Primer

eBook

The Decisive Decade: At the tipping point of AI in national security



The world is at a critical crossroads when it comes to AI. In the 2020s we've seen a surge of advancements, from the expanded productivity and creativity of ChatGPT to the increased trustworthiness of RAG-V.1 As a result, intelligence analysts and leaders are calling the 2020s "The Decisive Decade" for AI in both government and industry.

In 2025, we find ourselves at the midpoint of a decade where geopolitical instability and advancements in AI are converging to create multiple opportunities for national defense and security. But we are also at a tipping point as to how we are going to use these rapidly advancing tools practically, strategically and ethically moving forward.

The decisions intelligence and defense leaders make over the course of the next year or two will impact our nation's AI dominance, decision superiority, and operational readiness for the remainder of the decade.

Putting artificial intelligence in context at the midpoint of the Decisive Decade

The world in 2025 looks drastically different than it did just five years ago in the COVID era. In support of these changes, advancements in AI are increasing at breakneck speeds. Whether you know it or not, you encounter AI every time you use Google or shop at Amazon. It is becoming ingrained in our society in many helpful ways.

In regard to national security and intelligence, however, developments are more intense and harder to quantify. Driven by geopolitical trends, AI is becoming a battleground in many senses of the word, from the way we fight wars to who is making key advancements.

In fact, AI is considered akin to the nuclear bomb in warfare—countries who have it will quickly defeat countries who don't. It is at least as impactful as demographic shifts and energy constraints are on military readiness. In fact, many characterize AI's future role as being an actor in conflicts and not just a factor.2

Here are some of the major threats and opportunities shaping the way we approach AI in 2025:

- **China is a major concern.** China is our greatest adversary in the AI race.3 We thought cutting them off from the advanced NVIDIA semiconductors needed for AI would at least hobble them and widen the US's lead in AI but, instead, they are closing the gap.4 They released Deep Seek, an AI chatbot that, according to its creators, uses less computing power and was developed at a fraction of the usual cost, upending the global industry.5 If that weren't enough, China also found a way to hack our government systems.6
- **The Axis of Chaos is growing.** New and stronger alliances are forming between China, Russia, Iran and North Korea.7 These are countries with both brilliant and devious approaches to AI and warfare. As they move forward with fewer restrictions on development and operationalization than the US, we need to find ways to counteract or zero out their advancements.
- **China threatens Taiwan.** Taiwan manufactures 90% of the world's advanced semiconductors, including those used by NVIDIA.8 Tensions between China and Taiwan are strained as Taiwan continues to hold on to its independence. Decisions made by the U.S. and other nations regarding Taiwan—whether positive or negative—can create grave economic, political and national security consequences for Taiwan, the U.S. and our allies.9
- **Our national stance brings opportunity.** The 2024 National Defense Authorization Act prioritizes AI research, industry collaboration and the identification of risks and mitigation strategies for the misuse of AI.10 In addition, Secretary Pete Hegseth released a memo directing the DoD to establish a rapid acquisition path for AI solutions supporting the warfighter.11 AI is a topic on everyone's lips in 2025 and the current administration is a strong supporter of further development and assimilation.
- **Ukraine is pioneering AI in warfare.** AI is already being used to great effect in the war between Russia and Ukraine.12 While both countries are using it, Ukraine has an intelligence edge thanks to AI—a factor that has benefited them in a war against a much larger adversary. Ukraine is using the technology to inform decision-making, gain geospatial intelligence, track Russian movements, allocate resources, drive operational efficiencies, impact cybersecurity and assess intelligence faster.

All of this is creating a perfect storm for AI in 2025. The decisions made this year could be the tipping point that determines global leadership and the U.S.'s strength in both national security and intelligence.

We can no longer "consider dipping our toes" into AI adoption. We need to incorporate into our intelligence workflows now. Technological developments are quickening. There is a learning curve with each new iteration. Countries like Russia and China don't have the same red tape we have when it comes to developing and operationalizing new technology.

While the US still leads in the development of AI overall and can learn a lot from recent advances by the Chinese and others, competitors are shortening the gap and developing new uses we are not prepared for. The decisions we make in 2025 will either cement or diminish U.S. leadership in AI.

How AI gives users an edge in OSINT and ISR

Today's world is data rich and knowledge poor. Social media posts, news organizations, websites, public records and online forums produce millions of documents each day—too great a volume for analysts to properly review using traditional methods. And that dataset grows exponentially each day.

The intelligence community is not in the deciding business. It's in the business of informing decisions. So, it's the IC's job to gather and analyze information to inform decisions and reduce uncertainty. And they need to do it in a timely manner. AI is the conduit through which the IC can search through all that raw data, unearth the relevant parts and transform it into actionable intelligence in the blink of an eye.

Simply stated, traditional intelligence workflows are no longer sufficient to keep with modern threats. The geopolitical landscape, the state of AI and the volume of open-source intelligence (OSINT) is progressing too rapidly. Analysts are already using AI as a tool to aggregate and make sense of all that data, and the tool is becoming more accessible as advancements make search easier and results more dependable.

OSINT is just one source of data available to the DoD and IC. There, AI is used to sort through classified and proprietary information, as well. The ability to merge human intelligence (HUMINT), signals intelligence (SIGINT), geospatial intelligence (GEOINT) and measurement and signature intelligence (MASINT) with OSINT gives analysts a 360 view of a situation that leaders can use to inform their defense and information, surveillance and reconnaissance (ISR) missions.

AI can process all this information in the time it takes to conduct an online search, cutting hours and days out of the process, while searching deeper and more thoroughly than possible through traditional means. For those in national defense, this spells the difference between victory and defeat, preparation and surprise, life and death.

Hallucinations and the impact they have on AI adoption

So far, everything in the AI world sounds ideal. But it's not. One of AI's biggest challenges in 2025 remains the issue of "hallucinations", fabricated or misleading information that sounds plausible but isn't supported by the data. Leading large language models (LLMs) can produce impressive results, but even the best models still generate inaccurate responses up to 10% of the time. This can have operational consequences.

Retrieval-Augmented Generation (RAG) helps reduce this risk by grounding AI responses in retrieved source material. But even with RAG, hallucinations still occur, especially in high-stakes environments where accuracy matters most.

That's why Primer developed RAG-V: a verification layer that breaks down AI-generated sentences into individual claims, then checks those claims against the retrieved sources. If a claim can't be verified, RAG-V aims to flag it before it reaches the user. Primer's approach cuts hallucination rates in half compared to standard RAG systems, and more importantly, makes each insight traceable to its source. This gives analysts and decision-makers the ability to see why a claim was made, and verify it for themselves when needed.

Trust is the tipping point for AI in national security. By making hallucinations visible and fixable, RAG-V helps build that trust, not through a black-box, but through transparent reasoning that teams can rely on.

The role of AI in malign influence campaigns

Geopolitical events are becoming increasingly shaped by malign influence campaigns. Russia and China employ information operations against the U.S., exploiting their positions on the Israel-Hamas conflict, for example. The goal is usually to influence public opinion, undermine trust and shape national policies.

OSINT has become critical in tracking and analyzing these threats, as well as helping us distinguish which information can be synthesized into actionable intelligence. The study and analysis of propaganda is called narrative intelligence (NARINT). NARINT may include data collection from open sources, analysis of trends and key actors, counter-messaging, and the use of AI to automate the data collection, identify patterns and predict emerging narratives.

Malign actors often use generative AI to generate text, images, audio and video and publish it to the internet. As you may have observed in your travels, generative AI struggles with idioms and basic grammar, leaving telltale signs of malign influence in their wake. But this is improving as narrative warfare gains in popularity with its ability to influence elections, create division, sway public sentiment and shape policy.

Integrating AI tools into military and IC operations offers several advantages to combat this type of narrative warfare:14

- **Speed.** AI can analyze vast amounts of data in real time to identify trends, predict future threats and zero in on the geolocation the threats are originating from.
- **Scalability.** AI enables smaller teams to support broader missions and cover more ground. This is essential for countering widespread malign influence campaigns.
- **Risk management.** AI can assess the potential impact of different messaging strategies, helping leaders understand the risks, benefits and likely responses to various courses of action.
- **Content generation.** Just as it does in the Russian troll farms, AI can generate high quality content at scale for US interests, countering adversarial narratives, reframing the messaging and providing a rapid response.

Why 2025 is the tipping point for AI adoption in the IC and DoD

AI is one of the battlefields—if not THE battlefield—of future wars. And we are reaching a tipping point in its use and development. Our adversaries are already successfully using it against us. So, 2025 is a critical year when it comes to the adoption and learning of this valuable tool.

In February 2025, Primer hosted a fireside chat with distinguished national security experts. While already using AI in the field, they put forth a wish list of things they'd like to see in the near future in regard to AI:

- **Faster speed of deployment.** There's a lot of red tape between the acquisition of a technology and actually getting it into the warfighter's hands. The sooner you equip yourself with the most powerful capabilities, the better equipped you are to preserve peace and deter threat. This issue recently got a boost with the memo Secretary Hegseth released to accelerate acquisition, but we have farther to go in our quest to speed operationalization.
- **Trust.** This may be the biggest barrier—and the one with the best solution. Simply put, operators and analysts need to trust their results. With RAG-V, we've already addressed this critical issue. But there's also the psychological issue that must be overcome regarding the trust in AI overall. Education and use can assist here.
- **Power/Storage/Compute.** If you are sitting at a desk in the DoD, you have plenty of power, storage and compute power. But if you are in a bunker in enemy territory, that's not necessarily the case. So we need a way to make the technology more transportable and translatable to the front lines. This will happen with ongoing AI optimization.
- **Partnerships.** The culture of being a partner is critical with AI. It's not just about calling a vendor with a "what if" scenario and getting an answer. It's about involving vendors from day one so they have both the context of and the commitment to the mission. This cultural shift is already underway in government.

Completing that list is affordability and interoperability. All these issues are currently being addressed in the industry and will continue to be for years to come.

The role of AI in ensuring U.S. dominance cannot be understated. The best time to adopt and embrace these technologies was yesterday. The second-best time is now. The sooner these technologies are adopted, the sooner they can be learned and optimized.

Take a look at the world around you. Geopolitical tensions are on the rise and adversaries like China and Russia are already invested in AI for everything from malign influence to situational awareness, drone warfare, ISR and other logistical and tactical purposes. That's why 2025 is a pivotal year. We can't afford to cede ground in the race for information domination.

Stop waiting for the future of AI. It's already here.

The battlefield in 2025 looks vastly different than just a decade ago. AI innovations that advance ISR and practically zero out hallucination rates have increased both the potential of AI and trust in its results. Today's AI-enabled ISR innovations and defense technology advancements are already used in warfare to improve decision-making, targeting, and resource allocation, not to mention helping to identify threats, gather intelligence, and prepare for battle.

AI is not a future capability. It's here. It's now. It's necessary. And while there will always be improvements and refinements to be made, it's battle-ready today. Without trusted AI, decision-makers risk acting on incomplete information, missing critical threats, or falling behind in AI-driven warfare.

The 2020s have greatly shaped the future of AI so far. It is the decade that will define how AI is used, how ethical its uses are and how prepared we are to face threats from countries who are already actively using the technology in battle and psychological warfare.

That's why 2025 is a critical year to adopt and embrace AI. The technology is developing so fast that the learning curve increases exponentially with each passing year. The next five years will define the global AI balance of power—leaders who act now will set the course for the future. To stay ahead, defense leaders and intelligence agencies must rethink how they process intelligence, assess threats, and execute missions.

Primer's AI solutions provide trusted, mission-ready intelligence for national security, ISR operations, and decision superiority. In fact, we've pioneered the most trustworthy AI solution in the marketplace and are continually looking to innovate new approaches to address industry concerns. To learn more, visit us at Primer.ai.

References:

[1] Defense News, October 16, 2024, *"PrimerAI introduces 'near-zero hallucination' update to AI platform."*

[2] Rand, November 3, 2023, *"AI and Geopolitics: How Might AI Affect the Rise and Fall of Nations?"*

[3] Time, January 28, 2025, *"How China is Advancing in AI Despite US Chip Restrictions."*

[4] BBC, January 27, 2025, *"NVIDIA shares sink as Chinese AI app spooks markets."*

[5] The Australian, December 31, 2024, *"US Treasury says it was targeted by China state-sponsored cyberattack."*

[6] VOX, February 3, 2025, *"Are America's four main adversaries really in cahoots?"*

[7] Wired, October 5, 2024, *"Taiwan Makes the Majority of the World's Computer Chips. Now it's Running Out of Electricity."*

[8] APNews, March 18, 2025, *"China conducts air and sea drills near Taiwan in response to US and Taiwanese statements."*

[9] Congress.gov, December 22, 2023, *"HR 2670—National Defense Authorization Act for Fiscal Year 2024."*

[10] ExecutiveGOV, March 10, 2025, *"Hegseth Wants to Accelerate DoD Software Acquisition."*

[11] Center for a New American Security, July 20, 2023, *"Roles and Implications of AI in the Russian-Ukraine Conflict."*

[12] Primer Webinar, November 27, 2024, *"Introducing RAG-V: the future of trustworthy AI."*

[13] Modern War Institute at West Point, October 25, 2024, *"Persuade, Change, and Influence with AI: Leveraging Artificial Intelligence in the Information Environment."*

Learn more: www.primer.ai