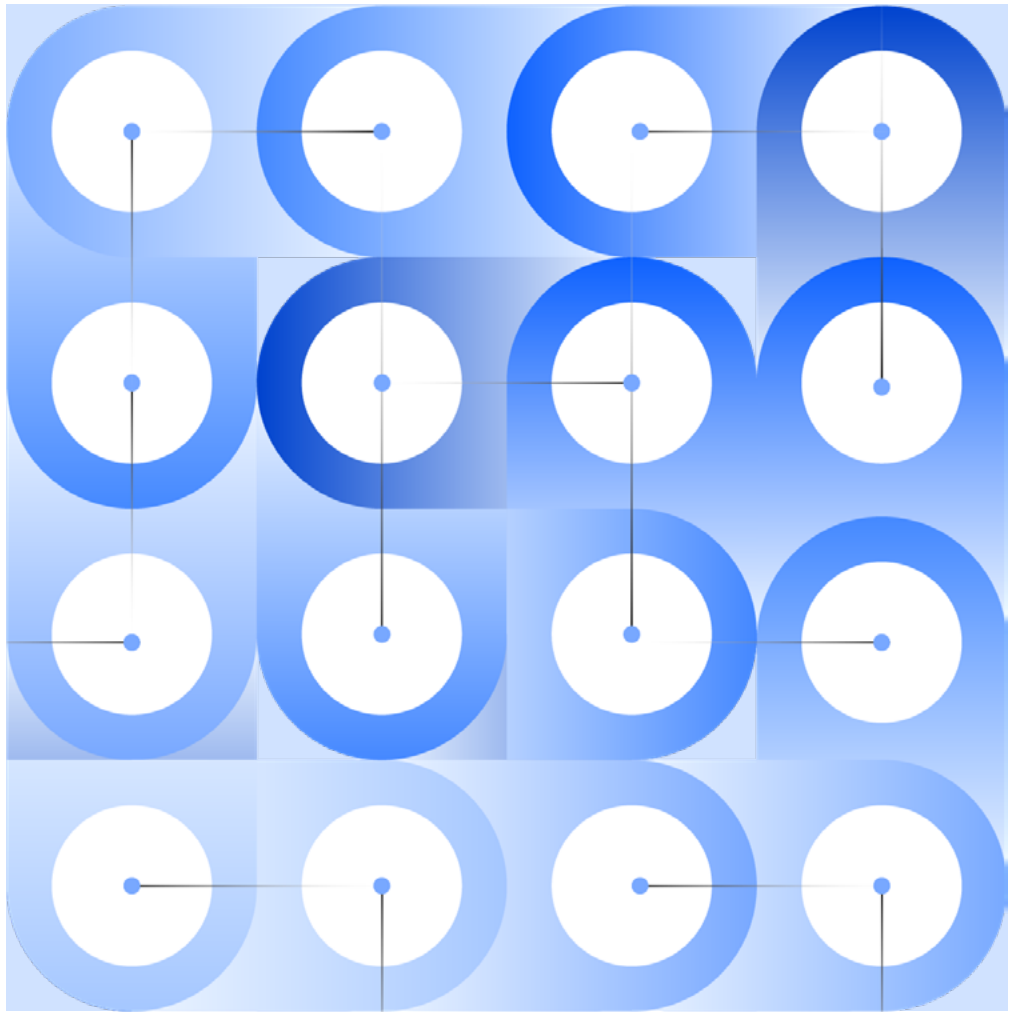
AI decision advantage for defense

Closing the gap between development and deployment



Foreword

Artificial intelligence (AI) has become a critical and strategic capability for defense organizations around the world, offering immense benefits such as improved efficiency, accuracy, and decision making. To understand the state of AI in defense and how this innovative technology is being leveraged by organizations globally, the IBM Institute for Business Value interviewed 600 technology executives from defense organizations representing 32 nations. Our research reveals a strong recognition of AI's strategic significance; however, certain obstacles hinder widespread integration including trustworthiness, data governance, and talent gaps.

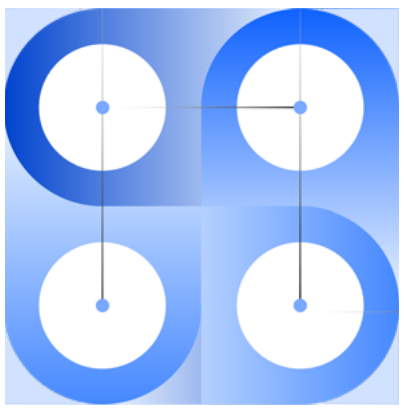
Despite the challenges, defense leaders remain optimistic about AI's potential to augment tactical superiority, enhance operational efficacy, and increase preparedness. Substantial resources are being dedicated to AI, as defense organizations collaborate extensively with private industry partners to develop and accelerate advanced AI tools and capabilities.

AI has the potential to revolutionize military operations, and influential leaders express confidence in its value. By effectively addressing challenges and forming partnerships and alliances with ecosystem partners in both the public and private sectors, defense organizations can fully leverage AI to improve mission outcomes and gain decision advantage. We hope this report provides leaders across the global defense community with useful insights that can assist their organizations in realizing the promise and potential of AI.

Cristina Caballe Fuguet
Vice President, Global Public Sector
IBM Consulting

Casey Werth
General Manager, Global Public Sector
IBM Technology

Key takeaways



- Defense organizations around the world are **prioritizing AI**, increasing investments in this game-changing technology, and seeing its potential for building strategic advantage.
- Three years ago, **defense leaders expected to be further ahead in AI**, but skill shortages, data governance issues, and ethical challenges continue to be speed bumps.
- Despite the challenges, the promise of AI is so compelling that **leaders are doubling down on this technology** during the next three years—especially on generative AI capabilities.
- Defense organizations are **building up internal AI capabilities** to reduce reliance on the private sector but work with contractors to a significant extent during initial consideration and evaluation stages.

Introduction

Since the invention of gunpowder in the first millennium to the advent of aviation, tanks, radar, and submarines in the 20th century, defense organizations have historically sought a strategic edge through advancements in technology. Today, in response to pacing geopolitical challenges, the demand for greater capabilities, and the need to extend human resources, defense leaders are turning to artificial intelligence for decision advantage.

From a geopolitical perspective in 2024, the world is experiencing the highest number of armed conflicts between nation states since World War II.[1] But as major defense establishments build up capabilities in an era of increased conflict potential, human resources are stretched. For example, the number of active-duty service members is declining in the US armed forces, reaching its lowest levels since 1940.[2] Since 2000, the UK has also experienced a 30% reduction in its military ranks.[3]

With fewer people tasked to do more in an increasingly complex operational environment, national defense strategists see advancements in data, analytics, and AI as force multipliers and force enablers. AI represents an unprecedented opportunity to harness the decision-making potential of defense leaders at every level. For the US, the North Atlantic Treaty Organization (NATO), and allied nations, AI is also key to maintaining traditional advantages in defense and national security technology.[4]

National defense strategists see advancements in data, analytics, and AI as force multipliers and force enablers.

Whether applied downrange to kinetic operations, to sustainment, support, and security, or to a host of other applications, AI—and especially generative AI—is developing rapidly. Concurrent with AI development, defense organizations are racing to understand, test, adopt, and exploit AI capabilities and determine where the most strategic impacts will come from.

However, the AI surge in defense has been tempered by technical and ethical considerations. These include issues related to trust, bias control, transparency, accountability, model integrity, and management of autonomous and automated systems. In response to the increasing tempo of cyberattacks, information operations, and hybrid conflicts, defense leaders must also build technical and organizational bulwarks to help ensure that sensitive and classified information used in AI is well-protected against hacking and misuse.

Given the rapid rate of development and the high stakes for deploying AI at scale, where do defense leaders see themselves in the race for AI decision advantage? How will they adopt AI, and what practical, technical, and cultural impediments stand in the way? And how will today's leading defense organizations make AI capabilities mission-ready in the areas that matter most?

To address these vital questions, the IBM Institute for Business Value (IBM IBV) surveyed 600 technology leaders from defense organizations in 32 countries in 2023. This follows up a similar survey of defense leaders in 2020 and offers insights into trends of how they are thinking and intending to act as they drive AI adoption in national defense organizations, defense contractors, and related defense industries.

Defense organizations are prioritizing and boosting investments in AI

In our survey, most defense leaders report that AI plays an important role in their organization's strategy today, with 48% indicating that AI is at least somewhat important, 37% ranking AI as very important, and 11% considering AI to be extremely important.

35%

of leaders indicate AI will be extremely important in the next three years.

The importance of AI to their organization's missions in the future continues to grow over the next three years, with 52% of leaders considering AI to be very important and 35% characterizing AI as extremely important.

Defense leaders are backing up their confidence in AI by increasing investments in this technology since 2020. In fact, 13% said their organizations had significantly increased investment in generative AI over the last three years, with another 40% pointing to significant investment increases in other AI technologies. In the US, this corresponds with the significant bump in funding requested by the Department of Defense (DoD), which received a 26.4% increase in AI funding for FY 2023 over FY 2022.[5]

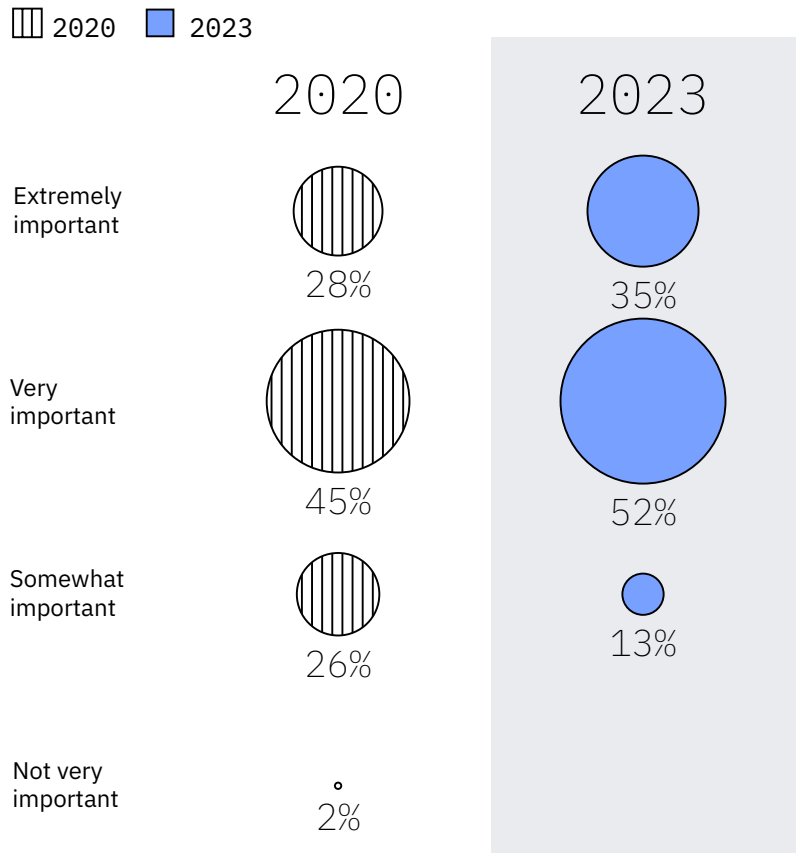
IT budgets continue to grow in the defense sector, and investments focused on AI are capturing an increasing share of this spend. During the next three years, leaders expect to increase annual IT budgets the most on cloud computing and AI, with the share of the IT budget dedicated to AI projected to increase over the next three years.

As AI investment levels grow, so do positive expectations that defense organizations can realize value from this technology. A solid majority of surveyed leaders say that AI, including generative AI, will improve their operational capability and readiness, with 44% saying this outcome is likely and 18% going further to say this outcome is extremely likely.

Conversely, less than a third of these leaders view AI as a future threat. When asked if they see AI—including generative AI—posing a threat to defense organizations and national security over the next five years, only 23% say this is likely, and only 6% see this as extremely likely.

FIGURE 1

How important will AI be to your organization's strategy in three years?



Case study

Launching a new wave of naval efficiency with AI-piloted vessels

Mayflower Autonomous Ship
ProMare

In June 2022, the Mayflower Autonomous Ship (MAS) became the first AI-controlled ship to cross the Atlantic Ocean, completing a 3,000-mile voyage from the UK to the US in 40 days.[6] MAS is piloted by a first-of-its-kind "AI Captain," which navigates the ship, collects data, avoids collisions, and maintains a safe operating environment—all without human intervention.

MAS is a full-sized ship designed for long-range oceanic research. Vessels fitted with this technology could also be deployed for military missions such as intelligence gathering, surveillance, mine detection, and other hazardous operations without putting sailors at risk. By eliminating the need for onboard crew accommodations, facilities, and support systems, autonomous vessels can significantly reduce operational costs while extending deployment schedules.

In addition to cost and safety advantages, autonomous vessels:

- Improve detection of potential threats with enhanced situational awareness
- Extend fleet reach and capabilities by augmenting crewed vessels
- Boost intelligence, surveillance, and reconnaissance capacity when operating in contested waters

Generative AI in defense creates new opportunities and interest is growing

For over 60 years, the US DoD has been a major investor in AI technology.[7] However, until recently, only engineers, data scientists, developers, and other experts had access to AI systems. But now, the arrival of generative AI enables anyone to use large language models and chat transformers to review huge troves of information in seconds and crystallize data into decision-making insights.

Our research indicates that generative AI has made an immediate and lasting impact on defense organizations. In fact, 25% of respondents say that their organization will use generative AI to a significant extent, and 38% anticipate they will use this technology to a large extent during the next two years. The top three areas considered for deploying generative AI include information technology at 60%, customer service, personnel support, and family services at 58%, and information security at 54%.

To take advantage of advances in generative AI technology, NATO is updating the AI strategy it adopted in 2021. The defense alliance is standardizing processes to use generative AI effectively and safely, especially in ways that can boost cybersecurity and help alliance members identify and fix network vulnerabilities.[8]

Through initiatives such as the Chief Digital and Artificial Intelligence Office (CDAO) and Task Force Lima, the Pentagon is marshalling resources to rapidly pilot and deploy responsible generative AI. CDAO is also asking for assistance and expertise from the private technology sector to build secure AI models that can meet US DoD requirements.[9]

The survey data indicates that less than half of defense leaders are aligned and in agreement on the top issues related to building foundational AI models. And less than half say they have the capability to train models on their own. Further, more than half of leaders indicate that their organizations relied heavily on the private sector for generative AI capabilities in 2023. But as in-house capabilities increase, most leaders expect to reduce that reliance during the next three years.

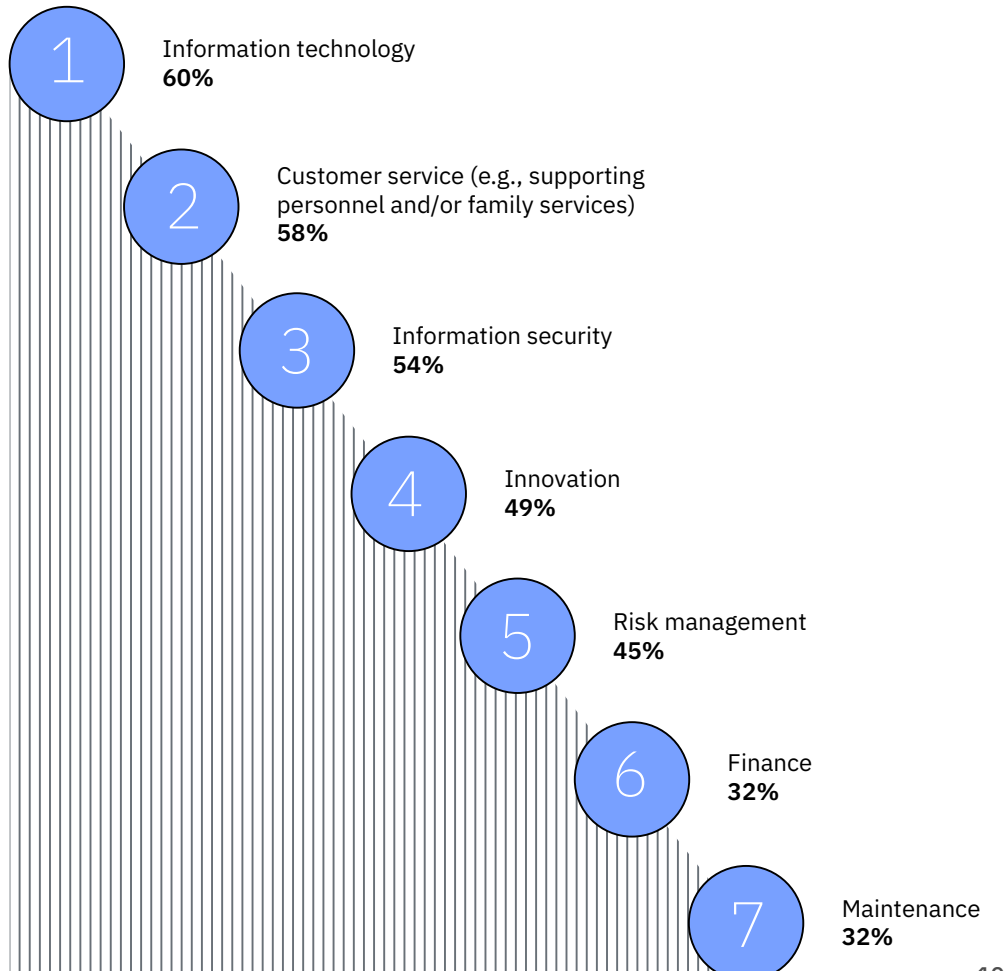
Like the leaders of other large enterprises, defense leaders share many concerns about generative AI and its implications. **In a summary of survey responses, these generative AI issues, in a defense context, rose to the top of the list:**

- How can organizations ensure ethical and responsible use of generative AI in defense, address risks, control for biases, maintain human oversight, and adhere to international norms and standards?
- How can the security, privacy, and integrity of sensitive and classified defense data be maintained when training and deploying generative AI models for military applications?
- How can the transparency, explainability, and trustworthiness of generative AI models be improved for use in decision-making processes?
- What legal frameworks, international agreements, and ethical standards should be developed to guide the responsible use and deployment of generative AI in defense, including autonomous systems and cybersecurity?
- How can generative AI models be adapted and optimized to handle dynamic, unpredictable scenarios and perform reliably in critical defense situations?

Defense leaders point to a common denominator for addressing these concerns: **building trust in the models that inform generative AI**. Trust begins with a data fabric approach for data governance, with an understanding that data is useful when it is protected and when its context, content, and quality can be trusted and verified.[10]

FIGURE 2

Where is your defense organization considering deploying generative AI?



Case study

Deploying generative AI for military training and intelligence operations

Semantic Edge
Octo, an IBM Company

Every year, many members of the US military spend hundreds of individual hours in training sessions to learn how to use complex weapons systems and intelligence collection platforms. Now, the military is using generative AI to enrich these training experiences, while reducing training time.

With Semantic Edge technology, large language models enable real-time natural language interaction with curated user guides, manuals, and technical documentation. Trainees benefit from focused learning experiences and, with shortened training cycles, return to duty faster.[11]

According to US Special Operations Command (SOCOM) leadership, special operations forces capture more than 127 terabytes of digital material each year. Ths is the equivalent of 44,000 feature-length movies or 50 NFL seasons worth of video. Instead of sending data back to the US for processing, commanders can rapidly exploit documents for actionable intelligence in the field, because Semantic Edge enables generative AI to work on edge computing resources.

With secure military grade models built on open-source AI platforms, users can:

- Ask questions in natural language
- Get answers based on ingested documents
- Know the locations of source documents that generated responses

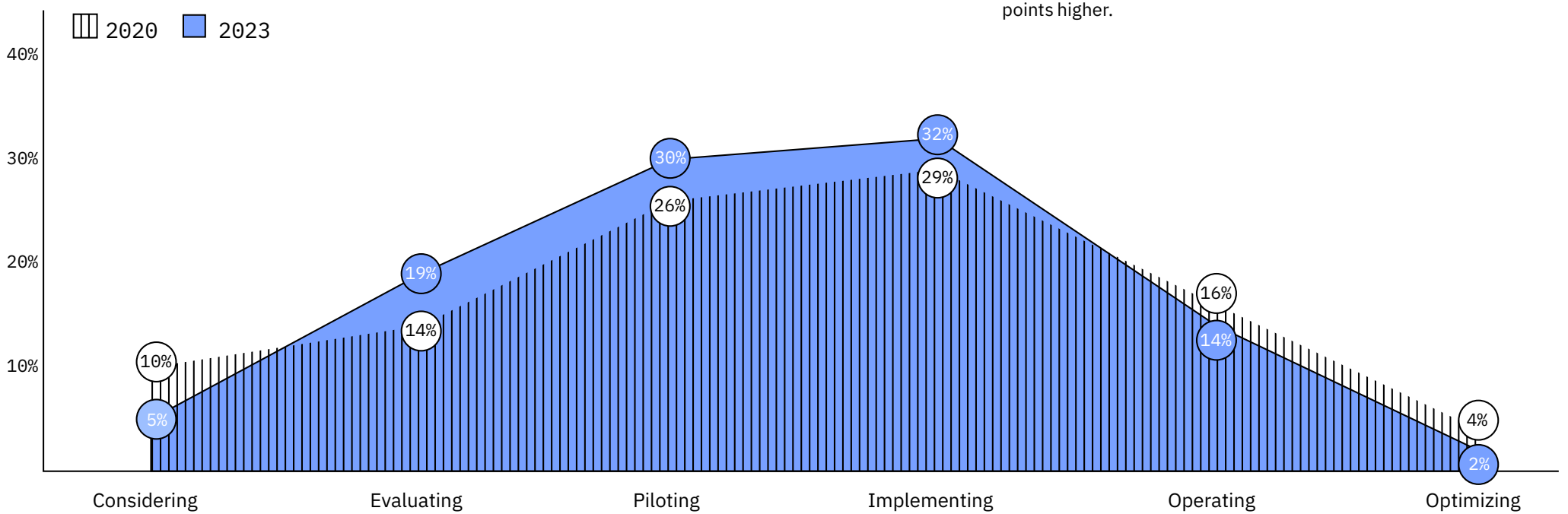
Progress lags behind expectations on adopting and scaling AI for defense

In our survey, 95% of defense leaders indicate that their organization has taken or is taking action to adopt AI technology to increase capabilities or support operations. However, despite this high rate of adoption, most leaders characterize AI progress as limited, uneven, and not up to the expectations they set three years ago.

For example, 29% of defense leaders reported in 2020 that their organization was at the implementation stage in adopting AI. In 2023, their reported level of AI implementation stood only three percentage points higher.

FIGURE3

Where is your organization in adopting AI?



Where are defense organizations reporting the greatest AI adoption maturity in 2023? The top three defense applications include incorporating AI into autonomous and semi-autonomous vehicles and in the delivery of medical and health services. But even in these areas, progress lags where defense leaders expected to be three years ago. For example, in 2020, 62% of surveyed leaders expected to be at least in the process of implementing AI capabilities for semi-autonomous vehicles in the next three years. However, when we asked these same leaders about their adoption process for this capability in 2023, only 32% of organizations reported progressing to the implementation stage.

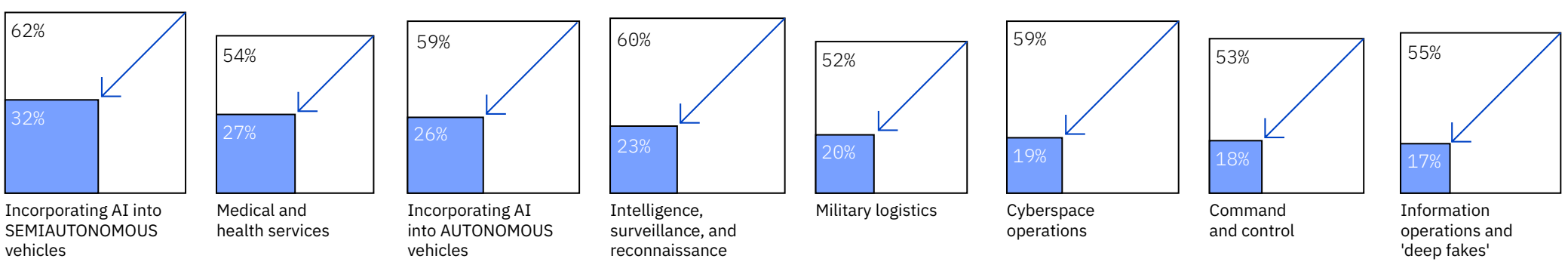
However, in the next three years, organizations expect to make big strides in adopting AI in other defense application areas—particularly in intelligence, surveillance and reconnaissance, command and control, and information operations—where they expect to see gains of over 40% in implementation, operation, and optimization.

Where does AI progress stand in the many functional areas that support defense applications? In some ways, survey indicators show these areas are lagging even further behind defense applications. For example, in 2020, more than two-thirds of leaders expected their organization would have progressed AI solutions for information security to the implementation stage in the next three years. However in 2023, only 28% of these leaders report matching this level of adoption progress.

FIGURE4

Where do you expect your organization to be in adopting AI for these defense applications in three years?

Variation between where defense leaders surveyed in 2020 expected they would be in 2023 and where they actually are in adopting AI for defense applications.



Case study

Boosting aircraft mission readiness with an AI Equipment Maintenance Assistant

US Air Force

In the US Air Force, aircraft technicians typically spend 80% of their time searching for information when executing a service order. In addition, due to high turnover among experienced technicians and a shortage of aviation maintenance specialists, new workers need immediate access to institutional knowledge to resolve problems quickly and effectively.

By using an AI-powered Equipment Maintenance Assistant (EMA), technicians can apply AI capabilities at the point of work. They get up-to-date answers in seconds through natural language queries, without searching through mountains of manuals, bulletins, and directives.[12]

EMA addresses knowledge gaps by operationalizing AI technology across maintenance data. **EMA also combines AI with human expertise, and combines predictive maintenance models, cognitive technology, and generative AI to:**

- Reduce mean time to repair (MTTR) through accelerated troubleshooting and recommended actions, parts, and tools
- Narrow the knowledge gap created by technician turnover
- Increase technician efficiency
- Improve the mean time between failure (MTBF) rate through suggested actions and improving the first time to fix (FTTF) rate

Defense organizations intend to bring more AI capabilities in-house and reduce reliance on the private sector

In 2020, more than half of defense leaders said they were heavily reliant on the private sector for AI capabilities in many areas.

In one top category—advanced analysis techniques specific to defense and the armed services—62% of these leaders said that they were mostly or significantly reliant on the private sector.

However, during the last three years, defense leaders have made it a priority to reduce dependence on the private sector for many AI capabilities, and it shows in the data.

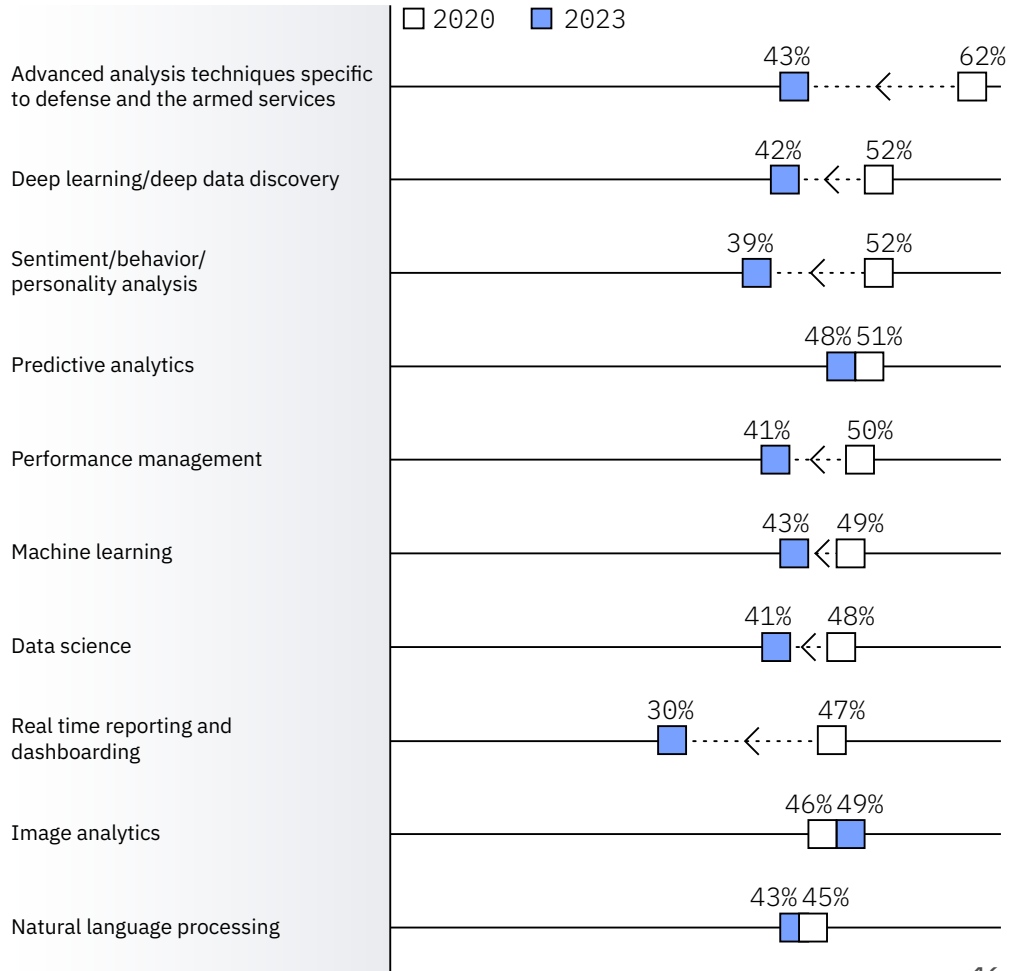
In one telling example, for the category of advanced analysis techniques specific to defense and the armed services, reliance on the private sector is now 43%, a decrease of 19%.

Despite the focus on greater autonomy, many defense leaders will continue to look to private sector partners for assistance in key areas. For example, in eight out of the ten top categories of AI capabilities, defense leaders expect to remain at least somewhat reliant on their private sector partners in 2026. This trend suggests that engagement with the private sector across a wide range of capabilities will continue at meaningful levels and defense leaders will be strategic in prioritizing the AI tasks where more internal capabilities are needed.

For example, in several areas where defense leaders were significantly or mostly reliant on the private sector in 2023, they intend to make great strides in bringing these AI capabilities in-house. By 2026, these priorities will include: reducing image analytics from 49% reliance on the private sector to 16%, reducing predictive analytics from 48% reliance to 19%, and reducing machine learning from 43% reliance to 12%.

FIGURE 5

How reliant is your organization on the private sector for the following capabilities today?

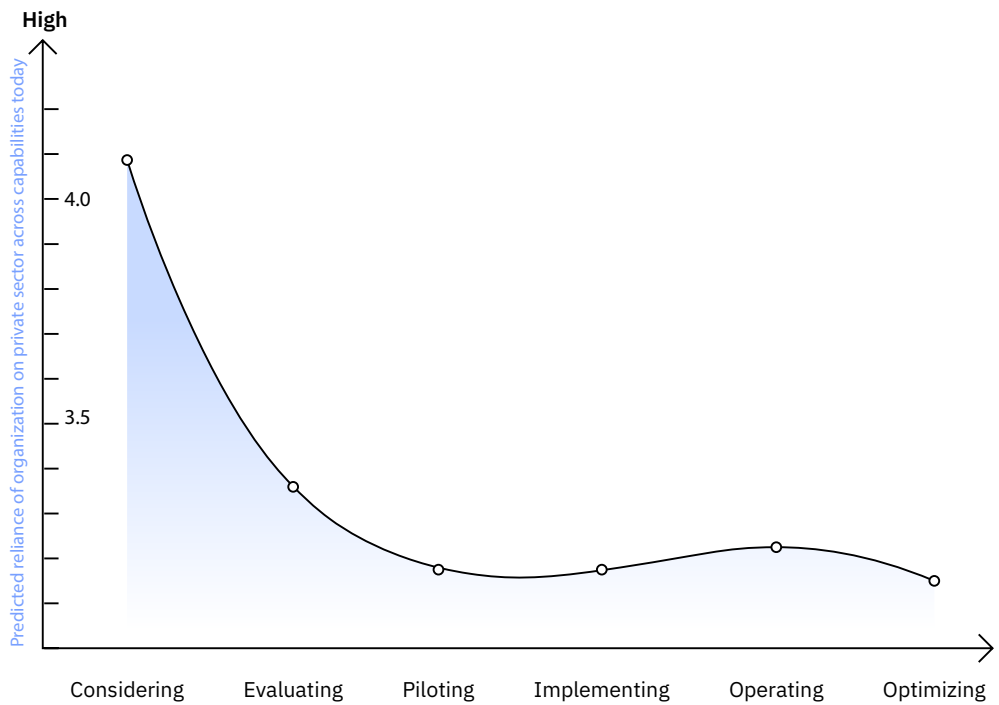


One trend remains the same now as it did in 2020: defense leaders depend more on private sector AI expertise during the earliest stages of AI adoption, especially during consideration and evaluation. As progress continues through piloting, implementing, operating, and optimizing, defense organizations are taking on more responsibility and taking on greater autonomy at later stages of AI adoption.

For defense organizations to increase their own internal AI capabilities and reduce reliance on contractors, they will need to recruit and retain more experienced AI professionals, especially at senior levels. This is an ongoing challenge because AI projects require more than an IT background, including advanced mathematics and statistical analysis skill sets. In addition, the private sector typically pays higher salaries than the government. However, by promoting opportunities to work with advanced AI technology on missions of national importance, defense-related departments are stepping up efforts to attract candidates for its AI corps.[13]

FIGURE 6

Defense organization reliance on the private sector across the adoption life-cycle



Confronting barriers to AI adoption and increasing co-creation between defense organizations and the private sector

Collaboration between defense organizations and the private sector will be key to accelerating AI adoption

In our survey, defense leaders most often cite data governance, security and privacy, availability of skilled resources, and cultural issues as the biggest roadblocks to developing and deploying AI.

Leaders expect these issues will slow down AI adoption during the next three years as defense organizations transform attitudes and operations to address them.

Interestingly, risk and governance, organization and skills, and data and platform issues were also identified as the top three AI readiness gaps that concern global business executives, as expressed in a 2023 IBM IBV report on the state of the enterprise generative AI market.[14]

Defense leaders and private sector business leaders are closely aligned on where they need to focus efforts to accelerate AI adoption, and what needs to change to bring AI goals within reach. But in practical terms, **how can defense organizations work with private sector defense experts on high-value AI projects and expedite knowledge transfer through co-creation?**

To foster collaborative research and development among defense organizations, the private sector, and academic partners, consulting company Octo has built an "oLabs" AI center for mission innovation.[15] The center brings together AI engineers, data scientists, special operators, intelligence analysts, and other domain experts to develop AI applications and build AI-powered prototypes.

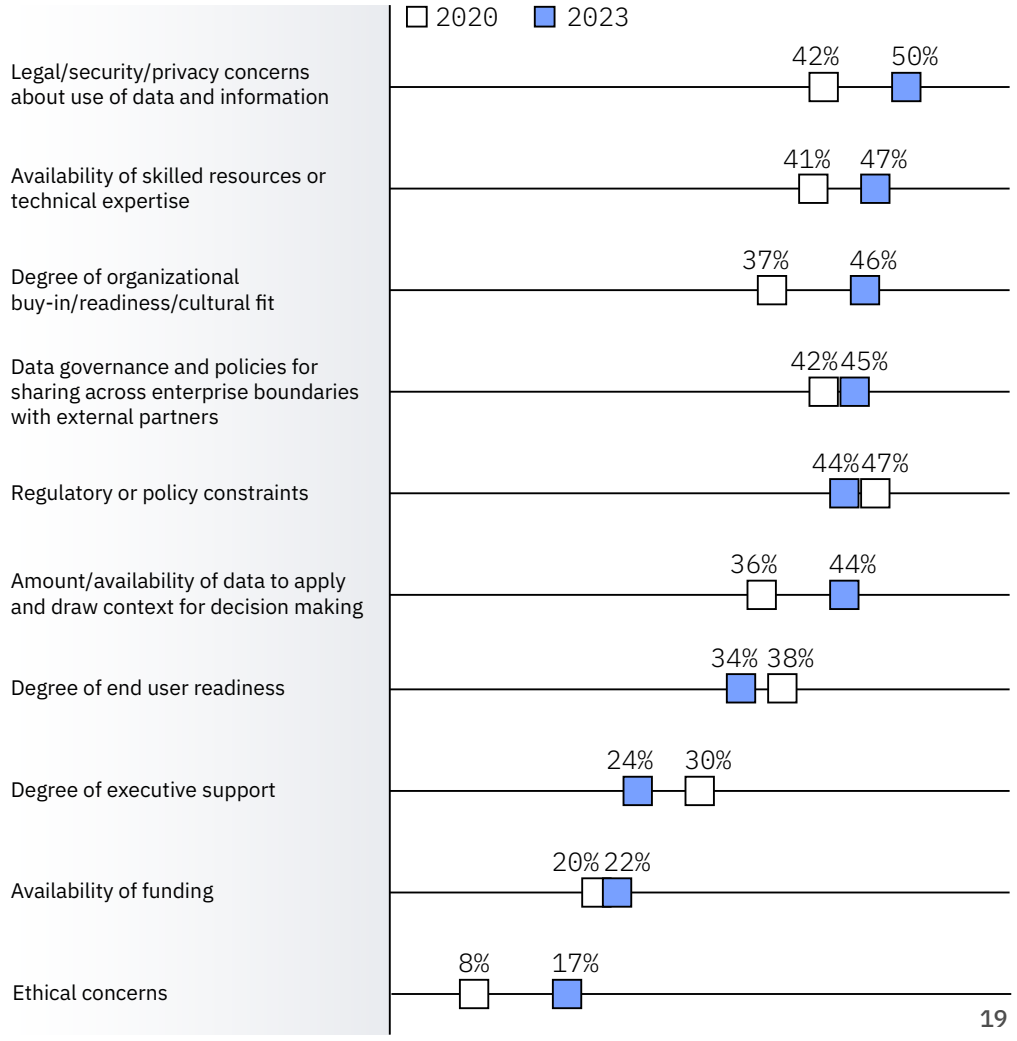
The center includes a virtual close-quarters battle facility and a robotics laboratory, enabling military personnel to evaluate sensor and data performance in many types of operational environments. Teams can also remotely access computing and data storage infrastructure, while building capability and expertise to support AI edge computing in challenging communication situations.

AI innovation centers such as "oLabs" are designed to be magnets for AI talent. The dynamic workspace culture attracts tech industry and academic experts who want to explore, research, and solve complex problems with the defense and intelligence community partners, and boost the defense AI knowledge base in ways that can be quickly and decisively deployed in the field.

Innovation centers bring together domain experts to develop and test AI applications and prototypes.

FIGURE 7

What are the top barriers your organization faces in implementing AI?



Case study

Improving autonomous vehicle readiness with predictive and prognostic maintenance modeling

US Army

From self-driving systems for convoy vehicles to high-speed robotic vehicles that can cross uneven terrain, the US Army is deploying a growing fleet of autonomous vehicles. However, despite the tactical advantages these vehicles provide, they present a new range of maintenance challenges.

Without a driver, no one notices degrading performance. This creates uncertainty around readiness—not an ideal situation for mission-critical vehicles whose failure can expose personnel to physical risk. Autonomous vehicles with Lidar pose additional maintenance challenges because these sensors are sensitive to vibration and can become inaccurate, leading to navigational issues, collisions, and vehicle damage.

Onboard predictive and prognostic maintenance modeling (PPMx) uses AI technology to predict autonomous vehicle failure and improve vehicle readiness.[16] When deployed, the models assess vehicle condition and send alerts on anomalies and deteriorating performance. This provides lead time to perform maintenance before equipment failure.

On average, predictive maintenance has been shown to:

- Increase productivity by 25%
- Reduce breakdowns by 70%
- Lower maintenance costs by 25%

Action guide

1

Leaders set the pace for AI advantage in defense

- Think big and role-model a “no excuses” mindset to accelerate AI development, deployment, and iterative improvement.
- Support an organizational culture that understands and embraces the transformative potential of AI.
- Create a common AI framework, a common language, and consistent methodology.

2

Build a trusted and secure AI infrastructure

- Prioritize and enable data governance to build trustworthy, auditable, and explainable models, especially for generative AI deployments.
- Construct ethical frameworks that are transparent and resistant to bias drift.
- Leverage a hybrid-by-design approach with proprietary and open-source models that can be securely trained, tuned, and owned.

3

Scale AI capacity and capability

- Start with carefully selected use cases and minimum viable products and scale rapidly to transform to new ways of working.
- Leverage ecosystem partner and private sector expertise. Consider creating a defense industry AI advisory board to share lessons learned and expedite adoption.
- Expand AI training of staff and service members and explore new ways to recruit AI talent to fill gaps.

Study approach and methodology

In 2023, the IBM Institute for Business Value, in cooperation with Oxford Economics, surveyed 600 chief information officers and chief technology officers from 32 nations, including members of the North Atlantic Treaty Organization (NATO) and the Five Eyes intelligence alliance among Australia, Canada, New Zealand, the UK, and the US. Respondents were screened to ensure they were both familiar with AI and their organizations' strategies and plans for investing in and implementing AI capabilities in the future.

These leaders represent organizations from a broad range of mission functions, including combat and fighting arms (29%), combat support (44%), and combat service support (27%). Research provides longitudinal insights from a survey of similar leaders from 250 defense organizations conducted in 2020 and includes additional insights on the topic of generative AI.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBM IBV's email newsletter at ibm.com/ibv. You can also find us on LinkedIn at https://ibm.co/ibv-linkedin.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

Notes and sources

1 Uppsala Conflict Data Program-Department of Peace and Conflict Research web site. Uppsala University. 2024. https://ucdp.uu.se

2 Shane III, Leo. “Amid recruiting woes, active-duty end strength to drop again in 2024.” *MilitaryTimes*. December 14, 2023. https://www.militarytimes.com/news/pentagon-congress/2023/12/14/amid-recruiting-woes-active-duty-end-strength-to-drop-again-in-2024/

3 Allison, George. “British military shrinks by nearly 30% since 2000.” *UK Defence Journal*. January 26, 2024. https://ukdefencejournal.org.uk/british-military-shrinks-by-nearly-30-since-2000/#

4 *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage*. US Department of Defense. June 27, 2023. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

5 Burgan, Kate. “Feds Spent $3B on AI Last Year, Lawmakers Hurried Legislation.” *MeriTalk*. April 18, 2023. https://www.meritalk.com/articles feds-spent-3b-on-ai-last-year-lawmakers-hurried-legislation/

6 Mayflower Autonomous Ship. https://www.mayflower400uk.org/mayflower-autonomous-ship/

7 *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage*. US Department of Defense. June 27, 2023. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF

8 Gosselin-Malo, Elisabeth. “NATO to update artificial intelligence strategy amid new threats.” *C4ISRNet*. November 30, 2023. https://www.c4isrnet.com/artificial-intelligence/2023/11/30/nato-to-update-artificial-intelligence-strategy-amid-new-threats/

9 Eva Dou, Nitasha Tiku, and Gerrit De Vynck. “Pentagon explores military uses of large language models.” *The Washington Post*. February 20, 2024. https://www.washingtonpost.com/technology/2024/02/20/pentagon-ai-llm-conference/

10 *Data governance for data driven organizations*. IBM ebook. January 2023. https://www.ibm.com/downloads/cas/V348GDJ2

11 Based on internal IBM oLabs white paper.

12 AI and autonomy: AI assisted aircraft maintenance. IBM case study. https://staging.catalysis.co.uk/IBM/08-006-government-interactive-asset-us/pages/ai-and-autonomy.html

13 Doubleday, Justin. “DHS sets ‘aggressive recruiting strategy to fill AI jobs.” *Federal News Network*. February 19, 2024. https://federalnewsnetwork.com/artificial-intelligence/2024/02/dhs-sets-aggressive-recruiting-strategy-to-fill-ai-jobs/

14 *Enterprise generative AI: State of the market*. IBM Institute for Business Value, October 11, 2023. https://ibm.co/enterprise-generative-ai

15 Octo oLabs Center for Innovation. https://olabs.octo.us

16 AI and autonomy: Increasing operational readiness. IBM case study. https://staging.catalysis.co.uk/IBM/08-006-government-interactive-asset-us/pages/ai-and-autonomy.html

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2024