

[BLOGS](#)[PODCASTS](#)[REGIONS](#)**THE
NATIONAL
INTEREST**[MILITARY](#)[POLITICS](#)[TECHNOLOGY](#)

Why Analytic Superiority Matters Most in the AI Race

July 6, 2026

By: [Emily O. Goldman](#), and [Robert L. Grossman](#)

Integrating artificial intelligence of varying capacities may outshine investing in the most powerful models.

<https://nationalinterest.org/blog/techland/why-analytic-superiority-matters-most-in-the-ai-race>

The United States is in a race it does not fully comprehend. It is a race for analytic superiority—not for the most powerful [artificial intelligence](#) (AI) model, or for artificial general intelligence (AGI). AI's transformational potential is comparable to radio and computing in importance, but AI does not confer an enduring advantage without analytic superiority. America's adversaries are already deploying AI models at scale, learning in real time on the battlefield and testing on their own populations. US national security and military leaders should adopt analytic superiority as a north star to gain a decisive advantage and avoid strategic surprise.

What Is Analytic Superiority?

Analytic superiority is a state of relative advantage achieved from the systematic analysis of data to build models and deploy them toward an operational or strategic end. In the language of the military professional, analytic superiority is the operational and informational advantages gained from collecting and processing data, building powerful analytic models, and deploying the models into military systems to achieve tactical, operational, and strategic objectives, while degrading the ability of adversaries to do the same.

Data-driven models in warfare are not new. Statistical models increased the precision of artillery fire in the 19th century. In 2007, the National Security Agency's [Real Time Regional Gateway](#) helped defeat the threat of improvised explosive devices in Iraq by fusing and processing in-theater data from signals intelligence, raids, satellite images, and on-the-ground reports of enemy movements, cutting the time to get information to

the warfighter from days and weeks to hours and even minutes. Today, the US national security community is laser-focused on the most powerful AI models, but analytic models of all sorts are pervasive in contemporary warfighting systems.

[The 2024 Defense Science Board Task Force on Future Cyber Warfighting](#)

[Capabilities](#) called for analytic superiority in the cyber domain, and we elaborated in [Cyber Defense Review](#) that powerful models alone do not provide an advantage in competition, crisis, or conflict. Others make a similar claim. [Michael Horowitz](#) ([with Lauren Kahn](#)) argues that the real race is not for the most powerful models, where the United States is leading, but in the race for adoption. [Jon Rosenwasser](#) warns that China is pulling ahead in AI adoption and diffusion. [Kyle Chan](#) testified that China lags American frontier models but is ahead in model efficiency, AI adoption, and AI integration into the physical world. Chan said China and the United States are pursuing different AI strategies. But they are really pursuing different analytic superiority strategies.

Many are raising an alarm, but what is the practical path ahead? National security professionals must first reframe the AI race as a contest for analytic superiority. Otherwise, the United States risks losing to adversaries that build many more specialized models rather than a handful of much more powerful models, that use manufacturing capacity to achieve greater diffusion of their models, or that focus on algorithmic advances rather than chasing ever larger data centers.

How Thought Experiments Corroborate the Necessity for Analytical Superiority

Two thought experiments drive home the importance of analytic superiority.

First, imagine the US military applying the latest frontier AI models to support commanders and AI-powered logistics for a distant conflict. On the contrary, imagine an opposing force applying advances in small- or mid-scale large language models to put “good enough” models into mobile phones and network them to leverage collective AI and overwhelm US forces in the opening hours of a conflict. Who would have the advantage? A [January 9, 2026 memo](#) from Secretary of Defense [Pete Hegseth](#) to Pentagon leaders calls for “AI Model Parity”: “We must have the latest and greatest AI models deployed for our warfighters.” But the most advanced models do not guarantee victory. It will be the force that develops, deploys, and disseminates capable models and implements an analytic strategy to deploy the models into enterprise systems, forces, and operational commands for specific outcomes.

A **second** thought experiment involves Claude’s [Mythos model](#) and [widespread concern](#) over its release. Data analysts and engineers appreciate that Claude’s models produce high-quality computer code and will continue improving rapidly. Mythos’ discovery of zero-days in multiple software applications caught many by surprise. Yet it should have been very clear that a frontier model would soon emerge that could easily identify multiple zero-days, and that adversaries could [flip](#) any such AI capability to create attacks. What is not clear is how to achieve an advantage over adversaries with models like Mythos: how to defend and patch your infrastructure at the speed of AI-powered attacks, and how to attack your adversary’s infrastructure by leveraging AI. Reports suggest [smaller AI models](#) that are specialized

to find exploits can discover some of the same zero-days as Mythos. So, it is unclear whether the most powerful AI model would guarantee a decisive advantage over an adversary that deploys and diffuses smaller, more specialized “frontier-lite” models tailored for selected targets, such as attacking your computing infrastructure.

What Framework Can Achieve Analytic Superiority

Analytic superiority focuses on building complete systems for well-defined objectives. Our first vignette (the latest and greatest AI model processing Blue Force’s Intelligence, Surveillance, and Reconnaissance feeds and creating target lists versus good enough AI models in each red force handheld networked together for real-time intelligence, situational awareness, and suggested actions) juxtaposes two analytic strategies. Neither is inherently superior because there is no one way to achieve analytic superiority. Military, intelligence, commercial, and scientific organizations should aim to deploy the best AI model over the most reliable data available to achieve a mission objective. In other words, a good enough model in production beats a better model in the lab; a good enough model with access to the data it needs for deployment beats a better model whose data lags; a small or midscale model over high-quality data beats a larger model over worse data; and usually, a decent analytic model running with great data beats a great analytic model with decent data.

Working through these trade-offs is easier with a framework like the [Analytic Diamond](#), which one of us developed and used to deploy machine learning and AI models in financial services, cybersecurity, healthcare, logistics, and defense applications. In this framework, the analytic model is one of four elements that contribute to analytic superiority. The others are analytic operations, which use models as a basis for designing and optimizing systems and processes to achieve desired effects; analytic infrastructure, which is the computing infrastructure that runs the models and operations; and analytic strategy, which prioritizes which analytic opportunities are of greatest value to the organization. The Russia-Ukraine drone war has involved integrating better and better AI models but also changing computing infrastructure (e.g., replacing RF communications with fiber-optic communications) and innovating supporting operations (e.g., using low-tech means such as [fishing nets](#) to defeat AI-powered drones).

Without analytic operations, an AI model, no matter how good, cannot achieve the intended outcomes. Discovering, prioritizing, and patching zero-days are all analytic operations that consist of steps (or [agentic workflows](#)), each done by AI agents connected to AI models, and each requiring an extremely capable analytic infrastructure. Analytic operations for offensive cyber operations enable much less powerful models than Mythos to be quite effective. [David Mussington](#) shows that with the appropriate analytic operations, a mid-tier open-weight model can chain together vulnerabilities and orchestrate effective end-to-end attacks. These days, the term harness is being used for the software infrastructure layer that turns an AI model into a useful system, agent, or team of agents. From this perspective, analytic operations

include the harness as well as all the other software systems and processes needed to achieve desired outcomes.

The most neglected element of analytic superiority is strategy. Analytic superiority is a strategic problem that requires ruthless prioritization and a “Commander” or “CEO” perspective. Many organizations have sensor, data, cloud, and AI strategies, yet often these are stove-piped and untethered from an organizing principle like analytic superiority that drives sub-strategies together for decisive advantage. Without an analytic strategy, a military organization pursuing the latest and greatest model may lose sight of the analytic competition pitting its capabilities against an adversary actively trying to defeat its strategy.

Which Actions Are Crucial Now for Winning the AI Race

Integrating analytic models, infrastructure, operations, and strategy is a tall order, but some immediate steps can guard against strategic surprise.

First, actively work to balance an exclusive focus on the largest and latest models from a few vendors, when smaller specialized models may perform as well, with less cost and effort, and be much easier to update.

The [scaling laws of OpenAI](#) and [Google DeepMind](#) spurred the drive for ever-larger AI models with ever more GPUs, requiring ever more energy. Recent work by one of us introduces a quality-aware [scaling law](#) quantifying how, with high-quality data, AI models with orders of magnitude fewer parameters—requiring much fewer GPUs and much less power—can perform as well as much larger frontier models. Smaller specialized models are much faster to train and update. Distillation is another method that uses a large general-purpose large language model (LLM) to train smaller LLMs and produce smaller models for use in specific domains. US adversaries have used distillation to reduce the effort to build their own models. Also, [many advances](#) in LLMs have come from academia or small vendors that lack the large-scale infrastructure of frontier model vendors. Don’t let this be a surprise: adversaries will most certainly leverage some of these advances, as well as advances that are not generally known.

Second, avoid chasing AGI when a frontier model or a more specialized AI model can deliver a decisive advantage. The value of the latest and largest frontier models is critical, but so is achieving the right mix between frontier models and more specialized models.

Third, improve analytic operations by quickly deploying good enough models into systems and continuously improving them. This will always contribute more to analytic superiority than a better model still in the lab or with less capable analytic operations.

Finally, assess how widely models are diffused across enterprise systems and operations. Diffusion density is the ratio of the number of systems that deploy AI models divided by the number of systems that could benefit from AI. Many [accounts](#) rank China

higher than the United States on diffusion density. A key role of analytic strategy is to prioritize diffusing AI into those systems most consequential for winning. The AI landscape is littered with expensive failures. Models and data are not enough to win. The key to analytic superiority is not faster computers, better models, or more data. It is the combination of these factors and their integration into operational systems that provides a decisive advantage. The United States can achieve analytic superiority, but this requires adopting a perspective focused on analytic workflows, systems, and infrastructure—as well as models—while degrading and defeating those of adversaries. This is the race the United States is in and must win.

About the Authors: Emily Goldman and Robert Grossman

Emily O. Goldman combines national security experience and policy scholarship, gained and applied at the National Security Council, the Department of State, US Cyber Command, the National Security Agency, and the University of California, Davis. She has published and spoken on strategy, technology diffusion, and cyber operations, and has implemented the resulting concepts for more than two decades.

Robert L. Grossman is the Frederick H. Rawson distinguished service professor in medicine and computer science and the Jim and Karen Frank director of the Center for Translational Data Science at the University of Chicago. He founded Open Data Group in 2002 and was its managing partner from 2002-2015, where he led teams to develop and deploy machine learning and AI models in financial services, cybersecurity, healthcare, logistics, and defense applications.