurgents and civilians in Iraq and Afghanistan. Perhaps most of all, a critical mass of interest groups — all pushing for new investments — made the pitch for (and development of) biometrics by the Army all the easier.[109]

Of course, there are also some challenges to such parallel developments of an innovation like biometrics, namely the ability to coordinate communication, interoperability, and matching standards among diverse systems with distinct "data owners." Identity dominance was premised on overcoming institutional differences in these three criteria so threat identity information could be shared across the law enforcement apparatus.[110] According to a 2011 Government Accountability Office (GAO) study, the initial effectiveness of biometrics in the War on Terror was hampered by early disagreements between the DoD, FBI, and Department of Homeland Security in establishing interagency biometric sharing agreements and direct connectivity between their respective databases.[111] The institutional context of the Pentagon's biometrics development highlights both the benefits of agency cross-linkages for an innovation's development and the importance of technology implementation in order to realize its true potential.[112]

While the discussion has so far been oriented around procurement and development, defense biometrics highlights how other concerns — namely ethics — can come into play in

[106] *Agency defunct on March 1, 2003, with functions transferred to U.S. Citizenship and Immigration Services (USCIS), U.S. Immigration and Customs Enforcement (ICE), and U.S. Customs and Border Protection (CBP) in theDepartment of Homeland Security

[107] NSTC Subcommittee on Biometrics and Identity Management. "Biometrics in Government Post-9/11." National Science and Technology Council, August 2008. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/nstc-biometrics-2008.pdf.

[108] *See* Cuthbertson, David, and Jane Horvath. "Privacy Impact Assessment | IAFIS." Page. Federal Bureau of Investigation. Accessed April 14, 2020. https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/iafis.

[109] Voelz (2016)

[110] *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns*. Rand Corporation.

[111] U. S. Government Accountability Office. "Defense Biometrics: DOD Can Better Conform to Standards and Share Biometric Information with Federal Agencies," no. GAO-11-276 (May 2, 2011). https://www.gao.gov/products/GAO-11-276.

[112] Murray, Williamson. *Military Adaptation in War: With Fear of Change*. Cambridge: Cambridge University Press, 2011. doi:10.1017/CBO9781139005241.

deploying a military innovation. In deciding to introduce a new technology to warfighting, both the Pentagon and commercial firms must respond to the ethical implications of this decision. The armed services could be seeking to procure a technology which has largely settled ethical questions in the consumer market or remains controversial still in that setting (e.g. mass data collection).[113] For spin-on innovations more so, the ethical questions of a technology can be particularly distinct from its commercial application. If these questions are not adequately addressed, technology adoption can be stymied by stakeholders in the process, such as employees at various commercial firms themselves protesting work that could assist the U.S. military. Defense biometrics highlights this challenge: As discussed, biometrics in the consumer marketplace traditionally revolved around a cooperative end-user. For example, in access control as a sensitive university research facility, faculty and staff give their explicit consent to enroll their biometric characteristics in the system. There is little question over the ethics of voluntary enrollment in such a system, besides perhaps the importance of safeguarding this personally identifiable data.

In the military domain, however, we must remember that most individuals being enrolled in the DoD's ABIS are *involuntary* users. Whether they are detainees on the battlefield or even Afghani or Iraqi civilians, their autonomy is limited in regard to granting consent to be enrolled in an American-owned and operated biometric database. In other words, what are the ethics of U.S. military forces possessing the biometric data of thousands of foreign nationals, many of them simply innocent men, women, and children? The Pentagon was prescient in this manner, and the 2001 RAND study "Army Biometric Applications" prepared defense officials for the sociological, legal, and ethical issues associated with biometrics and measures the Army might take to mitigate these concerns.[114] Even with guidance and early steps taken in regard to individual privacy rights, governance, and standards for the collection of this personally identifiable information, the Pentagon has received criticism from some privacy and human rights groups over what they consider the military's overreach in its mass collection of biometric data on Afghani and Iraqi civilians, as well as the potential spill-over effects from this (e.g. selective targeting, privacy violations).[115] Despite pointed criticism from some parties, the armed services have not experienced concerted vocal opposition from key stakeholders — The House and Senate Armed Services Committees, the White House, GAO, etc. — that would have the ability to undermine or delay the implementation of the technology.[116] It is likely that the

[113] *See* (for example) Steimer, Sarah. "The Murky Ethics of Data Gathering in a Post-Cambridge Analytica World." American Marketing Association (blog), May 1, 2018. https://www.ama.org/marketing-news/the-murky-ethics-of-data-gathering-in-a-post-cambridge-analytica-world/.

[114] *Army Biometric Applications: Identifying and Addressing Sociocultural Concerns.* Rand Corporation.

[115] *See* Boone, Jon. "US Army Amasses Biometric Data in Afghanistan." The Guardian, October 27, 2010, sec. World news. https://www.theguardian.com/world/2010/oct/27/us-army-biometric-data-afghanistan.; Morrow, Nicola, "Defining Biometrics: Toward a Transnational Ethic of Personal Information" (2017). *International Studies Honors Projects.* 26. http://digitalcommons.macalester.edu/intlstudies_honors/26

[116] *See* Woodward, John D. "Legal Assessment: Legal Concerns Raised by the U.S. Army's Use of Biometrics." In *Army Biometric Applications*. Rand Corporation, 2001. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1237/MR1237.appc.pdf. and *"If today we just started to legislate the standard [of biometrics], I'm not sure we have sufficient expertise to be able to do that. What I would recommend is that Congress should create a task force and have some leading academics and industry experts and non-profit groups help advise*

Pentagon's proactive approach in tackling the ethical implications of biometrics pre-empted potential protestations and allowed for a smoother roll-out of the technology to warfighters.

4.5 Implications for the Third Offset Strategy

The most important lesson learned for military innovation from defense biometrics was for the prototyping of new technologies: If possible, prototypes should be placed in the hands of warfighters in the field as a "natural experiment." The Third Offset Strategy, in seeking to incentivize innovation in both industry and government, has made procurement reform a keystone of its approach to improving the military's ability to adopt and develop cutting-edge technologies for national security needs.[117] Procurement reforms such as Other Transaction Authority and Commercial Solutions Opening have been implemented to accelerate the contracting process and create alternative ways to engage with commercial partners. Similarly, the overhaul of DoD Directive 5000 under Defense Undersecretary Ellen Lord to create different acquisition pathways versus a "one-size-fits-all" acquisitions policy is a step in the right direction toward enabling and making the process of prototype contracting simpler for private firms whose technologies are of interest to Army officials. For example, Directive 5000's new "middle tier acquisition policy" would allow DoD program managers to prototype or field mature technologies in an operational environment within five years, a rapid procurement pathway reflective of the agility in which the Army was able to develop its biometric capabilities: from research in its Battle Command Battle Laboratory in 1999 to a working BAT prototype fielded in the Balkans by 2001.[118]

One cautionary note from relying on the case of defense biometrics for future military innovations concerns the ability of warfighters to prototype in the "natural experiment" setting of the battlefield. Biometrics was uniquely suited for the use case of insurgency tactics and counterterrorism in Iraq and Afghanistan and saw quick operational deployment during those conflicts, but the Pentagon does not envision the Middle East to be the theatre of armed conflict in the years to come. As noted, in a new era of great power conflict, the armed services are seeking to respond to the asymmetric military capabilities of its rival competitor states. In this environment, the feasibility of a "natural experiment" environment — in other words, the battlefield — is likely to be limited at the present *de facto* absence of military hostilities between the United States and great power adversaries. This does not obviate the ability of the Pentagon and its partners to begin the process of procuring, prototyping, and experimenting with new

us on what those standards should be." Rep. Ro Khanna (October 2019) from Boyd, Aaron. "Silicon Valley Rep Calls For Task Force, Legislation on Government Use of Biometrics." Nextgov.com, October 23, 2019. https://www.nextgov.com/emerging-tech/2019/10/silicon-valley-rep-calls-task-force-legislation-government-use-biometrics/160803/.

[117] *See* Hagel, Chuck. "'Defense Innovation Days' Opening Keynote (Southeastern New England Defense Industry Alliance)." U.S. Department of Defense, September 3, 2014: *"It will strengthen our efforts to incentivize innovation in both industry and government – recognizing that there are barriers to innovation, but we have the power to remove many of them."*

[118] *Of course, it would take another six years for the Army to deploy its next-generation biometrics device, HIIDE in 2007: *See* Seffers, George. "U.S. Defense Department Expands Biometrics Technologies, Information Sharing." SIGNAL Magazine, September 28, 2010. https://www.afcea.org/content/us-defense-department-expands-biometrics-technologies-information-sharing.

technologies, but it limits the opportunity to outline technology requirements in response to the challenges posed by an actual opponent, rather than a hypothetical one and to receive tactical feedback from warfighters engaging in the stated operational use case (e.g. Coalition soldiers utilizing BAT to collect the iris, fingerprint, and facial biometric data of detained Iraqi insurgents).

Additionally, biometrics illuminates the importance of deep relationships between the Pentagon and private commercial firms eager to work with defense customers in designing products uniquely suited to their needs. The Army worked successfully with what were then largely small biometric technology startups untested in the defense arena.[119] Some firms, like Lau Technologies which provided a facial recognition engine to the DoD, did have prior defense contracting experience, but on the whole, most of the vendors had seen their first products designed for commercial vendors.[120] In this way, the Third Offset Strategy has emphasized outreach to non-traditional (non-defense) firms, smaller enterprises, and tapping into the innovation hubs of Silicon Valley, Boston, and Austin. The Defense Innovation Unit perhaps embodies this desire to extend the Pentagon's relationships with cutting-edge technology firms with its exclusive focus on fielding and scaling commercial technology across the U.S. military at commercial speeds.[121] Indeed, alternative modes of contracting (Other Transaction Authority/Commercial Solutions Opening) are also beneficial beyond increasing the speed of prototyping but also enabling the Pentagon to work with (and get money in the hands of) small enterprises who may be looking to secure early backing, capital, and proof-of-concept for future R&D and success in the commercial market, a sequence of events which is mutually beneficial for the DoD and the innovative firms it seeks to work with. Lastly, while the Third Offset Strategy has not explicitly touched upon the Small Business Innovation Research (SBIR) grant program, its use by the Air Force for Lumidigm to develop spoofing-proof sensor technology offers an example of how the program remains highly relevant to allow small, high-tech U.S. businesses and academia the opportunity to provide innovative research and development solutions in response to critical DoD needs.[122]

Lastly, the case of defense biometrics highlights what has been outside the scope of the Third Offset Strategy and procurement reform: non-institutional characteristics of defense innovation. As discussed for defense biometrics, these include both the ethical challenges of fielding a new military technology and the imperative of developing the needed human capital to operate innovations effectively on the battlefield. Indeed, the challenge of also articulating a clear doctrine for an innovation exists, as biometrics had to be framed in terms of the evolving

[119] Now most of the firms mentioned herein no longer exist in independent form; most have been acquired by larger players, a sign of the industry's now maturity from its nascency during the development of defense biometrics

[120] *See* National Defense Industrial Association. "Joanna Lau."

[121] *See* DIU.mil. "Defense Innovation Unit | About Us." Accessed April 25, 2020. https://www.diu.mil/about.

[122] Army Small Business Innovation Research. "Army | SBIR." Accessed April 26, 2020. https://www.armysbir.army.mil; Air Force Small Business Innovation Research. "Air Force | SBIR STTR." Accessed April 26, 2020.

way in which the Army was waging war in the Middle East at the time. New innovations, if they promise to disrupt the traditional way of waging conflict, will have to be coherent with either existing Army methods or align with the Pentagon's future strategies for the warfare of the future.

5. CASE II: ARTIFICIAL INTELLIGENCE

Artificial intelligence is expected to define the future technological superiority of the U.S. military and how the armed services conduct warfare in the twenty-first century. AI technologies have experienced significant growth and development among both leading commercial technology firms (e.g. Google, Amazon, Microsoft) and leading-edge startups. These innovations are necessarily dual-use, and the Pentagon has devoted much of its acquisition processes and reforms to promote the adoption of AI algorithms. Part V defines artificial intelligence, explores the potential military applications of AI, and charts out the steps taken thus far to acquire and promote AI capabilities in the DoD. This Part then concludes with a discussion of Project Maven as its "first AI experiment," and implications for future AI procurement.

5.1 Defining artificial intelligence

Artificial intelligence (AI) is exceedingly difficult to define. Unlike automated biometrics, there exists no agreed-upon definition issued by a standards body like the International Organization for Standardization (ISO).[123] The academic literature on the subject of AI is equally inchoate, with most studies acknowledging that no commonly accepted definition yet exists.[124] Stanford University's One Hundred Year Study on Artificial Intelligence argues that Nilsson (2009) provides one of the more useful definitions of AI: "Artificial intelligence is that activity devoted to making machines intelligent, and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment."[125] On the other hand, the Brookings Institution in its *A Blueprint for the Future of AI* (2018-2019) lays out a three-tiered definition for artificial intelligence: intentionality, intelligence, and adaptability.[126] Intentionality refers to the design of AI algorithms by human engineers to *make* decisions, often using real-time data. Artificial intelligence is "intelligent" in the sense that its data inputs enable decision-making informed by *something*, often either machine learning or data analytics. The third quality, adaptability, underlies the unique ability of AI programs to learn and adapt as

[123] *See* International Organization for Standardization. "ISO/IEC CD 22989." ISO.org, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/42/74296.html: Currently under development with U.S. representatives involved in formulating an ISO definition and standards for AI

[124] Sayler, Kelley M. "Artificial Intelligence and National Security."; Wang, Pei. "On Defining Artificial Intelligence." ResearchGate, January 2019. http://dx.doi.org/10.2478/jagi-2019-0002.

[125] *See* Nilsson, Nils J. *The Quest for Artificial Intelligence*. Cambridge University Press, 2009.; Stone, Peter, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyanakrishnan, Ece Kamar, Sarit Kraus, Kevin Leyton-Brown, David Parkes, William Press, AnnaLee Saxenian, Julie Shah, Milind Tambe, and Astro Teller. "2016 Report | One Hundred Year Study on Artificial Intelligence (AI100)." Stanford University, September 6, 2016. https://ai100.stanford.edu/2016-report.

[126] West, Darrell M. "What Is Artificial Intelligence?" *Brookings* (blog), October 4, 2018. https://www.brookings.edu/research/what-is-artificial-intelligence/.

information is compiled and decisions are made. The definitions of Nilsson (2009) and Brookings share an emphasis on the unique value proposition of AI programs to “make machines intelligent” through data inputs that allow it to adapt (and improve) its performance over time in a changing environment. Taken together, these definitions also convey that while AI may be a singular “set” of innovations, it is not exactly a unitary “technology” in the sense of a new nuclear missile or satellite. In this way, artificial intelligence is akin to defense biometrics, considering both are ways of classifying the common techniques and methods behind the wide range of innovative applications they promise (e.g. iris recognition and hand geometry are both technologies understood to be “defense biometrics”).

For the purposes of this Article, I will rely on the Department of Defense’s working definition of artificial intelligence. The White House, despite the articulation of several executive orders and initiatives around AI, has also side-stepped issuing a singular definition to unify the federal understanding of the technology.[127] The origins of the Pentagon’s definition for AI is best captured in FY2019 National Defense Authorization Act (NDAA).[128] According to the FY2019 NDAA, AI can be understood as any of the following:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks
4. A set of techniques, including machine learning that is designed to approximate a cognitive task
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.

.

The National Defense Authorization Act does not stake out a singular definition for AI, instead offering several potential understandings of the concept. However, the Pentagon’s official Artificial Intelligence Strategy, released on February 12, 2019, provides a more succinct definition of AI that will guide all relevant initiatives across the armed services. For the purposes of my analysis, I will rely on this simplified definition of AI adopted by the military: The ability of machines to perform tasks that normally require human intelligence — for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or

[127] *See* Office of Science and Technology Policy. “Accelerating America’s Leadership in Artificial Intelligence.” The White House, February 11, 2019. https://www.whitehouse.gov/articles/accelerating-americas-leadership-in-artificial-intelligence/.

[128] Public Law No: 115-232 (H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019)

taking action — whether digitally or as the smart software behind autonomous physical systems.[129]

Artificial intelligence is not "new," per se, if traced to the early musings on "thinking machines." Alan Turing is often credited with the origin of artificial intelligence as a concept for a family of complex machines that could reason at the level of a human being.[130] The "Turing Test" evaluates the ability of computers to complete reasoning puzzles as well as humans such that they may be considered "thinking" in an autonomous manner.[131] "Artificial intelligence" as a term was first promulgated by researcher John McCarthy to denote machines capable of thinking autonomously.[132] With this early corpus of research, the contemporary resurgence of interest in AI — and its innovative (and disruptive[133]) applications across industries — arose in the 2010s due to the convergence of three developments: the rise of "big data" sources, improvements to machine learning[134], and increases in computer processing capabilities.[135] Existing artificial technology is that of "artificial narrow intelligence" (ANI), also known as "Weak" AI. Narrow AI refers to algorithms designed to perform a single task, whether it be image recognition, game playing, or even checking the weather.[136] ANI systems operate within a predetermined, pre-defined range, and they are not conscious or sentient in the form of human thinking. They attend to a given task in real-time (e.g. writing news reports), pulling information from a specific data set.[137]

The commercial applications of AI are varied, with innovative applications in industries as diverse as education, healthcare, and consumer technology. In the midst of the covid-19 pandemic, artificial intelligence is being deployed by both private firms and researchers in the healthcare industry in the quest to identify potential therapies for the virus. In February 2020, researchers from the AI drug discovery company BenevolentAI and Imperial College London published a paper in the medical journal *Lancet* describing a potential drug, baricitinib, which

[129] *See* Department of Defense. "Summary of DoD AI Strategy," February 12, 2019. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.; Horowitz, Michael. "Artificial Intelligence, International Competition, and the Balance of Power." Texas National Security Review, May 15, 2018. https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/:
"Autonomous systems have more latitude and are programmed, within constraints, to achieve goals, optimizing along a set of parameters."

[130] *See* West, Darrell M. "What Is Artificial Intelligence?" *Brookings* (blog), October 4, 2018. https://www.brookings.edu/research/what-is-artificial-intelligence/.

[131] *See* University of Toronto. "Artificial Intelligence | The Turing Test," 1999. http://www2.psych.utoronto.ca/users/reingold/courses/ai/turing.html.

[132] *See* Shubhendu, Shukla, and J. Frank Vijay. "Applicability of Artificial Intelligence in Different Fields of Life," 2013.

[133] Christensen, Clayton M, Michael Raynor, and Rory McDonald. "What Is Disruptive Innovation?," Harvard Business Review. December 2015, 11.

[134] *See* Meserole, Chris. "What Is Machine Learning?" *Brookings* (blog), October 4, 2018. https://www.brookings.edu/research/what-is-machine-learning/.

[135] Sayler, Kelley M. "Artificial Intelligence and National Security."

[136] *See* Jajal, Tannya D. "Distinguishing between Narrow AI, General AI and Super AI." Medium, February 13, 2020. https://medium.com/@tjajal/distinguishing-between-narrow-ai-general-ai-and-super-ai-a4bc44172e22; Sayler, Kelley M. "Artificial Intelligence and National Security."

[137] *See* Jajal, Tannya D. "Distinguishing between Narrow AI, General AI and Super AI."

could be efficacious against covid-19.[138] In order to identify baricitinib, the authors utilized BenevolentAI's proprietary algorithms, which were connected to molecular structure data on covid-19 to biomedical information about relevant receptors and diseases to determine potential drug targets. While further testing will be necessary to determine baricitinib's therapeutic efficacy, Benevolent AI-ICL's joint AI effort demonstrates one of the primary motivations for artificial intelligence solutions: increasing agility while conserving time and resources.[139] An interesting consumer technology application of AI is Duolingo, a Pittsburgh-based startup offering a language-learning website and mobile app. Duolingo provides its foreign language training using Automatic Speech Recognition (ASR) and Natural Language Processing (NLP) techniques to recognize language errors and help users correct them, all based on AI algorithmic technology.[140] Their AI capabilities rely on deep learning, a subset of AI and machine learning which uses neural networks to model the brain's behavior to analyze data and draw intelligent predictions.[141] Using these deep learning algorithms, Duolingo can analyze log data from its 300+ million active users, and then predict the likelihood that given users will get the answer correct, providing personalization for the language app's learning tests and content.[142]

These commercial applications demonstrate the versatility of existing "narrow" AI technologies, whether it be for drawing predictive models or natural language processing. More generally, artificial intelligence promises to increase the speed at which tasks are accomplished by supplanting previous human cognition — and the valuable time and effort it requires — with autonomous analysis. Moreover, artificial intelligence is considered to be a "relatively transparent enabling capability;" in other words, one may be utilizing a particular product or software and not even be aware of the AI algorithms working underneath the hood.[143] Indeed, Duolingo's users are not privy to the company's proprietary predictive technologies helping to personalize the language learning experience. While they may be running "in the background," the extraordinary value they present to the firm and its customers alike is not. Professor Michael Horowitz, associate professor of political science at the University of Pennsylvania, compares AI to an internal combustion engine or electricity, an enabling technology with a multitude of applications differing from, and broader than, any missile, submarine, or tank.[144] In this way, AI

[138] Richardson, Peter, Ivan Griffin, Catherine Tucker, Dan Smith, Olly Oechsle, Anne Phelan, and Justin Stebbing. "Baricitinib as Potential Treatment for 2019-NCoV Acute Respiratory Disease." *The Lancet* 395, no. 10223 (February 15, 2020): e30–31. https://doi.org/10.1016/S0140-6736(20)30304-4.

[139] *See* Lemonick, Sam. "Two Groups Use Artificial Intelligence to Find Compounds That Could Fight the Novel Coronavirus." Chemical & Engineering News, February 4, 2020. https://cen.acs.org/physical-chemistry/computational-chemistry/Artificial-intelligence-finds-drug-that-could-fight-Wuhan-coronavirus/98/i6: *"The use of AI to augment human capacity, to address a pressing public health concern using existing data without re-deploying a full team, should be a boon to researchers."*

[140] *See* "2016 Report | One Hundred Year Study on Artificial Intelligence (AI100)." Stanford University, September 6, 2016.

[141] *See* Peranandam, Cynthya. "AI Helps Duolingo Personalize Language Learning." Wired. Accessed April 27, 2020. https://www.wired.com/brandlab/2018/12/ai-helps-duolingo-personalize-language-learning

[142] *See* Peranandam, Cynthya. "AI Helps Duolingo Personalize Language Learning."; Sawers, Paul. "How Duolingo Is Using AI to Humanize Virtual Language Lessons." *VentureBeat* (blog), July 5, 2019. https://venturebeat.com/2019/07/05/how-duolingo-is-using-ai-to-humanize-virtual-language-lessons/.

[143] Sayler, Kelley M. "Artificial Intelligence and National Security."

[144] Horowitz, Michael. "Artificial Intelligence, International Competition, and the Balance of Power."

procurement is unlikely to result in countable objects, but algorithms will be purchased and incorporated into larger existing or newly fabricated systems: "We will not buy AI. It will be used to solve problems, and there will be an expectation that AI will be infused in most things we do."[145]

5.2 Ongoing and proposed military applications: Speed and lethality

At the most basic level, the overarching application of AI for the military is quite simple: to increase its speed and agility.[146] Lieutenant General Jack Shanahan, Director of DoD Joint Artificial Intelligence Center, has placed this objective at the center of the Pentagon's AI strategy: "[We] envision an American military that uses AI to move much faster."[147] Defense officials believe that the speed of warfare is rapidly increasing, considering the proliferation of hypersonic weapons and the growing use of cyber-attacks by American competitor states.[148] Of course, speed in-and-of itself can be a certain advantage on and off the battlefield, whether it be to catch an adversary unawares or to use speed as defense.[149] This is the promise of winning "the legs race:" to achieve the compression of time and space to field more nimble warfighters.[150] Of course, the Pentagon is not only seeking to increase the speed of its weapons, but also to improve military decision-making and general efficiency.

For example, intelligence and surveillance, logistics, and command and control are all military domains which stand to benefit from AI innovation. The Pentagon is perhaps the most "far-along" in the sense of imagining, developing, and deploying AI solutions to its intelligence and surveillance activities. This can be attributed to the large quantity of data sets available for analysis, whether it be from human-gathering intelligence, satellite imagery, or drone reconnaissance.[151] AI could be used to augment or replace existing human analysis of military intelligence, opening up the human capital previously devoted to manually searching through video to other tasks, likely more cognitively-intense decision making.[152] The DoD's Project Maven, launched in 2017, is an ongoing AI initiative which is exploring this potential use case through the application of AI to the analysis of aerial drone footage in the Middle East, to be discussed herein. Logistics is another realm of military operations which could stand to benefit

[145] Sayler, Kelley M. "Artificial Intelligence and National Security."

[146] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech." Wired, February 12, 2019. https://www.wired.com/story/pentagon-doubles-down-ai-wants-help-big-tech/.

[147] *See* Groll, Elias. "The Pentagon's AI Chief Prepares for Battle." Wired, December 18, 2019. https://www.wired.com/story/pentagon-ai-chief-prepares-for-battle/.

[148] Horowitz, Michael. "Artificial Intelligence, International Competition, and the Balance of Power."

[149] *See* Boyle, Vern. "The Need for Speed: How America's next Military Advantage Relies on Nimbler Cybersecurity." Christian Science Monitor, September 17, 2015. https://www.csmonitor.com/World/Passcode/2015/0917/The-need-for-speed-How-America-s-next-military-advantage-relies-on-nimbler-cybersecurity: *"A protection strategy based on speed can shift the advantage toward the defender and defeat many automated attack processes. Modern tools can be applied in new ways such that defenders can negate the temporal advantage of the attacker."*

[150] Hom, Andrew. "The New Legs Race: Critical Perspectives on Biometrics in Iraq."

[151] Sayler, Kelley M. "Artificial Intelligence and National Security."

[152] *See* Groll, Elias. "The Pentagon's AI Chief Prepares for Battle."; Sayler, Kelley M. "Artificial Intelligence and National Security."

from AI solutions. Predictive algorithms could be designed to alert support crews that a vehicle needs service, drawing on real-time sensor data and other in-vehicle systems for probabilistic analysis. This use case is already being driven by the Air Force for F-35 repair decisions, as opposed to relying on user recognition of a malfunctioning jet or a standardized fleet maintenance schedule.[153] AI could also be used to supplement human analysis of cost savings for army shipping and acquisition logistics, currently estimated to save the Army approximately $100 million a year in shipping request optimization alone.[154] The Army is pursuing this through its Logistics Support Activity's contract with IBM Watson, and officials hope to extend the ability of its shipping request analysis from 10% capacity with human analysts to 100% capacity with the assistance of AI.[155]

The implementation of AI solutions for command and control could perhaps prove to be the most consequential for military decision-making. Currently, human officers conceive and present potential weapons options to deploy against an adversary after analyzing battlefield conditions in real-time. But defense officials like AI Chief Shanahan believe that in the future, computers could speed up this process, providing "recommendations as fast as possible to a human to make decisions about employing weapons."[156] Artificial intelligence would not replace human cognition, as the technologies would only offer potential options to officers, but it could enable faster adaptation to complex events, improving the quality and speed of wartime decision making.[157] In the near-term, the armed forces are looking at the potential of AI to "unify" its disparate operations into a single dashboard. In other words, a "common operating picture" could be created by synthesizing data from sensors across air, space, cyberspace, sea, and land domains, providing a single display of friendly and enemy forces for military decision makers.[158] The Air Force is currently working on the concept development for a Multi-Domain Command and Control platform that would create such a dashboard, in collaboration with Lockheed Martin, Harris, and several AI startups.[159] These varying applications of defense AI all promise to make the armed services more nimble, supplementing or improving human-assigned tasks while allowing warfighters to devote their precious cognitive skills to more mission-critical objectives. At the same time, a more agile military can also result in significant cost savings, with scarce financial resources devoted to other needs.

[153] Sayler, Kelley M. "Artificial Intelligence and National Security."; Weisgerber, Marcus. "Defense Firms to Air Force: Want Your Planes' Data? Pay Up." Defense One, September 19, 2017. https://www.defenseone.com/technology/2017/09/military-planes-predictive-maintenance-technology/141133/.

[154] *See* Adam Stone, "Army Logistics Integrating New AI, Cloud Capabilities," September 7, 2017, https://www.c4isrnet.com/home/2017/09/07/army-logistics-integrating-new-ai-cloud-capabilities/.

[155] Sayler, Kelley M. "Artificial Intelligence and National Security."

[156] *See* Groll, Elias. "The Pentagon's AI Chief Prepares for Battle."

[157] Sayler, Kelley M. "Artificial Intelligence and National Security."

[158] Ibid

[159] *See* Pomerleau, Mark. "How Industry's Helping the US Air Force with Multi-Domain Command and Control." DefenseNews, September 25, 2017. https://www.defensenews.com/c2-comms/2017/09/25/industry-pitches-in-to-help-air-force-with-multi-domain-command-and-control/.

Artificial intelligence could also be used to enhance the lethality of the armed services and even reduce casualties among its personnel. As noted, AI is principally imagined increasing the speed of military decision-making, which can translate to greater effectiveness on the battlefield.[160] Semiautonomous and autonomous vehicles are also developing technologies with artificial intelligence critical to realizing the full potential of their defense use cases. For example, the Army is in the process of testing an automated gun turret, the Navy is pursuing unmanned surface vessels for its "Ghost Fleet" concept, and the Air Force has advanced beyond phase-2 tests for its "Loyal Wingman" program.[161] These concepts all rely on AI to perceive the environment, avoid obstacles, communicate with other vehicles and defense systems, and plan navigation. These autonomous systems could, in theory, lower the risks for warfighters by relying on these vehicles to enter particular combat zones or scenarios and also designing them to "support" human personnel in their missions.[162] The Loyal Wingman program, for instance, pairs an uninhabited, older-generation fighter jet (e.g. F-16) with a human-piloted F-35 or F-22. With AI, the Air Force imagines enabling the "loyal wingman" to perform tasks in conjunction with its flight lead as a complementary asset or serve as a decoy to protect the crewed system from offensive air defenses.[163] Lastly, lethal autonomous weapons systems (LAWS) are "a special class of weapon systems that use sensor suites and computer algorithms to independently identify a target and employ an onboard weapon system to engage and destroy the target without manual human control of the system."[164] These systems remain theoretical applications of AI, as the armed services do not currently field any LAWS. However, the military remains open to conducting research into autonomous weapons systems, as defense officials believe that the military must respond to ongoing development of such systems by potential U.S. adversaries.[165] Considering the uncertainty around the U.S. development of LAWS, and a lack of consensus around the future trajectory of artificial intelligence itself, experts believe that the applications of AI sketched out herein remain tentative.[166]

[160] *See* Groll, Elias. "The Pentagon's AI Chief Prepares for Battle.": *"In war zones around the world, American military forces request fire support. By radioing coordinates to a howitzer miles away, infantrymen can deliver the awful ruin of a 155-mm artillery shell on opposing forces. If defense officials in Washington have their way, artificial intelligence is about to make that process a whole lot faster."*

[161] *See* Jr, Sydney J. Freedberg. "Army To Test ATLAS Robotic Gun: Bruce Jette." *Breaking Defense* (blog), June 5, 2019. https://breakingdefense.com/2019/06/army-to-test-robotic-gun-bruce-jette/.; Axe, David. "The Air Force's Mysterious XQ-58 Valkyrie Drone Is Almost Ready." Text. The National Interest. The Center for the National Interest, November 4, 2019. https://nationalinterest.org/blog/buzz/air-forces-mysterious-xq-58-valkyrie-drone-almost-ready-93401; LaGrone, Sam. "Navy Wants 10-Ship Unmanned 'Ghost Fleet' to Supplement Manned Force." USNI News, March 13, 2019. https://news.usni.org/2019/03/13/navy-wants-ten-ship-3b-unmanned-experimental-ghost-fleet.

[162] Horowitz, Michael. "Artificial Intelligence, International Competition, and the Balance of Power."; Maneuver, Aviation, and Soldier Division Army Capabilities Integration Center. "The U.S. Army Robotic and Autonomous Systems Strategy." U.S. Army Training and Doctrine Command, March 2017. https://www.tradoc.army.mil/Portals/14/Documents/RAS_Strategy.pdf.

[163] *See* Stevenson, Beth. "'Loyal Wingman' Part of the Future of Air Combat." Aviation International News, June 13, 2019. https://www.ainonline.com/aviation-news/defense/2019-06-13/loyal-wingman-part-future-air-combat; Drew, James. "Pentagon Touts 'Loyal Wingman' for Combat Jets." Flight Global, March 30, 2016. https://www.flightglobal.com/pentagon-touts-loyal-wingman-for-combat-jets/120140.article.

[164] *See* Sayler, Kelley M. "Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems." *Congressional Research Service*, In Focus, December 19, 2019, 3.

[165] Sayler, Kelley M. "Artificial Intelligence and National Security."; Vergun, David. "Esper Makes Case That China Is a Growing Threat to Europe." U.S. Department of Defense, February 15, 2020. https://www.defense.gov/Explore/News/Article/Article/2085573/esper-makes-case-that-china-is-a-growing-threat-to-europe/.

[166] For example, a more advanced application of AI in warfare could involve an autonomous system which could better protect a base or city from a missile saturation attack, which would overwhelm inherent human cognitive abilities and instincts, an "escape" from the limitations of

5.3 An (ongoing) spin-on innovation: The effort to bring artificial intelligence to warfighting

What is behind the Pentagon's concerted interest in the development and deployment of artificial intelligence? In the most basic understanding, U.S. officials are motivated by the logic of the first-mover advantage: When a technology is first introduced, the actor who possesses it may hold an important benefit over its competitors. As a technological advantage in war can influence the outcome of any given conflict, the armed forces cannot afford to sacrifice their technological edge.[167] Potential American adversaries have not been coy about their grand intentions for AI. As previously noted, China and Russia have both announced state-sponsored development programs for artificial intelligence in 2017, tying it to the maintenance of their national security. Vladimir Putin's statement on AI has become quite infamous in the defense and AI communities, arguing that "whoever becomes the leader in [the AI] sphere will become the ruler of the world."[168] With the articulation of great power competition as the future of the U.S.'s national security strategy, and the inevitability of China and Russia one day fielding military AI capabilities, the logic for the Pentagon to develop its own AI programs is quite clear; If the United States' national security community fails to do so, it will find itself in an acute disadvantage against its great power rivals.[169] The strategic imperative then is for the U.S. to maintain its military supremacy through the superior development and deployment of AI.[170] It is worth noting, then, that the military adoption of AI is occurring in the context of *hypothetical* adversaries. While the United States currently has tense relations with Russia and China, the country is not in an active state of war with these powers. This contrasts with defense biometrics, which was developed and tailored to the operational environment of the War on Terror in the Middle East, an important qualitative distinction that I will elaborate on in Part VI.

To start, it is important to acknowledge the historical role the DoD has played in the development of AI as a field of study. The military provided funding for early AI and machine learning research during the 1950s and 1960s, primarily through the Advanced Research Projects Agency (ARPA).[171] The Pentagon's initial enthusiasm (and support) for the promises of AI began to flag by the 1970s, as the push to shift funding from basic to applied artificial intelligence projects for defense applications produced lackluster results. For example, the

human decision-making: *See* Horowitz, Michael. "The Promise and Peril of Military Applications of Artificial Intelligence." *Bulletin of the Atomic Scientists* (blog), April 23, 2018. https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/.

[167] Silverstein, Andrew Bernard. "Revolutions In Military Affairs: A Theory On First-Mover Advantage." *University of Pennsylvania ScholarlyCommons*, 2013, 119.

[168] *See* Vincent, James. "Putin Says the Nation That Leads in AI 'Will Be the Ruler of the World.'" The Verge, September 4, 2017. https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

[169] *See* White House. "National Security Strategy of the United States of America," December 18, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

[170] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech.": DoD CTO Dana Deasy: *"Russian and Chinese investments in military AI technology heighten the need for US forces to use more AI, too...We must adopt AI to maintain our strategic position and prevail on future battlefields."*

[171] *See* Tarraf, Danielle C., William Shelton, Edward Parker, Brien Alkire, Diana Gehlhaus Carew, Justin Grana, Alexis Levedahl, et al. "The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations." Product Page. RAND Corporation, 2019. https://www.rand.org/pubs/research_reports/RR4229.html.

Speech Understanding Program was funded as a five-year, $3 million program in 1971 with the end-goal of a speech recognition system that could attain a ten-thousand-word vocabulary.[172] By 1976, DARPA administrators and the AI researchers disagreed over whether the "performance criteria had been met;" a euphemism for a less-than-stellar program demonstration. The Pentagon's pursuit of AI remained elusive during the 1980s, with DARPA concluding that the 1983 Strategic Computing Program to develop "a new generation of computers that can SEE, HEAR, TALK, PLAN, and REASON" was far too ambitious with existing technologies.[173] While these early investments in AI research did not translate to a concerted adoption effort on the part of armed services, they reflect the traditional role of the military in promoting basic research into new technologies and the role it played in contributing to the amount of funding and academic talent devoted to AI. Unfortunately for the Pentagon, both computational power and the "intelligent" algorithms themselves remained too immature for the complex operational visions defense officials had in mind; the DoD's pursuit of artificial intelligence would have to wait for the twenty-first century acceleration of AI capabilities among the technology firms of Silicon Valley.

In this way, artificial intelligence in the twenty-first century can be best understood as a spin-on innovation. The Pentagon turned to the private sector from the beginning of its efforts to bring AI into the military in the early 2010s, and its leadership has been emphatic about the essential role technology firms must play in the military's adoption of AI technologies. AI Chief Shanahan, for example, has stated how "commercial solutions are available for most of the problems we've discovered in the past and will discover in the future [and] it is where some of the world's best talent resides right now."[174] Indeed, AI applications are necessarily dual-use, with both military and consumer applications. This makes sense: An image recognition algorithm trained to identify shoplifters using security camera footage could be similarly co-opted by the military. Instead of training the algorithm on security footage, it could be used to recognize terrorist activity in video footage recorded by drones in the Middle East.[175] More so, because the technology is still considered to be in its relative infancy, cutting-edge advances are occurring in labs run by Silicon Valley companies and academic research universities, not traditional defense contractors.[176] It was in recognition of these realities that the Department of Defense's Artificial Intelligence Strategy explicitly called for a close collaboration between the military and tech industry in order to procure the software and cloud computing technology

[172] Klatt, Dennis H. "Review of the ARPA Speech Understanding Project." *The Journal of the Acoustical Society of America* 62, no. 6 (December 1, 1977): 1345–66. https://doi.org/10.1121/1.381666.

[173] Roland, Alex, and Philip Shiman. *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993*. History of Computing. Cambridge, Mass: MIT Press, 2002.

[174] Ibid

[175] Sayler, Kelley M. "Artificial Intelligence and National Security."

[176] *See* Knight, Will. "Military Artificial Intelligence Can Be Easily and Dangerously Fooled." MIT Technology Review, October 21, 2019. https://www.technologyreview.com/2019/10/21/132277/military-artificial-intelligence-can-be-easily-and-dangerously-fooled/.

necessary to realize defense AI ambitions.[177] While the DoD stands to benefit from cutting-edge private sector work on AI, the benefits do not flow one way. The military is a compelling partner for technology firms, offering lucrative (and highly profitable) defense contracts and possessing valuable data sets typically inaccessible to research universities or companies.[178]

Recognizing that the majority of expertise and talent in the field of AI resides in the commercial technology sector, the Pentagon turned its sights to Silicon Valley. In 2016, the Defense Innovation Board (DIB) was chartered as a federal advisory committee tasked with "providing independent advice and recommendations on innovative means to address future challenges and technology applications."[179] The DIB was conceived by then-Secretary of Defense Ash Carter as part of the Third Offset Strategy, with the board designed to bring military officials and leaders of the commercial technology sector closer together in areas of emerging interest, first-and-foremost being artificial intelligence.[180] Dr. Eric Schmidt, former Executive Chairman of Alphabet, chairs the DIB, with members hailing from academic research institutions and commercial technology companies such as Microsoft, Facebook, and Google.[181] Artificial intelligence immediately became one of the DIB's main priorities, with its members issuing "Recommendation #5: Catalyze Innovations in Artificial Intelligence and Machine Learning" in October 2016.[182] Recommendation #5 calls for the military to harness the capabilities of AI and ML to "ensure technology superiority the way DoD did with nuclear weapons in the 1940s and with precision-guided weapons and stealth technology afterward."[183] This recommendation is an explicit reference to the Pentagon's previous success in its First and Second Offset Strategies, and a deliberate attempt at framing the importance of AI to the ongoing Third Offset Strategy. More importantly, however, the DIB recommended that the DoD establish a center for the study of artificial intelligence and machine learning, which would build expertise in these areas across the Pentagon. The DIB envisioned that this center would also serve as the military's liaison with labs in the private sector and universities and as an educational source to inform the armed services about the implications of AI technologies for military operations. Recommendation #5 thus formed the framework for the Pentagon's creation of the Joint Artificial Intelligence Center (JAIC) in 2018. From 2019 to 2020, the Defense Innovation Board

[177] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech."; Department of Defense. "Summary of DoD AI Strategy."

[178] *See* Defense Innovation Board. "Our Work | Recommendations." Accessed April 30, 2020. https://innovation.defense.gov/Recommendations/.

[179] *See* Department of Defense. "Charter of the Defense Innovation Advisory Board." Defense.gov, April 15, 2016. https://media.defense.gov/2017/Dec/14/2001856439/-1/-1/0/2566_2016.04.15_CHARTER%20(2016-2018)_(2016-04-15-09-33-09).PDF.

[180] *See* Defense Innovation Board. "Our Story." Accessed April 30, 2020. https://innovation.defense.gov/Recommendations/.

[181] *See* Defense Innovation Board. "Meet the Board." Accessed April 30, 2020. https://innovation.defense.gov/Members/.

[182] *See* Defense Innovation Board. "Our Work | Recommendations."; Pellerin, Cheryl. "Defense Innovation Board Makes Interim Recommendations." U.S. Department of Defense, October 5, 2016. https://www.defense.gov/Explore/News/Article/Article/965196/defense-innovation-board-makes-interim-recommendations/.

[183] Ibid

also spearheaded the creation of the Pentagon's Ethical Principles for Artificial Intelligence (to be discussed further herein).[184]

The Joint Artificial Intelligence Center (JAIC) was launched as the DoD's "Center of Excellence" on all artificial intelligence matters as the focal point of the Department's AI strategy.[185] The JAIC's mission statement is to "provide a critical mass of expertise to help the Department harness the game-changing power of AI," thus integrating technology development with organizational change to ensure the successful deployment of AI across the armed services.[186] This mission is broken down into several key objectives: To accelerate the delivery and adoption of AI, to scale the impact of AI across the Department, to develop partnerships with industry, academia, allies, and partners, to cultivate a leading AI workforce, and leading in military AI ethics and safety.[187] The JAIC is housed within the Office of the Chief Information Officer, and the unit is currently led by Director Lt. General Jack Shanahan and Deputy Director Stephen T. Homeyer. The JAIC has the authority to vet all DoD AI projects requiring funding in excess of $15 million, and it accomplishes this through two operational categories: National Mission Initiatives (NMIs) and Component Mission Initiatives (CMIs).[188] NMIs are the broad AI capability delivery projects that the JAIC will run for problems which cross Military Services or Departments.[189] CMIs are more narrow projects tailored to a specific DoD Component or Agency (e.g. no cross-functional capabilities required).[190] They will be run by the respective Component with support from the JAIC in the form of funding, data management, and AI standards.

Shanahan has stated that the JAIC's overriding prerogative will be to rapidly deploy *existing* AI algorithms and tools, contracted from commercial technology companies for military applications.[191] The unit's procedure for determining which AI projects to take on was illuminated by Rachael Martin, the JAIC's mission chief of Intelligent Business Automation Augmentation and Analytics, in January 2020. Four principles will be followed in picking its AI projects: mission impact, data-readiness, technology maturity, and "internal changemakers."[192] Mission impact involves an internal evaluation of "who cares" within the DoD, and an assessment of the target user base that would adopt and potentially benefit from the AI

[184] *See* Lopez, C. Todd. "DOD Adopts 5 Principles of Artificial Intelligence Ethics." U.S. Department of Defense, February 15, 2020. https://www.defense.gov/Explore/News/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/.

[185] *See* JAIC. "About the JAIC." Accessed April 30, 2020. https://www.ai.mil/about.html.

[186] *See* Office of the Chief Information Officer. "Joint Artificial Intelligence Center." U.S. Department of Defense. Accessed April 30, 2020. https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/.

[187] Ibid

[188] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech."; https://admin.govexec.com/media/establishment_of_the_joint_artificial_intelligence_center_osd008412-18_r....pdf

[189] *See* JAIC. "About the JAIC"; Office of the Chief Information Officer. "Joint Artificial Intelligence Center."

[190] Ibid

[191] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech."

[192] *See* Vincent, Brandi. "How the Pentagon's JAIC Picks Its Artificial Intelligence-Driven Projects." Nextgov.com, January 23, 2020. https://www.nextgov.com/emerging-tech/2020/01/how-pentagons-jaic-picks-its-artificial-intelligence-driven-projects/162594/.

technology. The second principle, data-readiness, seeks to determine where the data to be analyzed is “clean” and prepared for the complex modelling required of AI algorithms. Technology maturity relates to the JAIC’s mission to co-opt existing AI technologies for military use. Indeed, according to Martin, they aim to identify “what already exists and is ready to be deployed at this moment,” contrary to the impression of the unit as a R&D hub or base for emerging, untested AI. Lastly, the JAIC seeks to understand who the “changemakers” within the DoD will be. In other words, which officials or leaders will be the champions of the project, working in collaboration with the JAIC throughout the development cycle of a particular AI solution.[193] The JAIC is currently pursuing its first projects meeting these criteria, including Predictive Maintenance (PMX), Humanitarian Assistance and Disaster Relief (HADR), Cyber, Joint Warfighting, Intelligent Business Automation, Augmentation and Analytics (IBA3), and Warfighter Health.[194] The Joint Enterprise Defense Infrastructure (JEDI) contract is also being run by AI Chief Shanahan with the JAIC, as an enterprise cloud computing network spanning the federal government is deemed essential to the full exploitation of AI systems (and the data they run on) for national security users.[195] It is believed that the Pentagon intends to dedicate $1.7 billion to the JAIC and AI projects over the next five years, a sizable war chest that will require significant budget appropriations from a $268 million request for FY2020.[196]

While existing AI technologies are adopted by the JAIC, the Office of the Under Secretary of Defense for Research and Engineering is charged with the development and procurement of emerging capabilities. The Under Secretary, also known as the DoD’s Chief Technology Officer, is thus responsible for the “research, development, and prototyping activities across the DoD enterprise” to ensure the military’s technology superiority.[197] The Defense Advanced Research Projects Agency (DARPA) and the Defense Innovation Unit (DIU) are two organizations which report to the CTO and are playing an important role in the overall effort to adopt AI by focusing on early but promising advanced AI projects. As discussed, DARPA has a storied history within the DoD’s innovation ecosystem, and it is not sitting on the sidelines in the mission to translate AI technologies for military purposes. In September 2018, the organization announced its “AI Next” campaign, a multi-year investment initiative to pursue the “third wave of technological advance:” contextual adaptation. DARPA is devoting over $2 billion toward projects which advance beyond machine learning techniques towards contextual reasoning capabilities — the ability of machines to acquire human-like communication and

[193] Ibid: *“We're not in the business of coming up with good ideas and then creating something and trying to hoist it on somebody else...We really believe in a very user-centric approach.”* - Rachael Martin

[194] *See* JAIC. “About the JAIC”

[195] *See* McLeary, Paul. “Big Data For Big Wars: JEDI vs. China & Russia.” *Breaking Defense* (blog). Accessed April 30, 2020. https://breakingdefense.com/2019/08/big-data-for-big-wars-jedi-vs-china-russia/.

[196] *See* Metz, Cade. “Artificial Intelligence Is Now a Pentagon Priority. Will Silicon Valley Help?” *The New York Times*, August 26, 2018, sec. Technology. https://www.nytimes.com/2018/08/26/technology/pentagon-artificial-intelligence.html; Mitchell, Billy. “JAIC Director Jack Shanahan: ‘2020 Will Be a Breakout Year’ for DOD’s Artificial Intelligence.” FedScoop, September 3, 2019. https://www.fedscoop.com/jaic-fiscal-2020-jack-shanahan/.

[197] *See* Office of the Under Secretary of Defense for Research and Engineering. “DoD Research & Engineering | About.” Chief Technology Officer. Accessed May 1, 2020. https://www.cto.mil/.

reasoning capabilities, with the ability to recognize new situations and environments and adapt to them.[198]

The Defense Innovation Unit, on the other hand, is a recent addition to the DoD's technology acquisition capabilities, designed to be a kind of "Silicon Valley embassy" for the armed services.[199] It is focused on five technology areas — AI, autonomy, cyber, human systems, and space — where the commercial sector is considered to be at the cutting-edge. Its value-add in promoting AI adoption is two-fold: geographic proximity and rapid prototyping. The DIU has offices in Silicon Valley, Boston, and Austin, providing it with a unique reach to tap into the innovation ecosystems in the regions the Pentagon has typically been distant from with its centralized bureaucracy in Washington, DC. More importantly, the Defense Innovation Unit has the statutory authority to field and scale promising commercial technologies at *commercial speeds*.[200] In this way, the DIU can be best understood in the overall scheme of the Pentagon's AI efforts as a technology "scout" for potentially impactful AI technologies, linking small firms with the JAIC and other DoD leaders to accelerate their development with the ultimate objective of military adoption.

5.4 Project Maven: The Pentagon's First "AI Experiment"

In April 2017, then-Deputy Defense Secretary Bob Work announced the launch of an Algorithmic Warfare Cross-Functional Team devoted to a new assignment: Project Maven.[201] Led by Lt. Gen. Jack Shanahan (who would go on to direct the JAIC) and Marine Corps Col. Drew Cukor, Project Maven was conceived as the Pentagon's first experiment in advanced AI capabilities, a crash program designed to deliver AI technologies to the battlefield within six months of its initial funding.[202] The use case chosen for the experiment in defense AI was the Air Force's intelligence-gathering operations in Iraq and Syria in the United States' ongoing fight against the Islamic State (ISIS).[203] The Air Force possesses tactical aerial drone platforms such as the ScanEagle and the medium-altitude platforms such as a MQ-1C Gray Eagle and MQ-9 Reaper which collect many terabytes of data through their on-board video sensors. Traditionally, it takes a team of analysts working around-the-clock to comb through a fraction of one drone's

[198] *See* DARPA. "DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies," September 7, 2018. https://www.darpa.mil/news-events/2018-09-07.

[199] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech."

[200] *See* Defense Innovation Unit. "About." DIU.mil. Accessed May 1, 2020. https://www.diu.mil/about.

[201] *See* Pellerin, Cheryl. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End." U.S. Department of Defense, July 21, 2017. https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

[202] *See* Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS." Bulletin of the Atomic Scientists (blog), December 21, 2017. https://thebulletin.org/2017/12/project-maven-brings-ai-to-the-fight-against-isis/; Tucker, Patrick. "Project Maven Overseer Will Lead Pentagon's New AI Center." Defense One, December 14, 2018. https://www.defenseone.com/technology/2018/12/project-maven-overseer-will-lead-pentagons-new-ai-center/153555/.

[203] *See* Pellerin, Cheryl. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End."

sensor data.[204] Project Maven, then, was created to help address the laborious analysis of aerial drone intelligence, using machine-learning algorithms to automatically identify and label 38 classes of objects — images, buildings, and other landmarks — so Air Force analysts can identify unique targets.[205] The successful development of AI for drone intelligence analysis was imagined by the Cross-Functional Team as the ability of one analyst to do "twice as much work, potentially three times as much, as they're doing now."[206] In other words, Project Maven would automate low-level counting ability, freeing up valuable human capital for higher-value (and more complex) analysis.[207] For warfighters, the delay in human analysis and intelligence delivery means an evolving battlefield; Project Maven would also provide actionable intelligence to soldiers in the field in less time.[208]

The Cross-Functional Team turned to the commercial technology sector to source its training and image-processing algorithms for Project Maven. Upon the unclassified release of the AI project's details, Col. Drew Cukor announced that the Pentagon had a relationship with a "significant data-labeling company" that would provide services to allow DoD analysts and engineers to label existing data and prepare it for machine learning.[209] With Google as the vendor of choice for Project Maven, the cross-functional DoD-commercial team had to first clean up the Air Force's vast trove of data in order for the image-recognition algorithms to be "trained."[210] The initial defense leaders in charge of the program also sought to *structure* Project Maven correctly for a complex technical initiative like AI, using its ties to the Defense Innovation Unit — still an experimental unit at the time — to partner with industry experts on how to properly buy, field, and implement AI. With external counsel, Project Maven was modelled after project management techniques considered industry-standard in commercial technology. This approach calls for rapid product prototyping and iterative development by placing the developing technology in the hands of the end-users it is being designed for. Project management is of the utmost importance for AI development, as its essential tasks (e.g. labeling data, developing computational infrastructure, developing and integrating algorithms) are completed iteratively and in parallel.[211] Indeed, Gregory C. Allen, adjunct fellow with the Center for New American Security, has commented on the atypical development of Project AI compared to conventional defense projects: "The developers had access to the end-users very early on in the process. They recognized that [with] AI systems … you had to understand what your end-user was going to do

[204] *See* Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS."

[205] *See* Pellerin, Cheryl. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End."

[206] Ibid

[207] *See* Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS."

[208] *See* Atherton, Kelsey D. "Targeting the Future of the DoD's Controversial Project Maven Initiative." C4ISRNET, July 27, 2018. https://www.c4isrnet.com/it-networks/2018/07/27/targeting-the-future-of-the-dods-controversial-project-maven-initiative/.

[209] *See* Pellerin, Cheryl. "Project Maven to Deploy Computer Algorithms to War Zone by Year's End."

[210] Ibid

[211] *See* Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS."

with them… There was this iterative development process that was very familiar in the commercial software world, but unfamiliar in the defense world."[212]

The identity of the Pentagon's contractor remained unknown until March 2018, when *The Intercept* and *Gizmodo* unveiled the mysterious contractor to be Google. The company had routed its formal relationship with the DoD through a Northern Virginia technology staffing company called ECS Federal, obscuring its involvement in Project Maven.[213] Upon the disclosure of the Pentagon-AI relationship, Google employees condemned the project: Several employees resigned and thousands more signed a petition condemning Google's role in developing "warfare technology."[214] Initial efforts by Google executives to contain the controversy proved ineffective, as leaks demonstrated that senior leaders at the company saw Project Maven as an opening to land both an annual $250 million contract and future AI work. In response, Google executives declined to renew the Project Maven contract, even removing the firm from contention for Project JEDI.[215] Discontent at Google spread across the Valley, with the Tech Workers Coalition — a labor rights organization composed of tech industry workers, labor organizers, and community organizers — issuing a petition in April 2018 calling upon major technology firms, including Amazon, Microsoft, and IBM, to refuse to take up Google's role in Project Maven.[216] While major publicly-traded commercial technology firms passed on the opportunity to take on the Project Maven contract, Silicon Valley leadership and its employees were not united in opposition to defense AI work. Palantir has taken over from Google on developing AI for drone footage analysis, and AI-startup Anduril Industries, led by Oculus Rift founder Palmer Luckey, has also secured a contract with the Pentagon to work on virtual reality battlefield-management systems.[217]

5.5 Implications for Future AI Adoption

Ultimately, Project Maven can provide valuable insights into how the Pentagon should proceed with AI adoption for military needs. As AI Chief Shanahan has articulated about the program, Project Maven is "designed to be that pilot project, that pathfinder, that spark that kindles the flame front of artificial intelligence across the rest of the [Defense] Department."[218]

[212] *See* Fang, Lee. "Google Is Quietly Providing AI Technology for Drone Strike Targeting Project." *The Intercept (blog),* March 6, 2018. https://theintercept.com/2018/03/06/google-is-quietly-providing-ai-technology-for-drone-strike-targeting-project/.

[213] *See* Fang, Lee. "Google Hedges on Promise to End Controversial Involvement in Military Drone Contract." *The Intercept (blog),* March 1, 2019. https://theintercept.com/2019/03/01/google-project-maven-contract/.

[214] Ibid

[215] *See* Mitchell, Billy. "Google's Departure from Project Maven Was a 'Little Bit of a Canary in a Coal Mine.'" FedScoop, November 5, 2019. https://www.fedscoop.com/google-project-maven-canary-coal-mine/.

[216] *See* Atherton, Kelsey D. "Targeting the Future of the DoD's Controversial Project Maven Initiative."; Tech Workers Coalition. "Tech Should Not Be in the Business of War." Coworker.org, April 2018. https://www.coworker.org/petitions/tech-should-not-be-in-the-business-of-war.

[217] *See* Chapman, Lizette. "Palantir Wins New Pentagon Deal With $111 Million From the Army." *Bloomberg.Com*, December 14, 2019. https://www.bloomberg.com/news/articles/2019-12-14/palantir-wins-new-pentagon-deal-with-111-million-from-the-army.; Fang, Lee. "Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract." *The Intercept* (blog), March 9, 2019. https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/.

[218] *See* Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS."

First, it is important to discuss some of the features of Project Maven that are likely to define the DoD's AI programs for the foreseeable future. Indeed, Maven is an example of the application of artificial intelligence technology to increase the military's speed and agility. Its program directors envisioned the modification of commercial image recognition algorithms to assist Air Force analysts in the laborious task of combing through video footage collected from military drones. By applying AI, it is expected that the Air Force will be able to greatly increase the work of its human analysts. Algorithms like the ones used to identify different classes of objects in Maven also fall within the category of "narrow AI," demonstrating how the Pentagon's foreseeable AI implementation will involve programs designed to perform a single task like image recognition, outside of the more complex (and still immature) projects for machines to realize "conscious" human intelligence.[219]

Additionally, the use case for Maven came out of already-existing AI applications in the commercial technology industry, a reflection of the dual-use antecedents of Maven and other emerging DoD AI projects with direct private technology antecedents. As JAIC officials have expressed, the Pentagon will first prioritize what it deems *mature* AI to be— algorithms which have been commercially-proven and can be translated to a defense application for accelerated deployment.[220] In this way, Maven is an important demonstration of the possibilities of DoD-private sector technology collaboration on an emerging technology like artificial intelligence. The Pentagon was able to form commercial relationships with both major Silicon Valley firms (e.g. Google, Palantir) while also bringing small technology startups like Anduril on board through vehicles like the Defense Innovation Unit. Indeed, Palmer Luckey himself attributed his firm's participation in Project Maven as benefitting from the DoD's concerted outreach to non-traditional external partners. He attributes the DIU for demonstrating "that people in Silicon Valley could actually get stuff into production, actually do work with the government... and proving that you actually could get into [military work]."[221]

Both effective engagement with the tech sector and the successful deployment of Maven itself required a transformation in the DoD's organizational processes around technology acquisition. In order to work and operate at *commercial speeds*, Maven had to be handled and structured differently from traditional defense acquisition processes, which can last several years with separated organizations defining technology specifications and a sequential "hand-off" of results as each organization completes its activities, an approach deemed ineffective for digital solutions.[222] To start, the importance of cross-functional teams was illustrated by the original Algorithmic Warfare Cross-Functional Team, which detailed stakeholders and talent from its

[219] *See* Jajal, Tannya D. "Distinguishing between Narrow AI, General AI and Super AI."

[220] *See* Vincent, Brandi. "How the Pentagon's JAIC Picks Its Artificial Intelligence-Driven Projects."

[221] *See* Fang, Lee. "Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract."

[222] *See* Serbu, Jared. "Pentagon's Number-Two Officer Vows to Fix Software Acquisition 'Nightmare.'" Federal News Network, January 21, 2020. https://federalnewsnetwork.com/defense-main/2020/01/pentagons-number-two-officer-vows-to-fix-software-acquisition-nightmare/.; Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS."

partners at Google and the DoD to both develop the AI software, ensure its technology specifications matched Department needs, and to facilitate prototyping. Moreover, the guiding idea behind organizing Maven was a project management approach, involving rapid prototyping by delivering a minimum viable product (MVP) to end-users and incorporating their feedback for further productive development. While project management has an extensive history in the private sector, its use by the Pentagon remains quite new, and in this way, Maven began the DoD's experiment with a product development process more closely resembling the consumer technology industry. Lastly, some of the capabilities developed for Project Maven, including its own AI-ready infrastructure (e.g. computing clusters for graphics processing), can now be leveraged for future algorithmic training for other JAIC projects.[223] In sum, Maven helped to build the institutional infrastructure and human capital required for AI adoption, paving the way for a DoD that will be more nimble and adept at procuring, piloting, and fielding artificial intelligence capabilities in the years to come.

While Project Maven demonstrated the possibilities for approaching the DoD's AI acquisitions, it also highlighted some of the challenges going forward — the most important being the ethical implications of defense AI. As discussed, Project Maven suffered from the loss of Google as its main technology partner after internal protests at the firm erupted over the Maven contract. Google engineers disagreed with the decision to contract with the DoD on a "warfighting technology," and its withdrawal from the project, along with the negative perceptions created around Maven, led some to believe that Google was the "canary in the coal mine" for the Pentagon's commercial sector relationships.[224] In hindsight, the long-term implications of the Google protests seem far less dire. Other technology partners like Palantir and Anduril stepped into the Maven contract to maintain the project, with some Silicon Valley firms even using the Google debacle to promote their own eagerness to contract with the DoD on its future AI needs. This was the approach taken by Amazon, Palantir, and Anduril, with Palmer Luckey penning an editorial in the Washington Post condemning Google for abandoning the federal government as counterproductive and naive: "If tech companies want to promote peace, they should stand with, not against, the United States' defense community."[225] Despite its withdrawal from Maven, Google itself has refused to renounce future work with the military on AI, with Kent Walker, Senior Vice President for Global Affairs, conveying that "[Google] continues to explore work across the public sector, including the military, in a wide range of areas … in ways consistent with our AI Principles."[226]

[223] *See* Allen, Gregory C. "Project Maven Brings AI to the Fight against ISIS."

[224] *See* Mitchell, Billy. "Google's Departure from Project Maven Was a 'Little Bit of a Canary in a Coal Mine.'"

[225] *See* Luckey, Palmer, and Trae Stephens. "Opinion | Silicon Valley Should Stop Ostracizing the Military." Washington Post, August 8, 2018. https://www.washingtonpost.com/opinions/silicon-valley-should-stop-ostracizing-the-military/2018/08/08/7a7e0658-974f-11e8-80e1-00e80e1fdf43_story.html.

[226] *See* Fang, Lee. "Google Hedges on Promise to End Controversial Involvement in Military Drone Contract."

AI Chief Shanahan has taken the Google controversy as a learning lesson for the DoD, believing that some initial criticism over its AI adoption efforts was inevitable: “The fact that it happened when it did as opposed to on the verge of a conflict or a crisis where we’re asking for help, we’ve gotten some of that out of the way.”[227] In other words, the Pentagon can respond to the legitimate questions of defense AI ethics raised by the adoption of existing commercial technologies for military purposes, and therefore learn and do better going forward in the framing of its AI initiatives and collaborative dynamics with its private sector partners. For example, the Pentagon has directly addressed the controversy at the root of Google’s withdrawal with the promulgation of its AI Ethical Principles in February 2020. The Defense Innovation Board led the development of the principles, which apply to the use of AI for both combat and non-combat situations. The principles are as follows: DoD personnel will exercise *responsibility* in the development, deployment, and use of AI capabilities; *Equitability* will be ensured by taking steps to minimize unintended biases in AI programs; Defense AI will be *traceable*, with transparent and auditable methodologies, data sources, and design procedures; *Reliability* will be maintained with the DoD’s AI capabilities having explicit, well-defined uses with thorough testing; and lastly, the department's AI will be *governable*, with the ability to detect and avoid unintended consequences or shut down deployed systems which fail to work as intended. By promising to adhere to these five key AI principles, the Pentagon hopes to both maintain a standard of excellence in regard to its adoption and fielding of artificial intelligence, while also convincing external stakeholders of the seriousness in which the military views the technology’s ethical implications.

6. ASSESSING THE THIRD OFFSET STRATEGY: RECOMMENDATIONS AND CONCLUSION

6.1 From defense biometrics to defense AI: Lessons learned

Looking back on the case of defense biometrics, what lessons did the Pentagon learn which *translate* to AI procurement? The importance of a clear use case for developing and fielding a new technology for warfighting remains relevant. The operational need for biometrics emerged from the wars in Iraq and Afghanistan, when warfighters expressed a need to ascertain the identities of insurgents apprehended on the battlefield. At the same time as this operational application was emerging, national security planners at the Pentagon and other think tanks like the CSIS and RAND were elaborating on “identity dominance” theory, which expressed the significance of the United States to harmonize identifications capabilities across the defense and law enforcement agencies from the federal to the local level.[228] In this way, defense biometrics suggested that technology adoption benefits from the articulation of a compelling operational use

[227] *See* Lopez, C. Todd. “DOD Adopts 5 Principles of Artificial Intelligence Ethics.”

[228] *See* Woodward, John D. “Using Biometrics to Achieve Identity Dominance in the Global War on Terrorism:”

case, while the framing of an "overarching ideology" like identity dominance can provide further coherence to focus adoption efforts across the armed services.

The current trajectory of AI development suggests that the Pentagon is following a similar playbook, whether it be deliberate or not. As Shanahan and other officials at the JAIC have expressed, the Pentagon's acquisitions strategy is emphasizing AI applications with clear operational use cases. Project Maven, for example, identified an area where the military was struggling to perform a task essential to its mission — intelligence analysis of drone footage — and proposed modifying existing commercial AI technology to improve this operational challenge.[229] Also in line with the case of defense biometrics, the DoD has begun to put together a common framework for its pursuit of AI, a tentative theory of military "speed and agility."[230] In other words, as previous technology initiatives like nuclear power and precision-guided weapons heightened the destructive capabilities of the DoD, now artificial intelligence and other developing technologies will allow the military to field more agile forces while increasing its operational efficiency. With these commonalities in mind, it is important to distinguish where AI remains behind that of biometrics — AI technology is not yet being fielded against defined adversaries. While the push behind artificial intelligence has been strongly motivated by China and Russia's exploration of AI, these potential great power rivals remain *hypothetical*. On the other hand, defense biometrics came to be adopted and tested against the rigors of real opponents, with jihadist terrorists and other insurgents seeking to outwit the biometric technologies being fielded by coalition forces. This in turn allowed DoD technology managers to work with their commercial partners on devising more rigorous solutions, leading to more effective capabilities on the battlefield.

As discussed in Part IV, defense biometrics conveyed the importance of prototyping a new defense technology, particularly in the context of a "natural experiment." For biometrics, this natural experiment was the battlefield, where warfighters were given prototype biometric products and feedback was collected on their suitability for counter-insurgency initiatives. Warfighter feedback was then incorporated into the product's development, thus creating biometric technologies better suited to conditions on the ground. The Joint Artificial Intelligence Center has been pursuing a similar strategy, considering its emphasis on project management organizational techniques to rapidly deliver prototypes to DoD end users. AI Chief Shanahan has expressed this methodology as starting with "50% solutions ASAP."[231] Project Maven and later AI programs are following the private-sector best practices of a "field-feedback-fix-repeat" cycle in response to the urgent demands from warfighters for AI capabilities, perhaps best articulated by Shanahan himself: "I was in a room no more than a week ago with a group [special

[229] *See* Vincent, Brandi. "How the Pentagon's JAIC Picks Its Artificial Intelligence-Driven Projects."

[230] *See* Simonite, Tom. "The Pentagon Doubles Down on AI–and Wants Help from Big Tech."

[231] *See* Jr, Sydney J. Freedberg. "Joint AI Chief: Start With 50% Solutions ASAP." *Breaking Defense* (blog), August 30, 2019. https://breakingdefense.com/2019/08/joint-ai-chief-start-with-50-solutions-get-better-asap/.

operators], who were … pounding the tables, saying, 'Just give us the capabilities. We know it's not perfect yet. We're here to wring it out and tell you how to make it better.'"[232]

The "natural experiment" for artificial intelligence is less clearly defined, considering that most planned AI applications do not imagine direct translation to the battlefield and the United States is not engaged in active adversarial conflict with a great power rival. While the case of AI may currently lack as comprehensive of a natural experiment setting as the War on Terror in the Middle East, one could imagine many "mini-natural experiments" as each unique use case is deployed to warfighters from the JAIC and its performance is evaluated and iterated upon. One cautionary note for the unique technical basis of artificial intelligence is the reliance of the software on the data it is "trained on."[233] In other words, can Project Maven's image recognition algorithms, trained on surveillance data from Iraq and Afghanistan, be used to successfully discern key personnel or installations in an alternative context, such as a military conflict in China? As Michael Horowitz, professor of political science at the University of Pennsylvania states, there are "risks that algorithms trained on historical data might face battlefield conditions that are different from the one it trained one," a complication to the ideal situation of using one particular program to generalize technical specifications and learnings to other potential applications for rapid deployment.[234]

Lastly, both defense biometrics and artificial intelligence demonstrated the importance of a "center of excellence" to coordinate technology acquisition, development, and integration across the DoD. For example, both the Biometrics Fusion Center and Joint Artificial Intelligence Center developed close external relationships with commercial technology vendors, selecting among existing products those which could be best suited for military specifications. The Centers worked with the different branches of the armed services on testing and evaluation and were crucial to the prototyping and development process for their respective technologies. Of course, the Pentagon's efforts to integrate AI into warfighting could also be said to have benefited from a consideration of the ethical implications of its adoption, which came to the fore with Google's exit from Project Maven. While defense biometrics largely avoided significant controversy over its logging of biometric data in the Iraq and Afghanistan theatres, both cases illuminated how technology adoption is best facilitated through an early and comprehensive formulation of ethical standards.

6.2 The Third Offset in Perspective

The most important legacy of the Third Offset may be its success in re-orienting the Pentagon toward the cutting-edge technological advancements of the commercial sector in areas

[232] Ibid

[233] See University of Toronto. "Training an Artificial Neural Network." Accessed May 3, 2020. http://www2.psych.utoronto.ca/users/reingold/courses/ai/cache/neural3.html.

[234] *See* Groll, Elias. "The Pentagon's AI Chief Prepares for Battle."

like biotechnology, robotics, and most importantly, artificial intelligence. The Defense Innovation Board has provided the Pentagon access to significant thought leaders in Silicon Valley and other innovation hubs around the country, including academic practitioners and executives in private industry. Indeed, the DIB has made important contributions to the Third Offset and the Pentagon's acquisitions efforts, including its recommendations to create an "AI hub," which led to the Joint Artificial Intelligence Center being stood-up in 2018, and its spearheading of the Artificial Intelligence Ethical Principles in 2020. The Defense Innovation Unit, one of the institutional innovations of the Third Offset for the Pentagon's procurement efforts, has also proved to be a valuable link connecting warfighters to firms with AI expertise, signified by its role in drawing potential vendors to Project Maven and other ongoing DoD investments.[235] Both developments as part of the Third Offset have brought the Pentagon and the commercial technology sector closer together, with demonstrated successes in the effort to field AI for defense use cases.

Similarly, tentative insights can be drawn from the reforms to Pentagon procurement and acquisition policies to facilitate prototyping of commercial technologies for "spin-on" adoption. Other Transaction Authority (OTA) is being piloted by both "new" units like the DIU and JAIC and "old" units like DARPA. Active use by these organizations within the DoD suggests that internal stakeholders are interested in utilizing the new procurement authorities to improve the acquisition process, and the use of accelerated contracting by the DIU and JAIC to bring AI capabilities to the Air Force within six months after contracting in Project Maven suggest that these reforms are working as intended, increasing the speed at which commercial partners can develop, deliver, and iterate on prototypes meeting military specifications. The OTA and other modifications to acquisition policies have also expanded DoD relationships to firms outside of the conventional contractor base, as seen in the case of ongoing artificial intelligence adoption. For example, the DIU's use of the Commercial Solutions Opening (CSO) as a competitive solicitation process for problems facing warfighters, followed by the awarding of an OT for prototyping, allows the Defense Innovation Unit to work with vendors it may not have once-considered in a fast, flexible, and collaborative process, broadening the vendor base available to the Pentagon.[236] Moreover, the flexibility these OTA contracts provide to commercial partners allow these firms, used to operating in the speed and relative "freedom" of the private sector, to avoid the burden of abiding by unfamiliar and at-times byzantine Federal Acquisition Regulation (FAR) policy.[237] While a more definitive and systematic assessment may have to wait as further data is collected on the success (and failure) of ongoing technology adoption initiatives, in

[235] *See* Defense Innovation Unit. "DIU Solutions | Portfolio." Accessed May 3, 2020. https://www.diu.mil/solutions/portfolio.

[236] *See* "DIUx Commercial Solutions Opening: How to Guide." Defense Innovation Unit Experimental Silicon Valley United States, November 30, 2016. https://apps.dtic.mil/docs/citations/AD1022451.

[237] *See* U.S. General Services Administration. "Federal Acquisition Regulation (FAR)." Accessed May 3, 2020. https://www.gsa.gov/policy-regulations/regulations/federal-acquisition-regulation-far.

allowing the military to more closely reach acquisition speeds typical of the commercial sector, the Third Offset can be judged to have reached one of its key expressed objectives.

Of course, the acquisition of new technologies is only half the battle; the cases explored herein illuminated how other concerns unrelated to the procurement of the technology itself can come into play in the successful adoption of a given innovation. There is more to fielding a new technology than "buying it." The impact of the Third Offset on this "non-acquisition" facet of military innovation remains inchoate, considering the heavy emphasis on expanding the DoD vendor base and rapid fielding of new prototypes thus far — all related to the acquisition process itself.

One of the first, and most important lessons, was revealed by the study of defense biometrics: The significance of a *guiding framework or "ideology,"* to organize and make sense of the efforts to field a new technology. "Identity dominance," for example, brought the diffuse efforts of the Pentagon, FBI, Homeland Security, and other agencies to bring biometrics to their respective missions together to consider how their programs could align and communicate across traditional institutional walls. Calls for an "all-of-government" effort to apply AI to the federal government could spark a similar push outside of existing intra-agency efforts. At the moment, the Pentagon's overarching emphasis on "getting faster" is unifying artificial intelligence initiatives across the branches of the armed services. Defense biometrics and AI point to how an articulated reform program like the Third Offset Strategy cannot provide a guiding framework like identity dominance or agility in and of itself; these paradigms must be produced and initiated by organizational leaders outside the scope of an "offset strategy."

A use case can be explored and a potential commercial product with a dual-use potential identified, but what comes next? A given technology must be piloted through *rapid prototyping, ideally in a "natural experiment" setting*. The Third Offset Strategy deserves commendation here for changes to procurement reforms which have made it easier for commercial technology companies to provide prototypes to program managers, such as the OT for Prototypes. However, the contractual capability alone is insufficient; DoD units themselves must be dedicated to the prototyping process — Warfighters must be content with receiving a 50% solution to their operational challenge, and the leaders of the armed services interested in fielding AI solutions must understand the role they can play in providing user-driven feedback for iterative product development.

The importance of a project management approach to accelerating technology adoption relates to the significance of *organizational dynamics* within the DoD, which the Third Offset Strategy has begun to promote with new units stood-up like the DIU and JAIC and procurement reforms to facilitate prototyping. Similarly, the DIB has recommended that the Pentagon embrace a "culture of experimentation," establish an Office of the Chief Innovation Officer, reward bureaucracy busting, and conduct innovation and technology training for senior DoD leaders.[238] These proposals all share the same motivation: to promote an organizational environment which emphasizes risk-taking and creativity. If the Pentagon is to continue its pursuit of cutting-edge commercial technologies, some of which will surely fail or struggle to realize their promised application, then DoD officials must not fear punishment or ignominy if the innovation initiative they champion stumbles. As General John E. Hyten — Vice Chairman of the Joint Chiefs of Staff and chairman of the Joint Requirements Oversight Council — has expressed, this culture of experimentation is ever-more important considering how many emerging technologies will be software-based. In remarks to an audience at the CSIS in January 2020, he remarked that risk aversion among senior leaders has proliferated across the Pentagon's acquisition programs, undermining the speed at which the DoD buys and builds software.[239] At the same time, he argued that altering buying procedures alone for software and other emerging technologies, as the Third Offset has prioritized to this point in time, is insufficient for a requirements process "built for tanks and aircraft carriers."[240] While a less risk-averse requirements process remains a concept for future discussion, Hyten raises a valid point: The organizational dynamics of innovation are equally as important to technology acquisition, and the Third Offset Strategy must pay closer attention to how the armed services are integrating and fielding new technologies post-procurement.

Lastly, it is worth remarking that *non-institutional factors*, such as the ethical implications of a commercial technology co-opted for military purposes, are worth considering during the "spin-on" process. Defense biometrics raised the issue of military ethics as the DoD received mild criticism over its mass collection of personal biometric data of innocent civilians and terrorists alike. Artificial intelligence more clearly demonstrated the potential perils of failing to address the ethics of an emerging technology applied to warfighting, as the well-publicized internal Google revolt led to the firm's withdrawal form Project Maven. While these dynamics outside of the "immediate" organizational scope of the armed services are impossible to fully envision with a reform program like the Third Offset, the challenges they can pose to potential defense innovation initiatives makes it worthy of the attention of senior Pentagon officials. In other words, by championing technologies like AI for defense purposes, military leaders should be vigorous in maintaining an early dialogue with internal and external stakeholders and be forthright about questions over its ethics for warfighting.

[238] *See* Defense Innovation Board. "Our Work | Recommendations."

[239] *See* Serbu, Jared. "Pentagon's Number-Two Officer Vows to Fix Software Acquisition 'Nightmare.'" Federal News Network, January 21, 2020. https://federalnewsnetwork.com/defense-main/2020/01/pentagons-number-two-officer-vows-to-fix-software-acquisition-nightmare/.

[240] Ibid

6.3 Conclusion

Defense biometrics illuminated the Pentagon's acquisition of an existing commercial technology for military purposes during the War on Terror, while the pursuit of defense artificial intelligence is an ongoing effort by the armed services begun in earnest with the onset of the Third Offset Strategy in the 2010s. Both cases can be placed within the twenty-first century context of innovation as technologies first targeted for commercial end-users, and later adapted by the Pentagon when military applications became apparent. In other words, biometrics and artificial intelligence are quintessential "spin-on innovations," and for this reason, their case studies of successful and ongoing adoption, respectively, provide a useful lens in which to answer the question posed at the beginning of this Article: is the Pentagon still capable of discovering and promoting the technological innovations of the future?

While the military finds itself in an altogether different innovation context in the twenty-first century than when it pursued advanced nuclear technology or precision-guided weapons during the First and Second Offsets of the twentieth century, I argue that the Department of Defense has begun to successfully respond to these changed circumstances in the form of the Third Offset Strategy. New organizations like the Defense Innovation Unit and Defense Innovation Board have brought the Pentagon and the commercial technology sector closer together, while alternative methods of contracting like the Other Transaction Authority (OTA) and Commercial Solutions Opening (CSO) have expanded the vendor base available to the armed services and increased its ability to practice rapid prototyping of new technologies.

The Pentagon has begun its effort to adopt next-generation AI capabilities by turning to the commercial technology sector, and it is deploying these new institutional tools created for the Third Offset in its effort to woo private tech leaders in Silicon Valley and elsewhere to develop innovative technologies for the armed services. While the DoD is in the early stages of executing its Artificial Intelligence Strategy, it has become apparent that the Joint Artificial Intelligence Center and other Pentagon leaders interested in AI are relying on the products of the Third Offset — the Defense Innovation Unit, the Defense Innovation Board, and the Other Transaction Authority/Commercial Solutions Opening — in their aspiration to procure, develop, and field artificial intelligence solutions at commercial speeds.

Using defense biometrics as a case study for a successful "spin-on" innovation, modest recommendations were offered for both the Pentagon's development of AI and for the Third Offset Strategy more generally. These recommendations largely focused on the dynamics of the spin-on process after "buying" the technology, including the importance of a guiding framework or ideology for the translation of a new innovation to warfighting, rapid prototyping in a "natural experiment" setting, organizational dynamics promoting experimentation and creativity, and awareness of non-institutional factors like military ethics which can impede technology development.

In sum, the Third Offset Strategy is not simple rhetoric. There is reason to believe that the U.S. military's innovation edge can be maintained through the reform program of the Third Offset. As its ideas have outlasted its initial promulgation by Secretary Carter during the Obama Administration, successive DoD Secretaries — Jim Mattis, Patrick Shanahan[241], and Mark Esper — have maintained their commitment to bolstering the innovative capabilities of the armed services, by promoting further acquisition reforms, expanding funding and capabilities to the Defense Innovation Unit, and leaning on the Defense Innovation Board to assist in the framing of the AI Ethical Principles. Even if the Trump Administration has let the organizing terminology of the "Third Offset" fall into disuse in recent years[242], the consensus among senior defense leaders and lawmakers is firmly rooted: The adoption of cutting-edge commercial technologies from the private sector — the "fourth channel" of the spin-on innovation — is of paramount importance in an era of resurgent great power competition in the twenty-first century; it is no exaggeration to say that the future of American military superiority depends on it.

[241] Served in an acting capacity from January to June 2019: *See* Historical Office of the Secretary of Defense. "Historical Office | Secretaries of Defense." Accessed May 3, 2020. https://history.defense.gov/DOD-History/Secretaries-of-Defense/.

[242] See Miller, James. "Is the Pentagon Truly Committed to the National Defense Strategy?" Defense One, March 12, 2019. https://www.defenseone.com/ideas/2019/03/how-committed-pentagon-national-defense-strategy/155502/.