Testimony

# Artificial Intelligence: Challenges and Opportunities for the Department of Defense

Jason Matheny

CT-A2723-1
Testimony presented to the U.S. Senate Committee on Armed Services, Subcommittee on Cybersecurity, on April 19, 2023

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/CTA2723-1

## Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.


## Limited Print and Electronic Distribution Rights



www.rand.org

*Artificial Intelligence: Challenges and Opportunities for the Department of Defense*

Testimony of Jason Matheny[1]
The RAND Corporation[2]

Before the Committee on Armed Services
Subcommittee on Cybersecurity
United States Senate

April 19, 2023

Chairman Manchin, Ranking Member Rounds, and members of the committee: Good morning, and thank you for the opportunity to testify today. I'm the president and CEO of RAND, a nonprofit and nonpartisan research organization. Before RAND, I served in the White House National Security Council and Office of Science and Technology Policy, as a commissioner on the National Security Commission on Artificial Intelligence, as assistant director of national intelligence, and as director of the Intelligence Advanced Research Projects Activity, which develops advanced technologies for the U.S. intelligence community.

For the past 75 years, RAND has conducted research in support of U.S. national security, and we currently manage four federally funded research and development centers (FFRDCs) for the federal government: one for the Department of Homeland Security (DHS) and three for the Department of Defense (DoD). Today, I'll focus my comments on how DoD can best ensure that progress in artificial intelligence (AI) benefits U.S. national security instead of degrading it.

Among a broad set of technologies, AI stands out for both its rate of progress and its scope of applications. AI holds the potential to broadly transform entire industries, including ones critical

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

to our future economic competitiveness and our national security. Integrating AI into our national security plans poses special challenges for several reasons:

- The technologies are driven by commercial entities that are frequently outside our national security frameworks.
- The technologies are advancing quickly, typically outpacing policies and organizational reforms within government.
- Assessments of the technologies require expertise that is concentrated in the private sector and that has rarely been used for national security.
- The technologies lack conventional intelligence signatures that distinguish benign from malicious use.

The United States is currently the global leader in AI;[3] however, this may change as the People's Republic of China seeks to become the world's primary AI innovation center by 2030—an explicit goal of China's AI national strategy.[4] In addition, both China and Russia are pursuing militarized AI technologies,[5] intensifying the challenges I just outlined. In response, I will highlight four sets of actions that DoD could take:

1. Ensure that DoD cybersecurity strategies and cyber Red team activities track developments in AI that could affect cyber defense and cyber offense, such as the automated development of cyber weapons.
2. To prevent bad actors from having access to advanced AI systems, (1) ensure strong export controls of leading-edge AI chips and chip-making equipment while licensing benign uses of chips that can be remotely throttled if need be; (2) use Defense Production Act authorities to require companies to report the development or distribution of large AI computing clusters, training runs, and trained models (e.g. >1,000 AI chips, $>10^{27}$ bit operations, and >100 billion parameters, respectively); (3) include in DoD contracts with cloud-computing providers a requirement that they employ "know your customer" screening for all customers before training large AI models; and (4) include in DoD contracts with AI developers "know your customer" screening, as well as strong cybersecurity requirements to prevent the theft of large AI models.
3. Work with the intelligence community to significantly expand the collection and analysis of information on key foreign public- and private-sector actors in adversary states involved in AI, including assessments of key foreign public and private entities; their infrastructure, investments, and capabilities; and their supply chains of tools, material, and talent. Strengthen DoD's institutional capacity for such activities by (1) creating new partnerships and information-sharing agreements among U.S. and allied government

[3] Although there are many ways to measure this, the Stanford Global AI Vibrancy Tool has consistently ranked the United States at the top. See Stanford University, "Global AI Vibrance Tool: Who's Leading the Global AI Race?" undated, https://aiindex.stanford.edu/vibrancy/.

[4] Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan,'" DigiChina, August 1, 2017, https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/.

[5] Forrest E. Morgan, Benjamin Boudreaux, Andrew J. Lohn, Mark Ashby, Christian Curriden, Kelly Klima, and Derek Grossman, *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*, RAND Corporation, RR-3139-AF, 2020, https://www.rand.org/pubs/research_reports/RR3139-1.html.

agencies, academic labs, and industrial firms and (2) recruiting private-sector AI experts to serve in the government on short-term or part-time appointments.

4. Invest in potential moon shots for AI security, including (1) microelectronic controls embedded in AI chips to prevent the development of large AI models without security safeguards and (2) generalizable approaches to evaluate the security and safety of AI systems before they are deployed.

I thank the committee for the opportunity to testify, and I look forward to your questions.