Testimony

Challenges to U.S. National Security and Competitiveness Posed by AI

Jason Matheny

CT-A2654-1
Testimony presented before the U.S. Senate Committee on Homeland Security and Governmental Affairs on March 8, 2023

RAND CORPORATION

For more information on this publication, visit www.rand.org/t/CTA2654-1.

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

Challenges to U.S. National Security and Competitiveness Posed by AI

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

Before the Committee on Homeland Security and Governmental Affairs
United States Senate

March 8, 2023

Chairman Peters, Ranking Member Paul, 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. Today, I'll focus my comments on how artificial intelligence (AI) affects national security and U.S. competitiveness. 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 to our future economic competitiveness, such as medicine, manufacturing, and energy. Applications of AI also pose grave security challenges for which we are currently unprepared, including the development of novel cyber weapons,

[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.

large-scale disinformation attacks, and the design of advanced biological weapons. Threats from AI pose special challenges for national security 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, differentiate intentional from accidental misuse, or permit attribution with certainty.

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 eight actions that national security organizations, including DHS, could take:

1. Ensure that DHS cybersecurity strategies and cyber Red Team activities track developments in AI that affect cyber defense and cyber offense.
2. With the National Institute of Standards and Technology, industry stakeholders, and U.S. allies and partners, ensure that international standards for AI prioritize privacy, security, and safety, so that the technologies are less prone to misuse by surveillance states.
3. Consider creating a regulatory framework for AI that is informed by an evaluation of risks and benefits of AI to U.S. national security, civil liberties, and competitiveness.
4. Identify the high-performance computing hardware used for AI as critical infrastructure that can be stolen or subverted. Consequently, consider requirements for tracking where high-performance computing hardware goes and what it is being used for.
5. 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, and create new partnerships and information-sharing agreements among federal, state, and local government agencies; the research community; and industry.
6. Leverage AI expertise in the private sector through short-term and part-time federal appointments and security clearances for leading private-sector AI experts who can advise the government on key technology developments.

---

[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.

7. In federal purchases and development of AI systems, include requirements for security and safety measures that prevent AI systems from misbehaving due to accidents or adversaries. Also require socially beneficial techniques, such as privacy-preserving machine learning and watermarking to detect generated text and deepfakes.
8. Last, increase our investments in biosecurity and biodefense, given the potential applications of AI to design pathogens that are much more destructive than those found in nature.

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