Ai *is engineering* NOT MAGIC

By understanding the criteria for using artificial intelligence (Ai) technology, national defense and security leaders can determine whether Ai is the right solution to their problems before making a large investment.

Todd Borkey
Chief Technology Officer
todd.borkey@hii-tsd.com

Brendan McElrone
VP Technology Research Dev
brendan.mcelrone@hii-tsd.com

Huntington Ingalls Industries

ENGINEERING, NOT MAGIC

Thanks to massive marketing campaigns from big tech companies, nearly everyone in the U.S. federal government has heard that artificial intelligence (Ai) is The Future. They claim it's going to beat humans at every game, make inspiring art, eliminate boring work, cure cancer, and save lives in war.

The underlying promise is that Ai will do all these things almost magically. Just use our system, the ads say— no assembly required.

Bold claims, to be sure. And they aren't purely hype. Ai really is performing at superhuman levels against a wide array of challenges, and new forms of Ai are being invented so fast that the field barely has time to finish reading about the previous forms before learning about or inventing a new one. As a result, practitioners are constantly asked what new problems they can solve with Ai.

The missing piece in most Ai discussions, however, is the converse: When ***won't*** *Ai work?*

UNDERSTANDING THE POWER

Part of what makes modern Ai so powerful is its ability to find patterns and learn strategies that humans can't find or understand.

When learning how to play games, for example, humans develop both conscious strategies — concepts that we can express verbally — and subconscious feelings. For an Ai, all of its strategies are like our subconscious feelings: it learns them entirely from experience, without any explicit understanding as to why they work. In fact, deep learning is so powerful precisely because it is not restricted to using patterns and strategies simple enough for a human being to understand.

Because it can't concisely convey its reasoning, Ai can seem like magic— power without explanation. While it can be tempting for the field to sustain that perception — "Data Wizard" would make for an interesting business card — like everything else on a computer, Ai is ultimately a feat of science and engineering.

> Because it can't concisely convey its reasoning, **Ai can seem like magic— power without explanation.**

As a result, even though we might not easily understand why Ai makes the choices it makes, good Ai practitioners can still know when it's working and how it learns. And really good Ai practitioners can also diagnose what's wrong when an Ai is not working and help to identify when Ai might not be the most effective approach at all.

DETERMINING IF Ai IS THE ANSWER

Amid all of the hype, artificial intelligence is now a critical element of the U.S. national defense and security strategy, and with good reason. But, before leaders commit to Ai, they should first determine whether addressing their problem with an Ai solution is likely to work.

HOW ENGINEERING IGNITED THE AI REVOLUTION

The commonly accepted starting point for the modern Ai era is unusually precise, relative to other technological eras. It began with the publication of the "AlexNet" paper in 2012 by Alex Krizhevsky and his co-authors.

The paper was a response to the ImageNet challenge, an annual competition to see which algorithm could correctly classify small images by their main content. In the previous year, the top-performing algorithm was wrong — it didn't have the right answer in its top five guesses — on about 26% of its classifications, and the previous year's best was wrong on 28%. AlexNet cut that error rate to about 15%, which was only three-fifths as many errors as the previous year's best and an improvement about five times larger than the previous annual improvement.

How did AlexNet leapfrog the competition so dramatically? After all, the core science behind the technique was already well understood. Early neural networks had been around since the 1950s, and scientists had experimented with convolutional neural networks — the specific flavor on which AlexNet was built — since the 1980s.

Here are three key indicators that a problem is Ai ready:

1. **Existing solutions aren't good enough.**
It may seem obvious — why would something still be a problem if a solution already exists? — but the increased attention to Ai has caused many people to reconsider the way they have long performed a task. In many cases, this is a good thing … but not always.

The first step in assessing a problem's readiness for Ai is to survey existing technical approaches. For example, in many fields, high-quality data science methods offer additional benefits (such as explainability) and avoid costs (such as massive dataset collection and management) associated with the power of modern Ai.

Careful evaluation of those trade-offs is a key first step to determining both Ai readiness and to informing the design of an Ai solution, if one is appropriate. In some cases, leaders will find that Ai is not the best answer, and that's okay. The ability to distinguish the best approach is critical to making — and defending — informed technology investments.

2. **The end goal is well understood.**
Modern Ai depends entirely on a calculation that captures how well it solved the problem— the "loss" or "reward" function, depending on the type of Ai. The Ai uses the result of that calculation to help it do better next time. If the goal is not translated correctly into that equation, then the Ai's learning won't bring it any closer to the goal.

Getting the form of that function right requires subject matter expertise and technical chops. Getting it wrong means that the Ai will solve a different problem altogether, which may not do anything to advance the mission.

If the end goal can be clearly articulated, and trade-offs between the priorities within that goal can be clearly defined, then Ai may be the right way to achieve it.

3. **Good data can be found or made.**
Even the most magical descriptions of Ai recognize that it requires a lot of data; the number of data points is one of the easiest Ai requirements to quantify. Less straightforward are factors like coverage (how well the data capture all the nuances of the problem domain), cleanness (how much preparation the data need before use), and consistency (whether the statistical properties of the data are close enough to the statistical properties of the use case to be effective).

Researchers have developed a plethora of methods to address cases where these criteria are not met, but they rely on practitioners to make a careful assessment of the data before charging ahead with a solution.

For a problem to be Ai ready, the available data — whether real or simulated — should mirror the properties of the problem domain closely, so that an Ai trained on them will have a viable answer on hand across a broad range of mission needs.

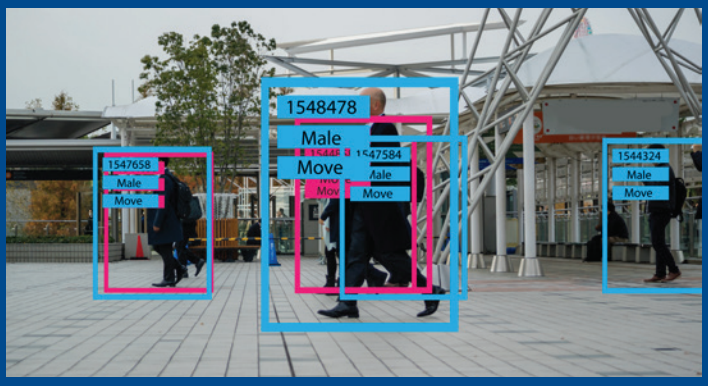
If a problem survives all three tests — a more powerful solution is needed for a well-defined goal, and high-quality data are available — then it is Ai ready. Without those foundations, the next step of actually designing and implementing an effective solution is likely out of reach.

This Ai-readiness recipe saves time and money by preempting the challenges that many leaders, having heard of the potential power of Ai, find themselves facing. Just as importantly, if an organization goes through the Ai-readiness evaluation process, it can discover which elements it lacks and focus resources on solving those sub-problems first, before turning to high-powered Ai solutions for the larger issues.

With the right insight, preparation, and expertise, U.S. defense and national security leaders can make smart investments into Ai to maintain the nation's technological edge through improved human-machine teaming across the full spectrum of military action.

AlexNet's success was, ultimately, a feat of clever engineering. The team wrote specialized code for commercial, off-the-shelf NVIDIA graphics cards to achieve the computational speed necessary to train a deep neural network— the technology behind most Ai advances since AlexNet, called "deep" because they are formed of multiple layers (linked calculations). Their software cut training times on 1.2 million images from weeks or months to days, and further engineering tweaks nudged accuracy up a few percentage points each.

As with the ImageNet challenge, domain-specific engineering is the necessary ingredient to move from the raw science to full, integrated Ai solutions to today's national defense and security challenges.



8350 Broad Street, Ste 1400
McLean, Virginia 22102
703.918.4480
tsd.huntingtoningalls.com

Learn more at tsd.huntingtoningalls.com/ai