At the U.S. Air Force and U.S. Space Force's Officer Training School, civilians and prior enlisted Servicemembers with college degrees undergo a rigorous 60-day training program, culminating in their commissioning as officers (U.S. Air Force/Damien Thomas)

From Data to Victory
The Race for Analytic Superiority in Warfare

By Emily O. Goldman and Robert L. Grossman

Artificial intelligence (AI) technologies have reached a tipping point after decades of development. They are diffusing widely and finding new military and intelligence applications. As more powerful models built on ever larger data sets become ubiquitous, militaries are racing to deploy AI. But that is the wrong race. They should be racing to achieve analytic superiority. By *analytic superiority* we mean the advantage obtained from the ability to collect and process data, build powerful analytic models, and deploy the models into military systems to achieve operational and information advantage while degrading or denying an adversary's ability to do the same.[1] Military systems include both information and physical systems.

Analytics is the systematic analysis of data through computational methods to produce models for use across a spectrum of applications, from improving performance of physical systems for operational superiority to improving performance in information systems for decision superiority. The volume, velocity, and variety of data, combined with ever more powerful models, has made analytic superiority the critical element for both operational and information superiority.

Emily O. Goldman is a Cyber Strategist at the National Security Agency. Robert L. Grossman is the Director of the Center for Translational Data Science at the University of Chicago.

The competition for military superiority has always been an intellectual and technological endeavor, as Andrew Marshall, director of the Office of Net Assessment, argued in the mid-1990s. Marshall predicted "information superiority" would occupy operational art because connectivity was essential for precision strike.[2] Military strategy must now embrace analytic superiority. To assist the warfighter in this, we describe the enduring importance of analytics in warfare and offer a roadmap to achieve analytic superiority.

Algorithms and Analytics in Warfare

Twenty-first century warfighters rely on analytic models, whether they know it or not, at all levels of systems and subsystems they use, at all echelons, and in all domains. Yet warfighting, in fact, has always used algorithms and analytics, even before the age of computers and digitization. An *algorithm* is a precise set of instructions that takes inputs and produces outputs. *Analytics* is a relatively recent term for a broad range of approaches that analyze data to produce models for tasks like prediction, summarization, and optimization.

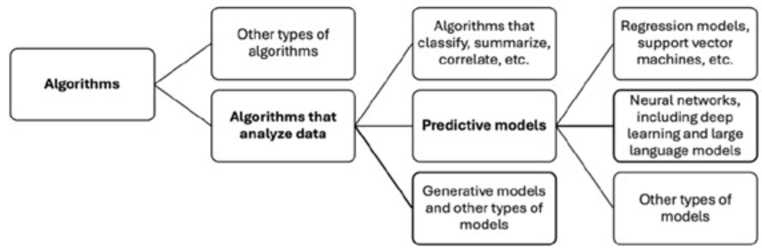
Data analysis was first done by hand, and then with simple mechanical devices like slide rules. In the American Civil War, range firing tables increased targeting accuracy with numerical integration algorithms and statistical models based on data collected and processed from experimental firings of the canon.[3] In World War II, British air defense benefited immensely from the use of radar, but just as important were algorithms, heuristics, information flows, and command and

Corporal Joseph McNutt, USMC, an intelligence specialist with 3rd Reconnaissance Battalion, 3rd Marine Division, flies a Neros Archer first-person view drone on Camp Schwab, Okinawa, Japan, May 22, 2026 (U.S. Marine Corps/Haley Munoz) control that developed around radar. The Tizzy angle, a simple heuristic algorithm used to plot the course of British fighters intercepting German bombers during World War II, increased the interception rate to approximately 90 percent (when the altitude of the bomber was known) and reduced the time to set the interception course by several minutes.[4]

Fast forward to today and the Russia-Ukraine War, where Ukraine reportedly applied AI image models to overcome remotely piloted drones' vulnerability to jamming. While outside the range of Russian jamming, a Ukrainian remote operator transfers control of the drone to a computer vision model that locks onto pixels ("pixel-lock") in an image of the target captured by the drone's camera.[5] AI image models are the basis for pixel-lock technology, which has been available since the 1970s in more expensive systems. The U.S. startup Auterion partnered with the Ukrainian company Vyriy Drone to mass-produce drones with Skynode software that uses pixel-lock techniques.[6] By employing new analytic models and changing analytic operations to pixel-locking instead of remote guidance by radio signal, Ukraine's drones defeated Russia's electronic warfare jamming. This is but one example of analytics employed by both Ukraine and Russia in drone warfare.

With the ubiquity of analytics in digital systems and services, *analytic competition*—the race to deploy analytics in operations to achieve mission effects and degrade and defeat adversary analytics—has become a critical dimension of strategic competition. The changing character of war is a story of competitive innovation—in strategy, operations, tactics, weapons, and analytics. Although less familiar to the warfighter, the competition to deploy analytics in operations to achieve mission effects and degrade and defeat adversary analytics is ongoing and accelerating. Yet there is no single way to achieve analytic superiority, just as there is no one way to achieve military superiority. Competitors will employ analytic models in different ways. This is a key lesson of the People's Republic of China's DeepSeek generative AI model, which caught the world by surprise and disrupted the AI industry in 2025. On the other hand, from the vantage point of analytic superiority, it should not have been a surprise that one of our adversaries would make an advance in AI that would catch us off-guard.

Figure 1. Types of algorithms



Source: Authors.

An Overview of the Evolution of Analytics

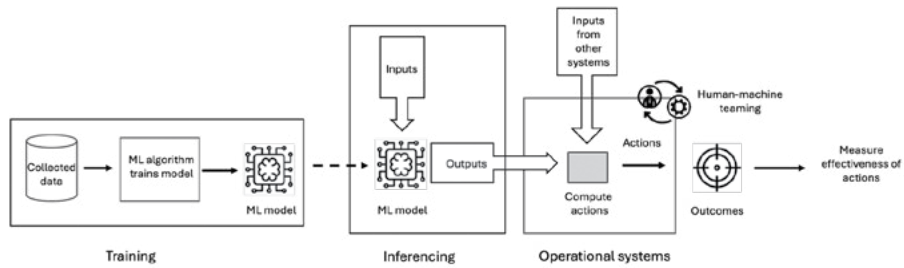
The purpose of this overview is to illustrate that many analytic approaches for processing data are available, they are continually evolving, their scale is growing, and the pace of innovation is accelerating. Expanding upon the definition above, an *algorithm* is a general concept that refers to a sequence of instructions to perform computations, process data, or solve problems that are precise enough for a computer to implement. Examples include computing the Tizzy angle and the numerical integration methods that compute firing tables. With the amount of data and computing power growing, the subclass of algorithms that process data is of special importance (see figure 1). In the examples above, firing tables and pixel-lock algorithms process data to produce models (paper models in the firing tables example and an AI model in the pixel-lock example).

More powerful digital computers dramatically increased the scale of data analysis and led to new analytic approaches like *machine learning* (ML).[7] The machine learning process collects data to build a model; uses the data to estimate a model (model training); uses the model to process inputs and produce outputs (model inferencing); and deploys the model in a system to derive operational value (model deployment) (see figure 2). Machine learning models, unlike traditional statistical models, can scale to very large datasets and build models that, for example, can accurately predict, classify, summarize, and correlate complex patterns and behavior.[8]

One example of a machine learning algorithm is a predictive model for threat detection. It can be built by analyzing user behavior in a computer network (training) and applied in real time (inference) to give a score that predicts the likelihood the user is an insider threat. Another example is a classification model. It takes an image as input and identifies whether the image contains a jeep, truck, tank, another prespecified type of vehicle (the label), or a label that indicates none are present. A *neural network* is a specific type of machine learning predictive model that processes data in layers, with each layer a very simplified mathematical model of a neuron. *Deep learning* is a type of neural network that uses many sequential layers to process data.

A *large language model* (LLM) is a machine learning predictive model built from a large amount of text, such as the text arising from crawling the internet. With enough data and compute to estimate models with billions of parameters, these models have a wide array of applications. Based on empirical "scaling laws,"[9] LLMs improve as the number of parameters grows, assuming enough data and computing capacity. Given their size, machine learning models often use a multistage training process. A pretraining stage builds general purpose models. A supervised fine-tuning stage hones pretrained models to perform well on a selected task. Although pre-training of models with hundreds of billions of parameters requires very large-scale computational infrastructure, supervised fine-tuning can be done with much more modest resources. A generative model is yet another type of machine learning model that takes a dataset as input and produces a statistical model of the data as the output, which can be used to generate new, similar examples of the data, for example produce images and videos from text prompts.

Figure 2. Machine learning process steps: training, inferencing, and deploying models into operational systems



Source: Authors.

Agentic AI is another evolution of analytics.[10] These systems autonomously pursue goals, make decisions without human input, interact with and respond to their environment, and adapt based on new information or changing circumstances.[11] Agentic AI is sometimes likened to human reasoning, but it really represents the confluence of ever larger AI models, of new algorithms such as chain of thought, and of orchestration frameworks that interoperate AI models with other systems like websites, databases, and planning applications. Rarely does an ML/AI model replace a human, but rather particular human tasks are automated or augmented using an AI model.[12] The human may be part of the process (human in the loop), supervise the process (human on the loop), or be able to intervene in the process depending upon certain conditions (human near the loop).[13]

A further advance involves two or more AI systems interacting, or *collective AI*. For some time, the outputs of one AI system have been used as inputs for another AI system.[14] More recently, AI systems are being developed that interact with multiple other agentic AI systems, each interacting with their environment and pursuing independent goals, while communicating to pursue collective goals. For example, a drone swarm powered by agentic AI systems could exchange information across the swarm.

To achieve military advantage from machine learning and AI, models must be deployed into systems that take actions. The effects of the actions are then quantified and measured (see figure 2).[15] Models typically produce scores, which are inputs to a system that takes an action when the score crosses a threshold. For example, an AI model embedded in a first-person view drone locks onto a pixel patch in an image and autonomously steers the drone to hit the object identified in the marked pixel patch.[16] The model takes an initial frame that is locked in the video stream, a later frame from the video stream, and pixel patch in the initial frame associated with an object, such as a tank. It produces a score for each pixel patch in later frames,[17] which is the likelihood that the pixel patch in the later frames is the updated position of the marked pixel patch in the original locked frame. A system module in the drone processes these scores to select the updated position of the tank and provide the data required to steer the drone (the actions) until the process repeats with a later frame. The measure is whether the tank is hit.

From an analytic superiority perspective, it is not necessary to have the latest or most advanced model. It is more important to have a deep understanding of the data to build a good enough model that can be deployed into an operational system or process to achieve an outcome. As an example, smaller specialized AI models were able to find some of the same long-standing and critical cybersecurity vulnerabilities that Anthropic's Mythos AI Model found in the spring of 2026.[18]

Large language and foundation models are generating remarkable innovations, but they have limitations. First, like any predictive model, LLMs can be wrong, but their incorrect responses retain the nuance and grammatical flow of language. These "hallucinations" are a natural consequence of how LLMs are built.

What are known as scaling laws quantify how the accuracy of LLMs improves as the size of the models grows, as the amount of data they are trained on grows, and as the quality of the data grows.[19] Larger models require large-scale computing infrastructure, and this is widely appreciated. Less well known is that many LLMs are data-starved; that is, they lack sufficient high-quality data, even though today's LLMs are trained on a wide array of data sources in addition to crawling the internet (for example, publicly available government data, open access technical publications, licensed sources of data such as books, purchased data, and text extracted from audio and video). Since the amount of data can be reduced by increasing the quality of data, by putting effort into increasing data quality, smaller more specialized models can be built for specific domains and applications that often perform as well or better than the large frontier models.[20]

Training LLMs also takes months, so many are out of date, leading to simple errors on ongoing events. Other factors that reduce accuracy are the various simplifications and shortcuts used to produce answers while keeping operating costs low.

Finally, evaluation and verification frameworks are essential to building high-quality LLMs. One reason LLMs that produce computer code have become so powerful is because of the large amount of training data available online and the relative ease of checking whether answers are correct. In specialized domains such as warfighting, the lack of large amounts of high-quality data is a fundamental limitation.

Analytic Superiority for the Warfighter

How should the warfighter incorporate analytics into doctrine and practice? First, the defense enterprise needs a framework to help avert common sources of failure. Second, leaders must decide where to employ an organization's limited analytic capabilities. This requires an analytic strategy that prioritizes which analytic opportunities will provide the most value to the organization. Third, new AI-based capabilities must be integrated into combat functions. We address each of these in turn.

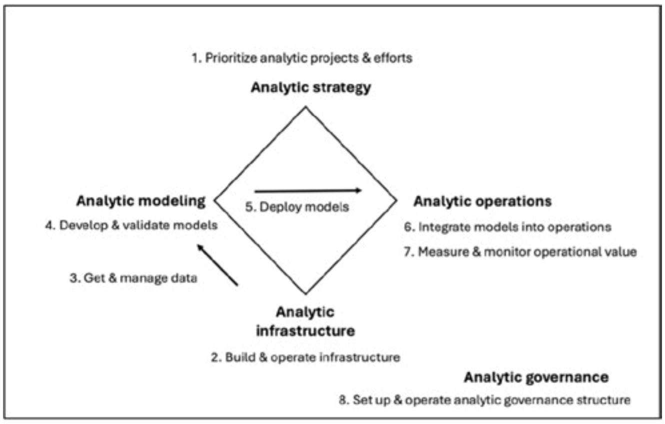
The Analytic Diamond Enterprise-Level Framework for Achieving Analytic Superiority

Analytic models are one element of analytic superiority. Building and deploying a successful model is like climbing a ladder. The first step is a successful software project; the second is a successful data management project; the third is a successful machine learning project. Any step can fail, and they often do[21] for some common reasons:

- The data collected to build the model is of low quality, insufficient quantity, or unavailable when inferencing.
- The information technology (IT) infrastructure to manage the data, build the model, and deploy the model is not available or lacks the scalability required for the application.

U.S. Marine Corps Lance Corporal Gabriel Demopoulos (left) and Corporal Humberto Castro both with 3rd Battalion, 7th Marine Regiment, forward deployed with 4th Marine Regiment, 3rd Marine Division as a part of the Unit Deployment Program, fly Neros Archer first-person view drones on Camp Schwab, Okinawa, Japan, May 22, 2026. This training sharpened their ability to operate advanced FPV drones that provide reconnaissance and precision strike capabilities. (Photo by U.S. Marine Corps Lance Cpl. Haley Munoz)

Figure 3. Analytic diamond framework



Source: Authors.

- The model lacks accuracy, specificity, or other performance parameters.
- The model is never transitioned from the lab to the application or service that requires it.
- The model is not integrated effectively into operational systems.
- The human-machine teaming is not effective, or the training provided is not sufficient to use the systems as planned.

In addition, each step in the machine learning process (as well as other steps in the analytic framework that we describe below) can be attacked by an adversary.

Averting failure is easier if one adopts an enterprise-level framework, such as the *analytic diamond* (figure 3) that captures all the required tasks for analytic superiority.[22] These include developing an analytic strategy that aligns with the organization's goals and prioritizes analytic efforts; setting up the computing infrastructure to manage the data, build the models, and support the inferencing; getting the data required for the models; cleaning and preparing the data and building the models; and deploying the models into operational systems or processes. This last step usually involves a hand off from the analytic modeling team that builds the model to the analytic operations team to integrate model inferences into processes or operational systems; develop tactics, techniques, and procedures for operationalizing the model; and devise an appropriate human-machine teaming/autonomy framework. An analytic governance structure manages and coordinates all these steps.[23]

Google's most important advances demonstrate the analytic diamond framework. In 2003, the company unveiled the Google File System, a new analytic infrastructure to analyze data at a scale not previously possible, which gave Google a significant competitive advantage.[24] In 2008, the company introduced the MapReduce algorithm,[25] which leveraged the Google File System and significantly sped up algorithms like Google's PageRank algorithm[26] (an example of an analytic model), which is the basis of its web search system (an example of analytic operations). The MapReduce algorithm also enabled Google to efficiently implement other analytic operations such as Google News, Google Translate, and processing data for viewing satellite images. Google's competitors did not have access to these technologies until the open-source Hadoop system[27] was introduced. By that time, Google had advanced to next generation versions of its core technology.

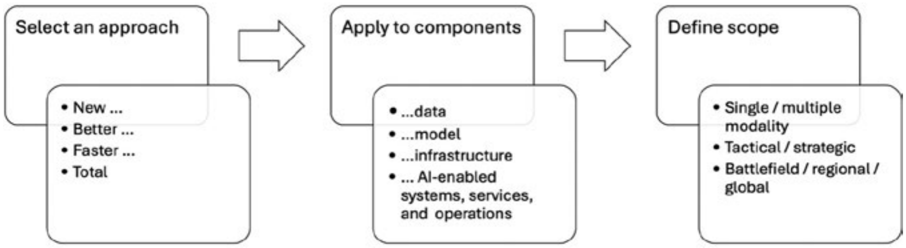
The analytic diamond applies to commercial and military organizations alike, with an important difference. Each step in the analytic diamond typically occurs in different organizational units: an IT organization builds the infrastructure; a modeling organization builds the models; and an operations organization deploys the models. In military organizations, those units are likely to be stovepiped. Senior military leaders need to not only understand and resource each of these interrelated steps; they must develop and implement an analytic strategy to guide and integrate across stovepipes.

Winning with Analytics Requires a Strategy

Analytic strategy sits atop the analytic diamond to emphasize its central importance for prioritizing which analytic opportunities will provide the most value to the organization. Analytic opportunities include investments in higher capacity or performance computing infrastructure, higher volumes or quality of data, higher accuracy models, a novel operational application of an analytic capability, or some combination that achieves a level of speed, scale, and performance to tackle a national-level priority. In a national security context, prioritizing analytic opportunities for investment should factor in threats, vulnerabilities, national goals, organizational missions, and how the military organization plans to fight (warfighting strategy). An analytic strategy can be applied at any echelon (Department of War, military Service, combatant command). It is an essential substrategy of any modern military organization.

The analytic diamond can help leaders construct analytic strategies whether for a narrow task, a broad function, or an operational challenge. For each of the four corners of the diamond, one could pursue an approach that is novel, better, faster, or any combination of these. For example, "novel" strategies could introduce new sources of data like using Wi-Fi-based location services in dense urban environments where global navigation satellite systems may not be reliable; new sensor data, including light detection and ranging (LIDAR), radar, and electrical-optical images for AI models supporting autonomous vehicles; new algorithms (like MapReduce); or new analytic infrastructures (like the Google File System). "Better" strategies can take advantage of higher quality,

Figure 4. Different strategies for achieving analytic superiority



Source: Authors.

more complete, or more timely data; more accurate models; or more compute power in analytic infrastructure. "Faster" strategies could entail moving data more quickly (for example, custom fiber networks in high-frequency trading)[28] or updating models more rapidly (for example, updating cyber threat models daily or hourly).

Figure 4 offers a guide for combining different elements into a tailored strategy. An approach (novel, better, faster) is applied to a component (data, model, infrastructure, operations) and scoped to a scale that aligns to mission. For example, one could introduce a novel model that provides an advantage in battle, or a novel type of data integrated with a current data modality to provide an advantage at the regional level. Multiple combinations can be developed and integrated.

Some strategies try to capture *all relevant data*. One exemplar was Real Time Regional Gateway capability, deployed by the National Security Agency in Iraq in 2007 in response to the increased threat of improvised explosive devices.[29] The program collected, integrated, and analyzed as much data as possible from all relevant available sources in as close to real time as possible. Real Time Regional Gateway combined traditional streams of signals intelligence with new sources of information from raids, satellite images, and on-the-ground reports of enemy movements and operations. Processing the data in theater reduced the time it took to get information to the war fighter from days and weeks to hours or even minutes.

Other "total data" strategies include China's social credit system, which tries to capture all relevant data on China's citizens and residents, and Google's global data platform, which tries to collect and organize "the world's information and make it universally accessible and useful."[30] A more targeted, narrowly scoped strategy is Ukraine's pixel-lock drone approach, which focused on employing better models and better deployment. An even more targeted approach is the use of novel microwave infrastructure for high-frequency trading. Larger is not necessarily better; rather, it depends on what is achieved from the perspective of analytic superiority.

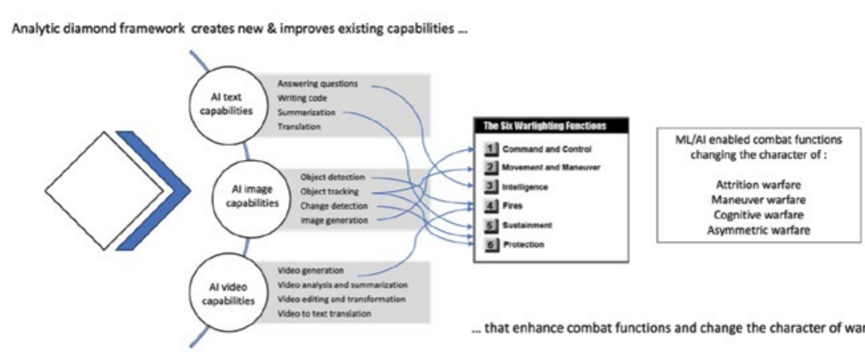
Alternatively, or in addition, one can attack the analytic tasks performed by the adversary, individually or in different combinations. The analytic diamond framework identifies ways to counter an adversary's analytics. For example, if both Blue Force (friendly forces) and Red Force (opposing forces) have AI models for writing intelligence assessments, Blue can build a more powerful model that integrates a new type of data and does it faster than Red, while Red can poison the data that Blue uses and pre-position exploits in Blue's analytic infrastructure that can be activated in times of conflict. Offensive strategies include infiltrating an adversary's analytic infrastructure, poisoning its data, weakening its analytic models, and degrading its analytic systems and services.

Integrating Analytics Into Combat Functions

Figure 5 illustrates how ML/AI can be leveraged to improve combat functions. New AI-based capabilities create more advanced, more powerful, or more adaptive combat functions, which are changing the character of war. Analytic superiority can deliver operational advantage by improving command and control, fires, logistics, movement, maneuver, evasion, cybersecurity, and force protection.

The U.S. defense and military communities are developing, experimenting, piloting, and deploying ML/AI into business and operational processes. Department of War AI projects include Project Maven[31] and the AI Rapid Capability Cell.[32] Automated intelligence-processing software, based on machine-learning algorithms developed under Project Maven, has supported counterterrorism operations.[33] ML/AI are being employed to improve a range of combat functions to include fires;[34] military decisionmaking;[35] distributed command and control in contested

Figure 5. AI-enabled combat functions and the changing character of war



Source: Authors.

U.S. Marines with 3rd Light Armored Reconnaissance, 1st Marine Division, Light Attack Helicopter Squadron 169 and Marine Special Operations Command conduct an in-aircraft system integration of a first-person view unmanned aircraft with a UH-1Y Venom helicopter at Marine Corps Base Camp Pendleton, June 16, 2026. (U.S. Marine Corps/Carlo SouzaDeluca)

environments;[36] supply chain, logistics, and sustainment for multidomain operations;[37] and protecting the cybersecurity kill chain.[38] For intelligence, ML/AI is being applied to improve intelligence summaries, situational awareness reports, strategic assessments, threat assessments, indicators and warnings, alerts, and operational intelligence reports. On December 9, 2025, Secretary of War Pete Hegseth announced the launch of GenAI.mil, a military-focused generative AI platform with initial capabilities from Google's AI application, Gemini, and directed all personnel to immediately incorporate it into all workflows to outpace adversaries.[39] Amid all the forward momentum, no overarching concept like analytic superiority guides resourcing and weight of effort. Without such a construct, militaries risk focusing in the wrong areas and falling victim to surprise.

Surprise

As warfighters employ ML/AI to enhance combat functions, they must anticipate and prepare for surprise. DeepSeek offers a cautionary lesson. Leading U.S. AI vendors were developing models based on scaling laws; they built ever larger models using ever larger clusters of graphics processing units (GPUs) with the price of developing an AI model rising to more than $100 million.[40] Meanwhile, the Chinese company DeepSeek—which itself is owned by a Chinese hedge fund, High-Flyer—took a different approach, developing new algorithms and methods that produced roughly competitive AI models at a much lower cost. DeepSeek's claim that its model cost $5 million to train accounted for only the last run that produced the model and so underestimates total cost. However, it is still likely a fraction of the investment that large U.S. AI frontier vendors were spending. The company presumably relied on U.S. frontier models to help train its models but still developed novel algorithms to make up for lack of access to the highest power GPUs at the scale typically required to build AI models. DeepSeek's model caused significant drops in share prices for some leading U.S. AI vendors. Nvidia's stock dropped 17 percent on January 27, 2025, one of the largest single-day dollar losses in U.S. history for any company. The fact that DeepSeek's model was open source immediately changed the competitive environment.

Given the many steps involved in moving from data to operational value, the increasing power of models, and the many ways to automate tasks and to augment humans with ML/AI (augmented intelligence), there are many paths to achieving analytic superiority and it is easy to be surprised. Your adversary may be more facile than you, more willing to change existing priorities and processes than you, and more competent at diffusing ML/AI than you. The rapid pace of innovation in AI—what might be called "analytic tempo"—has caught even AI experts off guard. It can be seen in the rapid introduction of new capabilities by the frontier AI companies, in the innovation of small and emerging AI vendors, and in the extremely fast-paced development of drone and counter-drone technology in the Russia-Ukraine War.

Mitigating surprise is an important component of achieving analytic superiority. This likely requires a paradigm shift focused on human-machine teaming to discover entirely new approaches to solving operational challenges, which is more than piloting and rapid prototyping. It is about rethinking how missions are executed, how decisions are made, how to build new capabilities that scale, and how AI systems collaborate with humans to create asymmetric advantages.[41]

Artificial General Intelligence and Analytic Superiority

Military professionals should not confuse analytic superiority with *artificial general intelligence* (AGI).[42] AGI, simply defined, is the ability of an AI model to understand or learn any intellectual task that a human can. Algorithms and models have been outperforming humans for decades. For 50 to 60 years, calculators have outperformed humans in arithmetic. For the past 40 years, software applications have performed better than humans at mathematical computations, including evaluating complex derivatives, integrals, and series. AI models are getting much better at doing mathematical proofs, but this is a continuation of a decades-long process.

AGI is not a simple milestone,[43] like developing the atom bomb. Instead, it is satisfying one of several definitions that involve passing multiple tests with certain scores, where the models are often designed to pass the specific tests. Many evaluation frameworks and leaderboards assess and track the progress of AI models. So-called frontier models perform 80 percent to 100 percent as well as humans on common tasks like handwriting, speech, and image recognition; reading comprehension; language understanding; common sense completion; grade school mathematics; and code generation. Models already perform most of these tasks at the college level or higher and will soon perform significantly better. In this simple sense, we are quite close to AGI. However, in terms of reasoning and creating like humans, significant gaps remain. It is not clear when, or even if, these gaps will be closed. Mathematicians are still in demand, and they use AI applications to create mathematics—a simple example of human-machine teaming.

From the viewpoint of efficiency and productivity, every job is a bundle of tasks[44] and the questions are which tasks are most important to automate and how AI can automate them. From the viewpoint of analytic superiority, what counts is the quality of models, how rapidly they improve, the efficiency of the infrastructure that computes them, and whether your models outperform your adversary's. Reaching some benchmark on an abstract evaluation framework does not matter. AGI does not provide advantage in warfare; analytic superiority does. A working deployed model always beats or provides more operational value than a better model still in the lab or not yet integrated into systems supporting operational art.

Autonomy frameworks can also be viewed in terms of analytic superiority.[45] Department of Defense (DOD) Directive 3000.09 provides safeguards for autonomous systems, including those using AI,[46] but as National Security Presidential Memorandum/NSPM-11—issued in June 2026—directs, these must be reviewed and updated annually to account for rapidly evolving AI capabilities.[47]

Conclusion

There is no substitute for battle to test and employ new technologies and capabilities. Innovations typically appear first in precursor wars between asymmetric powers and come to fruition in combat between peer competitors.[48] The Russia-Ukraine War represents a precursor war for the application of ML/AI. Ukraine used AI-enabled object tracking models in its first-person view drones in 2024 to circumvent Russian jamming of operator-drone communication.[49] In 2025, Russia regained an advantage by using a better analytic infrastructure of fiberoptic cables to provide communications to drones that could not be jammed.[50] By the time this article is published, the analytic competition in drone warfare will likely have evolved further. The war between Israel and Hamas provided another laboratory that hints at the value of ML/AI for military advantage. Israel's Unit 8200 seemingly increased the autonomy of AI-enabled fires by reducing the level of human confirmation required.[51]

For the warfighter, military planner, and commander, integrating analytic superiority into operational art is essential. The force that has the advantage from ML/AI is not the one with the most advanced models but the force that builds better and more capable models (analytic modeling); deploys them into applications, systems, and processes for desired outcomes (analytic operations); acquires, updates, and innovates the computing infrastructure (analytic infrastructure) to support these tasks; and adopts a strategy to prioritize among analytic opportunities (analytic strategy).

A useful exercise is to apply the analytic diamond methodology to the Secretary of War's January 9, 2026, memorandum, which outlines the Artificial Intelligence Strategy for the Department of War.[52] The strategy draws attention to two of the four corners of the analytic diamond—compute infrastructure and model development—and to the supporting processes of data access, deployment, and governance. The importance of robust experimentation to achieve AI-native warfighting is also highlighted, but without a framework that includes processes, best practices, and infrastructure for moving models into operations (a third corner of the diamond), experiments often do not end up in production systems or changing tactics, techniques, and procedures. Most importantly, the memo is silent on analytic strategy; it focuses on the "latest and greatest" frontier AI models, and it frames the endeavor as a race for AI dominance through using the most powerful model rather than achieving analytic superiority relative to an adversary. As we have argued, it is not about having the latest model available, but rather having a "good enough" model deployed in the right systems and processes in support of an analytic strategy. Without the North Star of analytic superiority, the Department runs the risk of racing toward AGI while our adversaries drive toward victory through analytic superiority.

We leave readers with a final thought experiment. Imagine Blue applying the latest frontier AI models to provide the best support to commanders and breakthrough next-generation logistics for a distant conflict, and Red applying the most recent advances in "small" large language models to put "good enough" models into mobile phones, using ad hoc networking to connect nearby mobile phones, and leveraging emerging collective AI to create an overwhelming analytic superiority in the first 24 hours of a conflict. Both sides have good analytic superiority strategies, but who would have the advantage in a military conflict? That is what the joint force should be anticipating, analyzing, and wargaming. **JFQ**

Notes

[1] Robert L. Grossman and Emily O. Goldman, "The Importance of Analytic Superiority in a World of Big Data and AI," *Cyber Defense Review* (Summer 2024): 1–49, https://cyberdefensereview.army.mil/Portals/6/Documents/2024_Summer/Grossman_Goldman_CDRV9N2-SE-Summer-2024.pdf.

[2] Andrew W. Marshall, "Memorandum for the Record: Some Thoughts on Military Revolutions," Office of the Secretary of Defense, August 23, 1993, https://stacks.stanford.edu/file/druid:yx275qm3713/yx275qm3713.pdf.

[3] Alan Gluchoff, "Artillerymen and Mathematicians: Forest Ray Moulton and Changes in American Exterior Ballistics, 1885–1934," *Historia Mathematica* 38, no. 4 (2011), https://doi.org/10.1016/j.hm.2011.04.001; Earl MacFarland, *Textbook of Ordnance and Gunnery* (New York: John Wiley and Sons, 1929).

[4] David Zimmerman, "Information and the Air Defence Revolution, 1917–40," *Journal of Strategic Studies* 27, no. 2 (June 2004): 370–94, https://doi.org/10.1080/0140239042000255968.

[5] James Marson and Daniel Michaels, "Killer Robots Are About to Fill Ukrainian Skies," *Wall Street Journal*, November 16, 2024, https://www.wsj.com/world/europe/ukraine-russia-war-ai-drones-9337f405.

[6] Marson and Michaels, "Killer Robots Are About to Fill Ukrainian Skies."

[7] For simplicity, we use the term "machine learning model," or if the meaning is clear from the context, simply the term "model."

[8] More technically, it is useful to distinguish two types of machine learning models: discriminative models and generative models. A *discriminative model* is a model that learns the probability of the output given the input. In contrast, a *generative machine learning model* learns the probability of the data distribution, enabling it to create similar data through sampling. See, for example, Andrew Ng and Michael Jordan, "On Discriminative vs. Generative Classifiers: A Comparison of Logistic Regression and Naive Bayes," *Advances in Neural Information Processing Systems*, no. 14 (2001), https://ai.stanford.edu/~ang/papers/nips01-discriminativegenerative.pdf. Both discriminative and generative models are widely used in today's AI models and systems.

[9] Jared Kaplan et al., "Scaling Laws for Neural Language Models," arXiv, 2020, https://doi.org/10.48550/arXiv.2001.08361; Jordan Hoffmann et al., "Training Compute-Optimal Large Language Models," arXiv, 2022, https://doi.org/10.48550/arXiv.2203.15556.

[10] The name is derived from the term *agency*, the ability for a system to act independently. Craig S. Smith, "China's Autonomous Agent, Manus, Changes Everything," *Forbes*, March 8, 2025, https://www.forbes.com/sites/craigsmith/2025/03/08/chinas-autonomous-agent-manus-changes-everything/.

[11] There are several different approaches to pursuing agentic AI. An LLM or GenAI model may interact with other systems and applications, which are sometimes called agents. This may be done through an orchestration framework in which an LLM or GenAI model can communicate through application programming interface calls to other systems such as databases, knowledgebases, planning systems, simulation systems, the internet, and so on. Another approach is for the LLM or GenAI prompt to be broken up into a sequence of prompts and subprompts that can be processed using different algorithms, such as chain of thought. Jason Wei et al., "Chain-of-Thought Prompting Elicits Reasoning in Large Language Models," *Advances in Neural Information Processing Systems*, no. 35 (2022), https://doi.org/10.48550/arXiv.2201.11903.

[12] Ben Shneiderman, "Human-Centered Artificial Intelligence: Reliable, Safe and Trustworthy," arXiv.org, February 23, 2020, https://doi.org/10.48550/arXiv.2002.04087.

[13] Ruth A. David and Paul Nielsen, *Defense Science Board Summer Study on Autonomy* (Washington DC: Defense Science Board, 2016), https://apps.dtic.mil/sti/citations/AD1017790.

[14] Ian Goodfellow et al., "Generative Adversarial Networks," *Communications of the ACM* 63, no. 11 (2020): 139–44, https://doi.org/10.48550/arXiv.1406.2661.

[15] Models produce *Scores*, systems use scores to take *Actions*, and *Measures* are used to assess the effectiveness of the actions. This is sometimes called the SAM Framework. Robert L. Grossman, *Developing an AI Strategy: A Primer* (Open Data Press, 2020).

[16] Marson and Michaels, "Killer Robots Are About to Fill Ukrainian Skies."

[17] To reduce the computational burden and speed up the computation, not all subsequent frames are scored in this way, but just enough frames to be able to track the object during the flight of the drone.

[18] Stanislav Fort, "AI Cybersecurity After Mythos: The Jagged Frontier," *Aisle* (blog), April 7, 2026, https://aisle.com/blog/ai-cybersecurity-after-mythos-the-jagged-frontier.

[19] Kaplan et al., "Scaling Laws for Neural Language Models"; Hoffmann et al., "Training Compute-optimal Large Language Models"; Anirudh Subramanyam et al., "Scaling Laws Revisited: Modeling the Role of Data Quality in Language Model Pretraining" (Fourteenth International Conference on Learning Representations [ICLR-26], April 23–27, 2026, Rio de Janeiro, Brazil), https://openreview.net/forum?id=x54wwB6QvL.

[20] Subramanyam et al., "Scaling Laws Revisited."

[21] For some common reasons, see Narcisco Cerpa and June M. Verner, "Why Did Your Project Fail?," *Communications of the ACM* 52, no. 12 (2009): 130–34, https://doi.org/10.1145/1610252.1610286; Robert N. Charette, "Why Software Fails," *IEEE Spectrum* 42, no. 9 (2005): 42–49, https://doi.org/10.1109/MSPEC.2005.1502528.

[22] Robert L. Grossman, "A Framework for Evaluating the Analytic Maturity of an Organization," *International Journal of Information Management* 38, no. 1 (2018): 45–51, https://doi.org/10.1016/j.ijinfomgt.2017.08.005.

[23] In figure 3, although the analytic governance is identified as step 8 in the flow, the earlier it is set up and effective, the more likely the other steps will succeed.

[24] Sanjay Ghemawat et al., "The Google File System," *Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles* (Association for Computing Machinery, 2003), 29–43, https://doi.org/10.1145/945445.945450.

[25] Jeffrey Dean and Sanjay Ghemawat, "MapReduce: Simplified Data Processing on Large Clusters," *Communications of the ACM* 51, no. 1 (2008): 107–13, https://doi.org/10.1145/1327452.1327492.

[26] Sergey Brin and Lawrence Page, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," *Computer Networks and ISDN Systems* 30, nos. 1–7 (1998): 107–17, https://doi.org/10.1016/S0169-7552(98)00110-X.

[27] Konstantin Shvachko et al., "The Hadoop

Distributed File System," in *Proceedings of the 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies* (New York: IEEE, May 2010), 1–10, https://doi.org/10.1109/MSST.2010.5496972.

[28] Michael Lewis, *Flash Boys: A Wall Street Revolt* (New York: W.W. Norton & Company, 2014).

[29] "National Security Agency/Central Security Service, National Cryptologic Museum Debuts Service and Sacrifice, Real Time Regional Gateway Exhibits," National Security Agency/Central Security Service, July 12, 2017, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/1670296/national-cryptologic-museum-debuts-service-sacrifice-real-time-regional-gateway/.

[30] "How Our Business Works," Google, accessed June 23, 2026, https://about.google/company-info/how-our-business-works.

[31] Katrina Manson, "AI Warfare Is Already Here," Bloomberg, February 28, 2024, https://www.bloomberg.com/features/2024-ai-warfare-project-maven/.

[32] "AI Rapid Capabilities Cell," Chief Digital and Artificial Intelligence Office, U.S. Department of War, https://www.ai.mil/Initiatives/AI-Rapid-Capabilities-Cell/LINK.

[33] Mariella Moon, "The Pentagon Used Project Maven-Developed AI to Identify Air Strike Targets," *engadget*, February 27, 2024, https://www.engadget.com/the-pentagon-used-project-maven-developed-ai-to-identify-air-strike-targets-103940709.html.

[34] "Datalink-Enabled AI for Fires Optimization," U.S. Army Small Business Innovation Research and Small Business Technology Transfer Program, October 12, 2021, https://armysbir.army.mil/topics/datalink-enabled-ai-for-fires-optimization/; "How Artificial Intelligence Is Revolutionizing Aegis Combat System for Modern Naval Defense," *Global Defense News*, January 28, 2025, https://armyrecognition.com/news/navy-news/2025/how-artificial-intelligence-is-revolutionizing-aegis-combat-system-for-modern-naval-defense. Modern long-range air- and missile-defense systems, including the latest variants of the U.S.-made Aegis combat system, are using rudimentary machine-learning algorithms to defend against incoming ballistic- and cruise-missile threats.

[35] Emelia S. Probasco et al., *AI for Military Decisionmaking: Harnessing the Advantages and Avoiding the Risks* (Washington, DC: Georgetown University, Center for Security and Emerging Technology, 2025), https://cset.georgetown.edu/publication/ai-for-military-decision-making/. The authors found a surge in military adoption of AI to assist in decisionmaking.

[36] "Artificial Intelligence and Machine Learning Aim to Boost Tempo of Military Operations," *Military and Aerospace Electronics*, August 19, 2024, https://www.militaryaerospace.com/computers/article/55126930/artificial-intelligence-ai-machine-learning-military-operations. Air Force researchers are trying to apply AI to command and control and to consider enemy AI use in mission planning by pursuing a switch from monolithic command and control node to distributed command and control.

[37] Sharlene Tilley, "Smart Logistics: Navigating the AI Frontier in Sustainment Operations," U.S. Army, October 17, 2024, https://www.army.mil/article/280377/smart_logistics_navigating_the_ai_frontier_in_sustainment_operations. The Russia-Ukraine War proves that the U.S. Army can no longer depend on uncontested sustainment. Army sustainment capabilities lack the tactical mobility and tactical distribution of fuel and Army pre-positioned stocks in a contested environment. AI gives units down to the battalion level the ability to leverage the capabilities needed to improve supply chain management, resource distribution, mobility, and planning and preparation.

[38] Bonnie Johnson et al., "Mapping Artificial Intelligence to the Naval Tactical Kill Chain," *Naval Engineers Journal*, no. 135-1 (March 2023): 155–67, https://nps.edu/documents/10180/142489929/NEJ+Hybrid+Force+Issue_Mapping+AI+to+The+Naval+Kill+Chain.pdf.

[39] Secretary of War, "Harness Artificial Intelligence Now with GenAI," memorandum, December 9, 2025, https://www.documentcloud.org/documents/26367576-memo-on-integrating-genai-mil/.

[40] Ben Cottier et al., "The Rising Costs of Training Frontier AI Models," *arXiv*, accessed June 23, 2026, https://arxiv.org/abs/2405.21015.

[41] Defense Science Board Task Force on Balancing Security, Reliability, and Technological Advantage in Generative Artificial Intelligence, "Final Briefing," AD1321622, February 2025.

[42] Leopold Aschenbrenner, "Situational Awareness: The Decade Ahead," situationalawareness.ai, June 2024, https://situational-awareness.ai/; Michael C. Horowitz and Lauren Kahn, "The Cost of the AGI Delusion," *Foreign Affairs*, September 26, 2025, https://www.foreignaffairs.com/united-states/cost-delusion-artificial-general-intelligence. Horowitz and Kahn make this same case, but they offer no alternative conceptual framework, like analytic superiority, to prevail in analytic competition.

[43] Sayash Kapoor and Arvind Narayanan, "AGI Is Not a Milestone," normaltech.ai, May 1, 2025, https://www.aisnakeoil.com/p/agi-is-not-a-milestone.

[44] Erik Brynjolfsson et al., *What Can Machines Learn and What Does It Mean for Occupations and the Economy* (Pittsburgh, PA: American Economic Association, 2014), 43–47, https://doi.org/10.1257/pandp.20181019.

[45] Grossman and Goldman, "The Importance of Analytic Superiority in a World of Big Data and AI," 36–37.

[46] DOD Directive 3000.09, *Autonomy in Weapon Systems* (Washington, DC: Department of Defense, 2023), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

[47] National Security Presidential Memorandum/NSPM-11 (Washington, DC, 2026), https://www.whitehouse.gov/presidential-actions/2026/06/national-security-presidential-memorandum-nspm-11/.

[48] Emily O. Goldman and Richard Andres, "Systemic Effects of Military Innovation and Diffusion," *Security Studies* 8, no. 4 (Summer 1999): 79–125, https://doi.org/10.1080/09636419908429387.

[49] David Kirichenko, "The Rush for AI-Enabled Drones on Ukrainian Battlefields," *Lawfare*, December 5, 2024, https://www.lawfaremedia.org/article/the-rush-for-ai-enabled-drones-on-ukrainian-battlefields.

[50] Siobhan O'Grady et al., "Ukraine Scrambles to Overcome Russia's Edge in Fiber-Optic Drones," *Washington Post*, May 23, 2025, https://www.washingtonpost.com/world/2025/05/23/ukraine-russia-drones-fiberoptic-jamming/.

[51] Elizabeth Dwoskin, "Israel Built an 'AI Factory' for War. It Unleashed It in Gaza," *Washington Post*, December 29, 2024, https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/.

[52] Secretary of War, "Artificial Intelligence Strategy for the Department of War," memorandum, January 9, 2026, https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/artificial-intelligence-strategy-for-the-department-of-war.pdf.