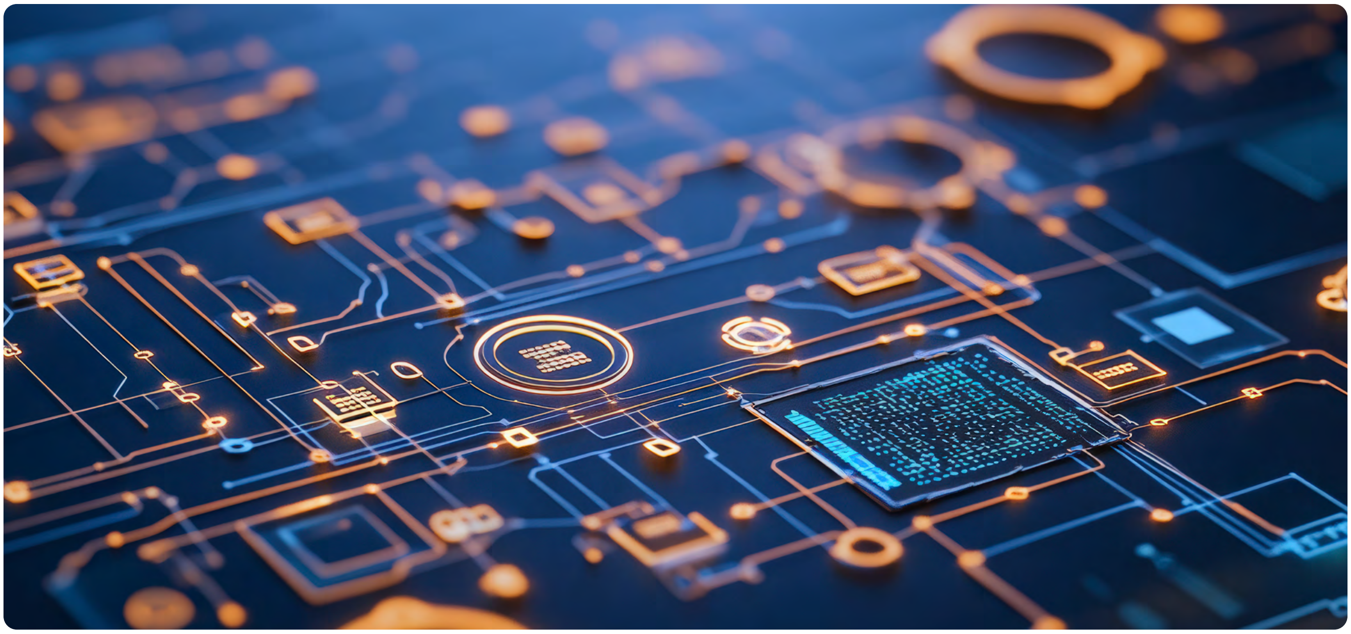
CLOUDERA ATARC

WHITEPAPER

Agencies say AI is boosting speed and scale — but not without growing pains

Federal leaders say AI is transforming national security operations, but success hinges on clean data, zero trust, responsible governance, and a culture of collaboration.



As artificial intelligence adoption accelerates across national security, agencies are asking the right questions: where it fits, where it falls short and what it takes to use it responsibly.

In a recent discussion hosted by ATARC and Cloudera, federal and industry leaders examined how AI and data are reshaping defense operations. They explored what's working, where gaps remain and how people, policy and infrastructure must evolve to meet mission demands. The group also discussed the growing need for interagency collaboration, the importance of clean, trusted data and how zero trust and governance frameworks are adapting for predictive analytics, agentic AI and beyond.

HERE ARE SIX KEY TAKEAWAYS:

AI is speeding up ops, but not without tradeoffs

AI is already delivering real-world results, but participants agreed: Speed and scale don't matter if data is fragmented or untrusted.

A senior researcher at a federally funded R&D center said her team combines CVE data with public exploit databases like Metasploit to prioritize vulnerabilities most likely to be exploited in the wild. AI helps merge disparate datasets across public and DOD sources — something previously too complex or time consuming.

A senior IT leader described "growing pains" from decades of siloed data across engineering, maintenance, real estate and contracting. AI and machine learning are now helping integrate those silos to support operational and strategic decisions.

"And now in order for us to be as effective as possible, we've got to bring that data together in some way, shape or form," he said.

But pulling data together can introduce new vulnerabilities. A cyber leader warned that Large Language Models expose insights but also increase the attack surface.

AI is also improving decision-making speed and breadth. At a defense education institution, instructors are using AI and data analytics to help students — rising military leaders — generate and evaluate multiple operational paths.

Another cyber operations leader shared a live example: His team uses AI across hybrid multi-cloud environments to locate precise 10-digit grid coordinates for kinetic operations and execute cyber missions like persona targeting and network disruption.

Zero trust only works if the basics are in place

As AI scales across hybrid environments, agencies are embracing zero trust — but participants emphasized: It only works with strong fundamentals. A senior IT leader said inconsistent or overloaded networks at the edge delay real-time AI-driven decision-making.

"Every endpoint must meet core security standards before gaining access to apps, data and the broader network," she said.

A cybersecurity leader supporting defense software efforts cited persistent data sprawl. His team uses data tagging and microsegmentation to isolate systems and flag risks with AI across IL2 to IL6 environments, aiming to stay secure without slowing operations. Another senior cyber operations leader raised a newer challenge: agentic AI.

"It's not just the people, but it's now that we've got AI that can create AI and that's going to proliferate, how do you handle the identity on that as it has access to your data, to your models and to your networks?" he asked.

AI makes threat detection faster, but trust still depends on people and process

AI-driven predictive analytics is helping agencies detect and respond to threats faster, but speakers stressed that speed isn't enough without safeguards. A senior academic in cyber operations emphasized the importance of distinguishing system access risks from data risks. Each requires tailored controls under a zero trust model.

"We also have to go with people, process, technology and policies, those things we have talked about f or many years and I think they still apply over here," he added.

A senior cyber operations leader described how AI integration with SIEM and SOAR systems helped his team align controls, cut response times from 16 minutes to 0.0033 seconds and boost capacity by 60%, saving $4.8 million without staff reductions.

But even with those gains, human oversight remains critical.

"Networks now are more prolific than ever," he said. "Everything is an endpoint with the cloud."

Another speaker noted predictive tools still rely on functioning physical infrastructure. Legacy IT plays a role, too.

"There is always going to be a mixture of both the old and the new and to make it work together," she said.

Collaboration won't work without culture, clarity and trust

Effective collaboration on AI and data hinges on shared understanding, trusted partnerships and a culture that supports both. A senior cybersecurity leader said it's time for agencies to evolve together. He compared this moment to prior transitions like virtualization and cloud.

"So what is the evolution of the cybersecurity community? And I think that has to happen together more so than it is separately," he said.

A cyber academic agreed. He pointed to data sanitization and revisiting established security models like Bell-LaPadula and Clark-Wilson to guide data-sharing protocols. He said AI can help speed decisions around what should and shouldn't be shared.

Another participant said interagency collaboration is key, especially with constraints around geography, staffing and funding. No agency can secure its systems alone. He's looking to AI to help identify others working on similar challenges and speed up shared progress.

Responsible AI starts with governance, boundaries and good judgment

As AI becomes embedded in national security operations, participants agreed: It's not just about policy; it's about culture, clarity and accountability. One participant noted governance is a must to ensure ethical AI use, especially in organizations where personnel switch between civilian and military roles. That dual identity can lead to missteps, like bringing commercial AI tools into secure DOD environments.

His team relies on governance frameworks, raises concerns through data boards and coordinates closely with oversight bodies.

"Governance is key for us," he said. "We continue to push along that guideline and it has done well for us in terms of our capabilities and being innovative."

A senior tech officer said the best place to start is with the basics — like automating base shuttle routes with computer vision — to build confidence and free up staff for more strategic roles.

"Ultimately, don't ignore the mundane, make use of it, harvest the information and use that to inform the more exotic as we go forward," he said.

Another participant said ethical AI starts with keeping humans in the loop. As adversaries push toward full automation, including cyberattacks and disinformation, U.S. agencies must model responsible use with clear ethical guardrails. That also means building AI and data literacy across the workforce. Users need to understand what systems are telling them and how to act on it.

Another participant put it bluntly: Bias is built into every model.

"The real challenge isn't whether AI is biased or may hallucinate; it's how we define and enforce what's ethical, legal and preferable in rapidly advancing technologies," he said.

AI readiness starts with training and fixing the data

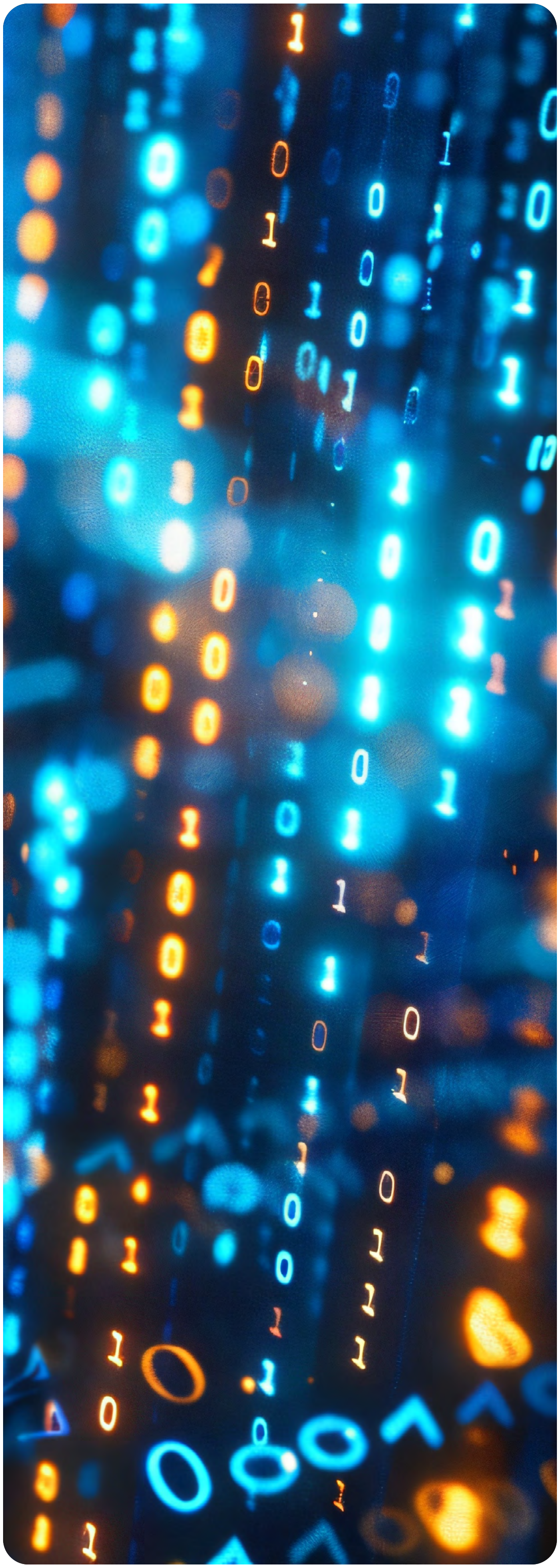
Getting the workforce ready for AI means more than tools. It requires hands-on experimentation and fixing data foundations. One participant described how her team built a secure AI sandbox so staff could safely experiment with controlled data.

"I think people are very afraid of crossing those boundaries because they're not really clear yet in terms of what is okay to ask ChatGPT given that it's an external system . . ." she said.

Another speaker advocated for mandatory AI and data literacy training, similar to annual cybersecurity or OPSEC requirements. AI, participants said, should no longer be considered someone else's job.

However, bad data is still a problem, another participant pointed out. He warned that agencies are moving fast with generative AI while skipping over basic data cleanup like unstructured formats, missing indexing and unclear ownership.

To fix it, his team is investing in workforcewide data education and offering graduate certificates for roles like chief data officers, many aligned with DOD 8140 requirements.



Click to learn how Cloudera is accelerating AI in the public sector.