Statement before the

Senate Select Committee on Intelligence

"Addressing the National Security Implications of Artificial Intelligence: People, Bureaucracy, and Data Infrastructure"

A Testimony by:

Dr. Benjamin Jensen

Senior Fellow, International Security Program, CSIS and

Professor, Marine Corps University, School of Advanced Warfighting

September 19, 2023

216 Hart Building

CSIS and Marine Corps University do not take policy positions, so the views represented in this testimony belong to Benjamin Jensen and not those of his employers.

Chairman Warner, Vice-Chair Rubio, distinguished Members of the Committee, I am honored to share my views with you on what might be the central intelligence question facing our nation: *how does artificial intelligence affect national security*? The magnitude of the moment is clear, and both the Senate and the House are embracing their responsibility to create a national dialogue. As a citizen I thank you for that.

Today as part of this ongoing dialogue, I ask you to consider the often-invisible center for gravity for integrating new algorithms and enduring aspects of military theory and intelligence tradecraft. That center for gravity rests not just in lines of code, but in the *people*, the *bureaucracy* and the *data infrastructure* that turns any technology into strategic advantage.[1] Get the right people in place with permissive policies and provide them access to computational capabilities at scale and you gain a position of advantage in modern competition. Deny your adversaries the ability to similarly wage algorithmic warfare and you turn this advantage into enduring strategic asymmetry.

Artificial intelligence and machine learning (AI/ML) will be a critical capability for the nation going forward and central to integrated deterrence campaigns and warfighting. The general or spy who doesn't have a model by their side in the 21st century will be blind man in a bar fight. Yet, that critical capability – strategic competition and war at machine speed directed by human judgment – rests on critical requirements. Our intelligence community and military need rank and file members who understand basic data science and coding. They need a smaller, nimble information age bureaucracy open experimentation in place of the labyrinth of middle managers and policies that stifle innovation. And they need reliable access to data centers to continually train and update machine learning models against adversaries. Failing to protect these requirements risks ceding the initiative to our adversaries.

People

Imagine a future analyst working alongside an AI model to monitor People's Liberation Army (PLA) cyber capabilities. The model shows the analyst signs of new adversary malware targeting U.S. critical infrastructure. The analyst disagrees. But the analyst cannot explain why they disagree because they haven't been trained in basic data science, statistics, and the foundations of AI/ML. It's the equivalent of a lawyer who never went to law school arguing a case.

Sadly, modern analytical tradecraft and even professional military education tend to focus more on discrete cases more than statistical patterns and trends. There is a tendency to treat technology like magic. As a result, model outputs are either sacred or evil creating a risk of skewed inferences across the national security enterprise. There is little to no discussion about the tradeoffs between model interpretability and accuracy, a critical task in national security crises prone to uncertainty and deception.[2] In other words, unleashing a new suite of AI/ML tools inside the national security enterprise will produce diminishing returns unless we retrain the workforce and teach them how to use model-generated insights to refine human judgment.

[1]Benjamin Jensen, Scott Cuomo, Christopher Whyte. *Information in War: Military Innovation, Battle Networks, and the Future of Artificial Intelligence* (Washington: Georgetown University Press, 2022).
[2] Giorgos Myrianthous. "Understanding The Accuracy-Interpretability Trade-Off" *Towards Data Science* October 6, 2021 <https://towardsdatascience.com/accuracy-interpretability-trade-off-8d055ed2e445> .

WWW.CSIS.ORG 1616 RHODE ISLAND AVENUE NW WASHINGTON, DC 20036 TEL. (202) 887.0200 FAX (202) 775.3199

Our adversaries face the same challenge. The intelligence and military profession need a paradigm shift if they are going to take full advantage of AI/ML. The good news is that despite "precision recruitment" efforts to attract college students, the PLA struggles to integrate and retain them in its formations.[3] The smart kids in China aren't rushing to join the army. Russian tech workers fled the country to avoid fighting an unjust war in Ukraine.[4] The bad news is that the knowledge required to retrain spies and soldiers is open and accessible even to non-state actors. The first actor to embrace the paradigm shift in military art and analytical tradecraft could gain a generational strategic advantage.

Bureaucracy

Imagine what the Cuban Missile Crisis would look like in 2030 with all sides using a wide range of AI-applications ranging from imagery recognition to logistics management and generative analysis of adversary intentions. There would be a tendency to speed up the crisis even when it might make more sense to slow down decision-making and be more deliberate. Computational propaganda and tailored media would increase public pressure on political officials. At a more technical level, there would be a need to constantly adjust and recalibrate models as adversaries shifted their tactics, techniques, and procedures and both sides operated outside of the norm. Crisis events are by definition outliers creating challenges for statistical analysis. Confusion could eclipse certainty unleashing escalation and chaos.

Unfortunately, neither our modern national security enterprise nor the bureaucracy surrounding government innovation and experimentation are ready for this world. If the rank-and-file analyst and military planner struggles to understand prediction, inference, and judgment in and through algorithms, the challenge is even more acute amongst senior decision makers. At this level, most international relations literature and diplomatic history show us that the essence of decision is as much emotion, flawed analogies, and bias as it is rational interests defined by power or the structure of the international system.[5]

There are even larger challenges with creating a bureaucracy capable of adjusting algorithms to match new contexts during a crisis. Because of complexity and uncertainty, all models will require a constant stream of data and updates to their weighting. The speed of update will dictate the terms of advantage. Slow adapters will succumb to quick deaths on the future battlefield. The side with

[3] Marcus Clay, Dennis Blasko, and Roderick Lee "People Win Wars: A 2022 Reality Check on PLA Enlisted Force and Related Matters" *War on the Rocks* August 12, 2022 < https://warontherocks.com/2022/08/people-win-wars-a-2022-reality-check-on-pla-enlisted-force-and-related-matters/>

[4] Gian M. Volpicelli "Russia is Facing a Tech Worker Exodus" *Wired* March 23, 2022 < https://www.wired.com/story/russian-techies-exodus-ukraine/>; Masha Borak "How Russia Killed Its Tech Industry" *MIT Technology Review* April 4, 2023 <https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/>

[5] Keren Yarhi-Milo. *Who Fights for Reputation? The Pscyhology of Leaders in International Conflict* (Princeton: Princeton University Press, 2018); ibid *Knowing the Adversary: Leaders, Intelligence Organizations and Assessments of Intentions in International Relations* (Princeton: Princeton University Press, 2014); Robert Jervis. *How Statemen Think: The Psychology of International Politics* (Princeton: Princeton University Press, 2017); Yuen Foong Khong. *Analogies at War: Munich, Dien Bien Phu, and the Vietnam Decisions of 1965* (Princeton: Princeton University Press, 1992); Hans Morgenthau. *Politics Among Nations* (New York: Knopf, 1948); Kenneth Waltz. Theory of International Politics (New York: McGraw-Hill, 1979).

the model that updates faster than the enemy will generate tempo and freedom of action. A culture of experimentation and constant model refinement and adjustment will be the key to gaining and sustaining relative advantage in the future.

In fact, Ukraine has shown us this truth. A network of civilian software engineers, non-profits, and soldiers built the Delta platform and constantly refined their ability to use AI on the battlefield while waging a war of survival.[6] They could move fast because they were willing to experiment and fail. Ask yourself, do we have a similar culture of experimentation across our military and intelligence organizations?

Data Instructure

Imagine the hunt for mobile missile launchers in a future crisis. A clever adversary knowing they were being watched could poison the data used to support intelligence analysis and military decision making. They could trick every computer model into thinking a school bus was a transporter erector launcher (TEL) causing decision makers to lose confidence in otherwise accurate model-generated insights. Even when you are right 99% of the time, the consequences of being wrong once can still add unique, human elements to rational decision making and risk assessments.[7]

AI/ML is only as powerful as the underlying data. The larger and more diverse the dataset, the more opportunities there are for analyzing it in higher dimensions. Instead of an X and Y axis we all learned in geometry there might be thousands of matrix vectors. Each new dimension allows the model to identify signatures buried in the data. Each new signature is a potential intelligence advantage.

Yet, to collect, process, and store that data will produce significant costs going forward. First, it will mean an increase in the number of intelligence collection missions required to capture data using both open source and more sensitive methods. It will require clear data labeling and architecture standards to make it easy to compare diverse inputs. Bad bureaucracy and policy can kill great models if they limit the flow of data. And it will require access to computational power at scale as analysts move to adjust their models during a fluid crisis and in the face of clever adversaries using the equivalent of digital terracotta armies to poison AI/ML intelligence models.

[6] "Ukraine to introduce Delta situational awareness system for military" *The Kyiv Independent* February 4, 2023 < https://kyivindependent.com/government-introduces-nato-standard-delta-management-defense-system/>; Julian Borger "Our weapons are computers: Ukrainian coders aim to gain battlefield edge" *The Guardian* December 18, 2022 < https://www.theguardian.com/world/2022/dec/18/our-weapons-are-computers-ukrainian-coders-aim-to-gain-battlefield-edge>.

[7] Karma Dajani and Sjoerd Dirksin. *A Simple Introduction to Ergodic Theory* (2009) < https://webspace.science.uu.nl/~kraai101/lecturenotes2009.pdf>; Merle van den Akker "Ergodicity: What Does It Mean for Behaviorial Science?" *Money on the Mind* September 9, 2021 < https://www.moneyonthemind.org/post/ergodicity-what-does-it-mean-for-behavioural-science>; and Pete Combe II, Benjamin Jensen and Adrian Bogart. *Rethinking Risk in Great Power Competition* (Washington: Center for Strategic and International Studies, 2023) < https://www.csis.org/analysis/rethinking-risk-great-power-competition>.

Algorithmic warfare is not static. The only good models will be ones that continually update based on a constant flow of data. In fact, the data centers required to make these adjustments will become prime targets for cyber operations and even kinetic strikes in future wars.

The authoritarian nations challenging United States have an advantage in centralizing and controlling data. This bureaucratic centralization gives them the ability to focus resources and test different models and AI/ML applications. For example, China uses a centralized planning model to promote AI development for everything from economic growth to domestic surveillance and military modernization.[8] At the same time, this centralization makes the system brittle. Closed systems are more focused and secure, but they struggle to learn. Yet, learning is the name of the game in artificial intelligence. The balance between open and closed approaches to AI and national security will have to grapple with this tradeoff between the adaptability of open systems and the security of closed system architectures.

Conclusion

Prometheus has already shared the fire. Adversaries now and into the foreseeable future will attack us at machine speed through a constant barrage of cyber operations, mis/dis/mal information as well as entirely new forms of anti-access/area denial kill webs that fuse open source and sensitive intelligence to direct swarm attacks at civilian and military targets.[9] Unless the United States is able to get the right mix of people, bureaucratic reform, and data infrastructure those attacks will test the very foundation of the Republic.

I am confident the United States can get it right. In fact, the future is ours to lose. Authoritarian regimes are subject to contradictions that make them rigid, brittle, and closed to new information. Look no further than Chinese generative AI regulations that require an adherence to socialist thought.[10] These regimes are afraid to have the type of open, honest dialogue this committee is promoting. This fear is our opportunity. Creating a vibrant marketplace of ideas will help calibrate the right mix of regulation to protect the critical requirements the United States needs to integrate AI into the national security enterprise.

---

[8] William Carter and William Crumpler. *Smart Money on Chinese Advances in AI* (Washington: Center for Strategic and International Studies, 2019); Nicholas Wright (ed) *Artificial Intelligence, China, Russia, and the Global Order* (Montgomery: Air University Press, 2019); Elsa Kania. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Washington: Center for New American Security, 2017).

[9] Brandon Valeriano, Benjamin Jensen, and Ryan Maness. *Cyber Strategy: the Evolving Character of Power and Coercion* (New York: Oxford University Press, 2018); Charles Cleveland, Benjamin Jensen, Arnel David, and Susan Bryant. *Military Strategy in the 21st Century: People, Connectivity, and Competition* (New York: Cambria Press, 2018); Philip N. Howard and Samuel Woolley. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2018). John Arquilla and David Ronfeldt. *Swarming and the Future of Conflict* (Santa Monica: RAND Corporation, 2000); Sean J.A. Edwards. *Swarming and the Future of Warfare* (Santa Monica: RAND Corporation, 2005); Bryan Clark, Dan Patt, and Harrison Schramm. *Mosaic Warfare: Exploring Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington: Center for Strategic and Budgetary Analysis, 2020); and Benjamin Jensen and John Paschkewitz. "Mosaic Warfare: Small and Scalable are Beautiful" *War on the Rocks* December 23, 2019 <https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/>.

[10] Meaghan Tobin "China announces rules to keep AI bound by 'core socialist values'" *Washington Post* July 14, 2023 < https://www.washingtonpost.com/world/2023/07/14/china-ai-regulations-chatgpt-socialist/>.