POLICY REPORT

BRENNAN CENTER FOR JUSTICE

The Business of Military AI

By Amos Toh and Emile Ayoub MARCH 2026

Brennan Center for Justice at New York University School of Law

Table of Contents

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that works to reform and revitalize — and when necessary defend — our country's systems of democracy and justice. The Brennan Center is dedicated to protecting the rule of law and the values of constitutional democracy. We focus on voting rights, campaign finance reform, ending mass incarceration, and preserving our liberties while also maintaining our national security. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, in the courts, and in the court of public opinion.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at
brennancenter.org

Introduction

In a world at war on five continents and amid intensifying great power competition, the U.S. Department of Defense (DOD) has forged extensive partnerships with the tech industry to modernize the military's capabilities.[1] Rapid technological advances have made artificial intelligence (AI) a compelling tool for mining data and speeding up decision-making in the battlefield. AI may also prove useful in a wide range of support functions, from helping the military forecast weapons maintenance and repair needs to organizing supply lines during conflict.

Military leaders have credited Project Maven — a pilot project with leading tech companies to develop AI that sifts through and interprets drone and satellite footage — with greatly reducing the time it takes to identify and strike targets.[2] And the Defense Innovation Unit (DIU), the Pentagon organization serving as a bridge between Silicon Valley and the military, has fast-tracked contracts for experimental drone technology, which the DIU promises will make combat operations "less expensive" and "put fewer people in the line of fire."[3]

Many claims about the technology's effectiveness, however, remain untested, and risks to soldiers and civilians remain unaddressed. AI errors can cascade into system failures that misidentify civilians as targets while overlooking genuine threats — undermining mission objectives, combat safety, and obligations under the laws of war. These failures could happen even with humans in the loop. Commanders and operators of weapons systems are generally supposed to independently verify and confirm AI-generated targets. In reality, they may become too willing to defer to algorithmic recommendations. Additionally, greater reliance on AI reduces the lives of individuals to blips and data points on a screen, which could desensitize soldiers to acts of killing and destruction.

Despite these dangers, tech and government leaders insist that the military is not moving fast enough. Shyam Sankar, Palantir Technologies' chief technology officer, has expressed alarm that "the West has empirically lost deterrence" against China because of excessive regulation and bureaucracy.[4] Secretary of Defense Pete Hegseth has said that the acquisition of new weapons technology is "unacceptably slow"; he has directed a slew of changes to put the military "on a wartime footing."[5] This push coincides with an unprecedented expansion of the department's annual budget to $1 trillion for fiscal year 2026, more than a 13 percent increase from fiscal year 2025.[6]

The Pentagon's race to adopt AI is poised to accelerate its substantial and increasing reliance on the technology. Since Project Maven's launch in 2017 and particularly since 2020, Pentagon contracts awarded to tech companies that specialize in building and supporting AI systems have grown exponentially. The two companies leading this growth — data analytics giant Palantir Technologies and autonomous systems manufacturer Anduril Industries — have grown their share of defense revenue faster than most other comparable government contractors. Industry leaders are also taking on a greater policymaking role, particularly when it comes to acquisition, testing, and oversight of the very technologies they have a financial stake in.

Responsible innovation requires the government to strike the right balance between speed and caution. The military must be able to make levelheaded, evidence-based assessments about the proper role of any new technology in filling capability gaps. It must also conduct the due diligence and testing needed to ensure that newly adopted technologies are safe and effective and do not infringe on fundamental rights.

Yet the accelerating use of AI in warfighting has not been met with commensurate urgency to reckon with its dangers. It has been subject to minimal transparency, insulating it from meaningful public scrutiny and legislative oversight. Even the most basic information about the types of systems the Pentagon is adopting, the degree to which they are effective and safe, and the extent to which their use adheres to the laws of war and other guardrails is often hidden from Congress and the public. The proprietary nature of many of these systems also raises questions about whether the Pentagon itself has access to the data necessary to conduct meaningful due diligence and monitor performance.

Further, there are few safeguards to ensure a proper accounting of the costs and risks of AI warfare. In addition to the acquisition overhaul that Hegseth is leading, the Pentagon has sharply curtailed agency-wide efforts to test and evaluate major weapons systems and assess the risks of civilian harm, making it more difficult to assure that AI-augmented systems will work as promised and without excessive collateral damage. Rules that President Joe Biden's administration introduced to manage AI risk — which were inadequate to begin with — may be further weakened under President Donald Trump.

Implementing regulations and oversight throughout the acquisition, training, refinement, and deployment of an AI program can spell the difference between success

and failure. Autonomous drones sent by U.S. tech start-ups to help Ukraine in its fight against Russia, for example, proved to be error-prone, difficult to repair, and easily foiled by relatively basic electronic jamming techniques.[7] Ukraine's reliance on these drones has been limited, but if the U.S. military were to embed such risky and unreliable AI tools into its core combat functions, it could put civilians and humanitarian workers in the crosshairs. In Gaza, too, inaccuracies in AI-generated intelligence about the identity and location of militants have informed Israeli strikes that killed scores of civilians,[8] while facial recognition errors have contributed to the wrongful arrest and interrogation of Palestinians.[9]

This report documents the military's expanded use of AI, the tech industry's role in pushing for even greater adoption, and the risks posed by ineffective regulation. Part I identifies the areas of warfighting where the DOD is making the heftiest investments in AI. Part II is a deep dive into defense procurement data to show how the department directs these investments increasingly toward a handful of tech firms with the resources to develop and support AI systems. Part III traces the growing policymaking impact and influence of these firms. Part IV analyzes gaps and loopholes in the existing patchwork of rules governing how the military acquires and uses AI. Part V examines how the rush to adopt AI without meaningful safeguards or independent oversight could burden the military with ineffective, unsafe systems that also inflict excessive civilian harm and infringe on privacy and civil liberties. Part VI offers a roadmap of checks and balances at this transformative moment for the future of war.

I. Military Spending on AI

The DOD defines AI as technology that performs tasks that would otherwise require human intelligence.[10] It makes up an increasing share of the defense budget. But identifying precisely by how much is difficult. One challenge is definitional: As a general-purpose technology, AI is used to increase automation or support decision-making across a wide range of military systems and programs.

For 2026, for example, the department requested $13.4 billion for "autonomy and autonomous systems," which includes unmanned and remotely operated drones and weapons.[11] While AI is neither a drone nor a weapon, it is an increasingly pervasive feature of how these systems navigate, communicate with each other, and strike targets. The $13.4 billion figure accounts for a lot more than the costs of embedding AI in autonomous systems, but it does not capture many other costs, such as the integration of the technology into other surveillance and weapons systems, or its use to forecast maintenance and repair needs,[12] identify bottlenecks in supply chains for essential equipment,[13] and automate administrative operations.[14]

This report focuses primarily on applications of AI that are most directly linked to military actions resulting in harm to civilians and civilian infrastructure. One such category is AI-enabled intelligence, surveillance, and reconnaissance,[15] as the DOD has sought to transform near endless streams of data from military sensors, commercial partners, and the internet into actionable recommendations on targets, weapon selection, civilian impact, and other aspects of battlefield decision-making. Recent breakthroughs in so-called foundation models — AI trained on massive datasets to perform a range of general tasks such as text synthesis, image manipulation, and audio generation[16] — have intensified the technology's appeal in helping the military make sense of complex information environments.[17]

The DOD is also increasingly fielding AI to enhance the autonomy of unmanned systems, such as reconnaissance or lethal drones.[18] The department has promoted these systems as an alternative to deploying ground troops while promising that they will ultimately cost less than conventional weapons such as tanks, combat aircraft, and warships.[19]

Spending forecasts over the past few years indicate that AI-related program costs for autonomous systems and surveillance and intelligence analysis could surpass $75 billion. For example, in 2018, the Army awarded a contract to Microsoft worth up to $22 billion to equip soldiers with headsets that combine augmented reality with AI.[20] (This partnership did not generate an effective prototype, and the Army has since reassigned the contract to Anduril.)[21] In 2025, the Army awarded a contract to Palantir worth up to $10 billion to develop "data integration, analytics and AI tools."[22] In the meantime, the Air Force plans to spend around $9 billion by 2029 on autonomous aircraft development.[23] And Congress has appropriated $25 billion for the Trump administration's Golden Dome missile defense shield project, which will rely on AI to detect and counter missile threats over U.S. territory.[24]

Training, refining, and hosting these systems also incurs significant data, energy, and infrastructure costs. In 2022, the DOD awarded a contract worth up to $9 billion to Google, Oracle, Microsoft, and Amazon Web Services to develop and maintain the department's cloud computing infrastructure.[25] Separate infrastructure to handle sensitive data and software needs for defense and other intelligence agencies are reportedly worth tens of billions more.[26]

These figures represent a modest proportion of the overall defense budget, which has grown to $1 trillion for fiscal year 2026.[27] But the Pentagon is pushing the military to become an "'AI-first' warfighting force," signaling that spending is likely to grow.[28] As such, this is a critical time to establish robust checks and balances and foster public trust in how the technology is used for the nation's defense.

Because DOD entities with intelligence missions may keep part or all of their spending on AI classified, only a partial picture of what the military is buying emerges.[29] The military's AI inventories are also secret, although unclassified spending reportedly covers more than 800 projects as of 2023.[30] A Brennan Center analysis of public records and interviews with AI and defense experts surfaced the following key investments.

Surveillance, Analysis, and Target Selection

The military has prioritized AI development to identify targets and organize missions. In 2017, it launched Project Maven (known officially as the Algorithmic Warfare Cross-Functional Team),[31] at the time a pilot program with Palantir, Google, and other tech companies to develop computer vision algorithms capable of combing through vast amounts of satellite imagery and drone footage to

pick out people and objects of interest.[32] The military has used Maven-developed capabilities to identify targets for strikes in Iraq, Syria, Yemen, and Ukraine.[33]

Project Maven, now simply known as Maven, has evolved into a "program of record" — military parlance for long-term programs with dedicated funding in the defense budget.[34] Its focus on gathering and analyzing video and satellite images has expanded to cover a wide range of data sources. This includes cell phone location information, social media analysis, and data from radar systems and infrared sensors capable of detecting points of interest through difficult conditions like clouds, darkness, and rain.[35] The National Geospatial-Intelligence Agency (NGA) assumed primary responsibility for Maven's geospatial intelligence functions in 2023.[36]

Maven has also led to the development of the Maven Smart System (MSS), which centralizes access to the military's vast catalog of data sources while providing a suite of AI tools to process and analyze the data.[37] In combat operations, for example, the Army has relied on MSS to visualize the battlefield and help it identify and choose potential targets.[38] Over the past few years, combatant commands — military commands responsible for planning and executing operations across geographies or functions (e.g., cyber or special operations)[39] — have also expanded their use of MSS.[40] The DOD plans to raise system spending to nearly $1.3 billion through 2029, nearly three times the amount it originally budgeted for in 2024.[41]

MSS is central to the Pentagon's strategy to modernize command and control — a commander's exercise of authority and direction over assigned forces to complete a mission.[42] This strategy, known as the Combined Joint All-Domain Command and Control (CJADC2) approach,[43] is analogous to the ride-sharing app Uber.[44] Just as Uber's algorithms connect a wide array of data points about drivers, riders, and their surroundings to dispatch and price trips in real time, CJADC2 aims to stitch together an all-encompassing view of the battlefield from military, commercial, and open-source data.[45] In a potentially related move, one of Defense Secretary Hegseth's first actions on AI was to direct the Army to deploy AI-driven command and control capabilities across units that oversee and coordinate combat operations by 2027.[46]

Additionally, AI is key to the Army's efforts to equip soldiers with augmented reality technology in combat. The Army has been developing augmented reality headsets — known as the Integrated Visual Augmentation System (IVAS) — for combat troops since 2018.[47] The latest prototypes of the headset rely on AI to help soldiers interpret the environment within and beyond their sight lines,[48] such as by detecting, tracking, and classifying objects of interest.[49]

Autonomous Capabilities

While the military has deployed drones for decades, AI is transforming how it uses them to conduct surveillance, gather intelligence, and strike targets. The DOD has been investing heavily in projects that aim to mass-produce drones and other unmanned systems that can communicate with each other and continue to strike targets even if they lose touch with their human operators.

The Air Force's Collaborative Combat Aircraft program aims to develop fleets of AI-enabled drones that will operate alongside manned squadrons to perform missions.[50] The DOD forecasts that it will spend $8.9 billion on the program from 2025 to 2029.[51] The Replicator initiative, another major autonomy project started during the Biden administration, aims to produce thousands of low-cost, disposable drones and weapons.[52] This program was overseen by the DIU, the Pentagon organization tasked with partnering with Silicon Valley to integrate the latest commercial advances in AI and other technologies into weapons systems[53] and has now transitioned to a new division under Special Operations Command known as the Defense Autonomous Warfare Group (DAWG).[54] In January 2026, DIU colaunched a $100 million contest with DAWG to prototype technology that directs drone swarms and missions based on orders given by battlefield commanders.[55] One successful submission, led by the autonomous software company Applied Intuition Inc., plans to use OpenAI's foundation model to translate voice commands into machine-readable instructions.[56]

These investments are inspired in part by the Ukraine war, the world's first large-scale drone war.[57] Hegseth is committed to expanding the U.S. military's drone and counter-drone capabilities: He has directed the Army to deploy drones in every division and to improve counter-drone mobility and affordability by 2027.[58]

Foundation Models

The explosive debut of ChatGPT in 2022 spurred government efforts to harness the underlying technology, known as foundation models, for military use. In July 2025, the DOD tapped OpenAI, Anthropic, xAI, and Google to prototype virtual agents based on their models across "a variety of mission areas."[59] These agreements followed the creation in 2024 of the Artificial Intelligence Rapid Capabilities Cell, responsible for driving model deployment in weapons development, command and control systems, intelligence activities, and administrative functions.[60] The department has since certified Anthropic's model, Claude, and xAI's Grok for use on its classified systems.[61]

Claude was reportedly used in the U.S. attack on Venezuela and the capture of Nicolás Maduro, leading to a standoff between Anthropic and the Pentagon about whether the company can restrict it from using the model for mass surveillance of Americans or operating autonomous weapons.[62] The DOD insists that it should be "free from usage policy constraints that may limit lawful military applications."[63] But deploying models to facilitate large-scale collection and analysis of Americans' personal and sensitive data is a significant invasion of privacy at odds with the Fourth Amendment,[64] and the automation of lethal targeting without sufficient human oversight may violate the laws of war.[65]

AI Infrastructure

As the military's AI capabilities grow, so too have its demands for data that can be collected and analyzed using AI technology to generate intelligence and other insights. A burgeoning share of this information is sourced from commercial data brokers,[66] which harvest data from mobile apps and social media, advertisers, cars, and other internet-connected devices and sell them to government and other buyers.[67] The Defense Intelligence Agency, for example, has purchased smartphone location data, and the Coast Guard has purchased a tool that aggregates and analyzes social media feeds and other publicly available sources of information.[68] Much of this may include U.S. person information that should be subject to constitutional and statutory protections requiring the government to obtain a judicial warrant.[69]

Large-scale AI adoption requires access to vast amounts of data to train and customize the technology according to user needs, along with massive computing power to support such training and customization.[70] In 2018, the DOD conceded that its "multiple disjointed and stovepiped information systems" were lagging far behind its growing reliance on data and AI in warfighting, announcing plans to acquire commercial cloud services for its data and computing needs.[71]

Cloud companies provide data storage and computing resources through online networks supported by data centers that are globally distributed (commonly referred to as the cloud). Commercial cloud services enable military users to "access information from anywhere at any time."[72] Since announcing plans to scale its cloud computing infrastructure in 2018, the DOD has committed billions of dollars to commercial cloud services.[73]

II. Trends and Growth

Even as the largest traditional defense contractors (commonly called defense primes) are expanding their AI offerings, newer defense tech firms backed by Silicon Valley are vying for a bigger market share.

The defense tech sector is sprawling, spanning not just military applications of AI and autonomous systems but also other emerging technologies, such as spacecraft manufacturing and nuclear fusion. Arguably, the most dominant firm of this sector is the rocket and satellite manufacturer SpaceX, the youngest company to place in the top 40 government contractors by 2025 defense revenue, on the strength of its satellite contracts with the Pentagon.[74]

But the two tech companies that have grown their share of defense revenue faster than nearly any others are Palantir and Anduril. (The appendix lists key relevant defense contracts.) Market valuations, funding rounds, and media mentions also show that both companies have attracted outsize funding and attention from investors.[75]

To be sure, the five biggest defense primes — Lockheed Martin, RTX (formerly Raytheon Technologies), Northrop Grumman, General Dynamics, and Boeing — continue to dominate defense spending. The Brennan Center's analysis shows that in fiscal year 2025, Lockheed Martin, the largest defense contractor, amassed $76 billion in contracting revenue. RTX, the second-largest defense contractor, amassed $35 billion. These numbers are many times the amounts that Palantir (at $903 million), Anduril (at $912 million), and other notable AI and data analytics firms brought in that year.

These figures, however, only tell part of the story: 2025 was the most profitable year for Palantir and Anduril since they began doing business with the military. This marks a period of extraordinary growth, during which both companies have increased their share of defense revenue faster than most other government contractors.

Comparing their respective revenue growth over two time frames — the 10-year period from fiscal years 2016 to 2025, and from the first year each company exceeded $10 million in revenue to 2025 — shows that on both measures, both companies vastly outperformed most of their competitors.

Between fiscal years 2016 and 2025, Anduril typically increased its revenue by 143 percent from one year to the next, while Palantir increased its revenue 54 percent by the same measure (see figure 1).

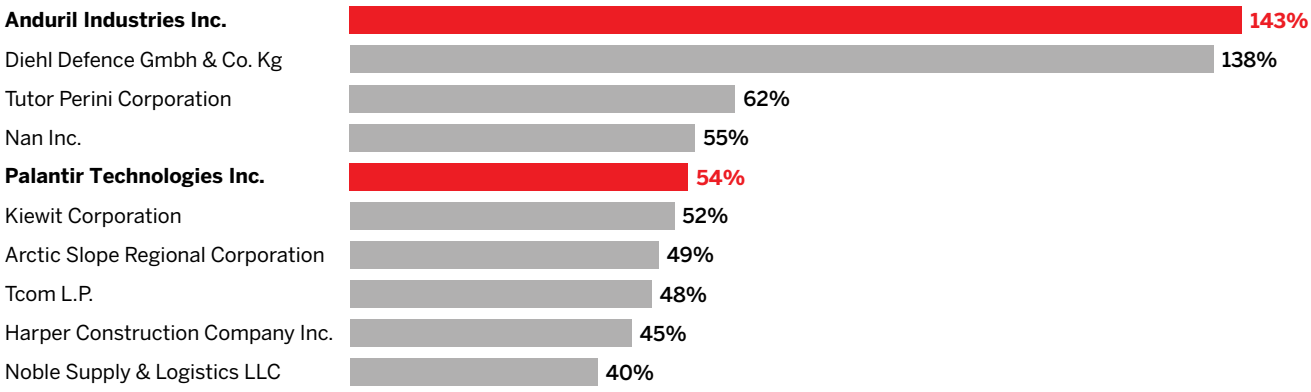
As figure 2 shows, this makes Anduril the fastest-growing among contractors with the largest defense revenues in 2025; Palantir is fifth.

Both companies continued to grow quickly, even after they had established themselves as government contractors with substantial defense revenue. Palantir exceeded

FIGURE 1

Fastest-Growing Major Defense Contractors

Median annual growth between 2016 and 2025

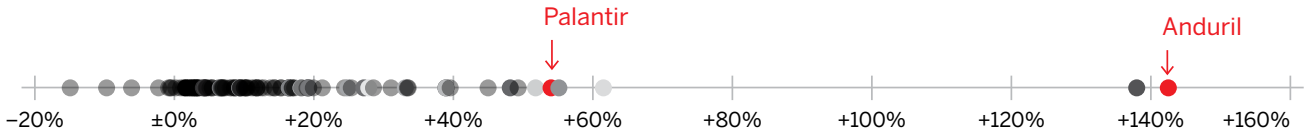


Notes: Major defense contractors are the 100 contractors with the highest defense revenues in 2025.

FIGURE 2

Typical Growth for Major Defense Contractors

Median annual growth between 2016 and 2025



Notes: Major defense contractors are the 100 contractors with the highest defense revenues in 2025.

$10 million in annual defense revenue in 2011, and Anduril hit the same milestone in 2019. Their growth since those breakthrough years has far surpassed that of comparable contractors, as figures 3 and 4 depict.

Palantir's and Anduril's projections that their government revenues have much more room to grow are driving up their valuations.[76] Palantir, a publicly listed company whose market capitalization has surpassed four of the five defense primes, was valued at $324 billion the week ending February 6, 2026.[77] A 2026 funding round for Anduril valued the company at $60 billion, double its valuation for the second year in a row.[78]

Company-specific offerings and contracts show that Palantir, Anduril, and the AI and data analytics start-ups following in their footsteps are transforming how decisions are made on and off the battlefield, such as how targets are identified and the types of weapons deployed. Even if expensive, bespoke weapons such as fighter jets and warships remain cornerstones of the military's arsenal, they are increasingly connected and mobilized through AI and fed targets generated with the help of the technology. In the coming years, conventional weapons systems are also likely to operate in concert with AI-powered ones, such as autonomous drones, submarines, and

FIGURE 3

Palantir's Growth in Perspective

Annual defense revenue for Palantir and the 20 defense contractors with the closest revenues in 2011

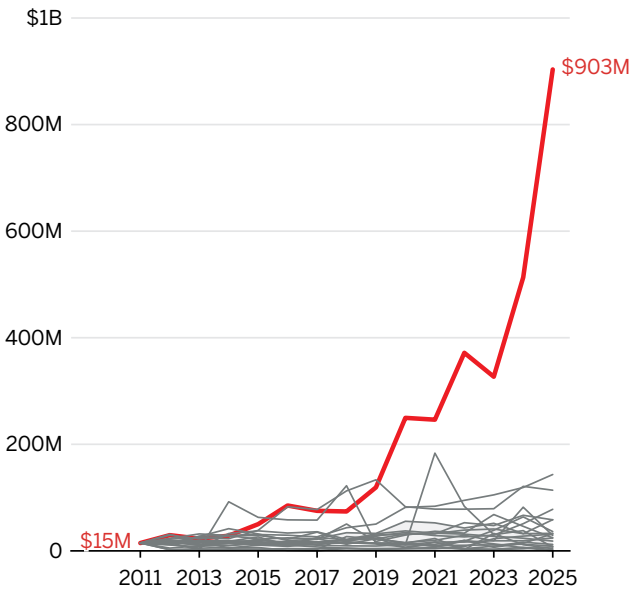
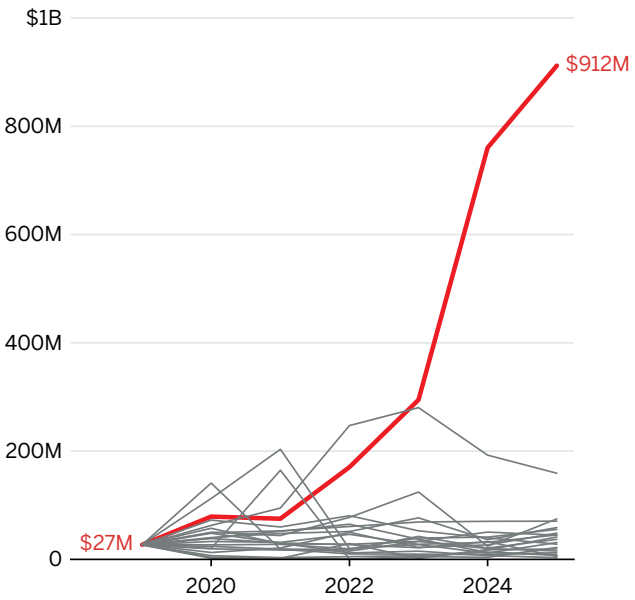


FIGURE 4

Anduril's Growth in Perspective

Annual defense revenue for Anduril and the 20 defense contractors with the closest revenues in 2019



ground vehicles. Urgent questions thus arise about how this paradigm shift increases the risks of civilian harm and friendly fire or otherwise complicates battlefield decision-making.

Palantir

In the wake of the 9/11 attacks, Peter Thiel, then best known as a cofounder of PayPal, wondered whether the software the platform used to detect fraud could be repurposed to identify terrorist threats.[79] He enlisted his law school classmate Alex Karp and a group of Silicon Valley colleagues to launch a company that would translate this concept into reality — Palantir, named after seeing stones used to extract and manipulate intelligence in *Lord of the Rings*.[80] Karp is now Palantir's CEO and Thiel the chair of its board.[81]

Palantir's technology has long been steeped in mystery, but declassified government documents and the company's own disclosures provide important details.[82] Its flagship product, Palantir Foundry, combines and makes coherent vast repositories of data that its customers collect, buy, or otherwise have access to (a capability known as data fusion or integration).[83] Palantir Gotham is a decision-making tool built specifically for defense and intelligence customers; it uses AI to help the military parse and visualize the data that Foundry has organized in order to identify targets and determine which forces and weapons to mobilize and in what order.[84]

Defense procurement records show how Palantir's brand of data fusion and analytics has become indispensable to the military's pivot to data-centric warfare. All branches of the armed forces have bought software from Palantir, as have a range of combatant commands.[85] The Army's volume of business with Palantir is so extensive that in 2025, it consolidated all 75 of its contracts into a single agreement worth up to $10 billion over 10 years.[86] This agreement covers the company's prototype of an AI-based command and control program, called Titan, that synthesizes data about troops, tanks, artillery, and unmanned weapons on the battlefield into intelligence that can help soldiers plot their next move.[87] The agreement also includes licenses and additional refinements to the company's Maven Smart System, which facilitates mission control.[88]

Some of these capabilities have spread to federal and local law enforcement as well. Palantir has, for example, created an Investigative Case Management (ICM) system for the Department of Homeland Security (DHS) that compiles immigration records, employment data, location information, and hundreds of other data points to generate reports on potential targets for detention and deportation operations.[89] Palantir has also sold predictive policing technology to local police departments.[90]

Anduril

In 2017, a group of tech entrepreneurs led by Palmer Luckey founded Anduril Industries, based on Luckey's vision of disrupting the defense industry with engineering and cost-saving innovations from the consumer technology sector.[91] Thiel's Founders Fund, Joe Lonsdale (another Palantir cofounder), and Marc Andreessen (the cofounder of one of the first internet browsers, Netscape) were early investors.[92]

One of Anduril's earliest forays into government contracting was in 2018, when it partnered with DHS to build a virtual wall that it promised would secure the U.S.–Mexico border at low cost.[93] The project consists of a network of surveillance towers loaded with AI features that has become the company's hallmark. Instead of Border Patrol agents having to manually scan surveillance footage, Anduril equipped its towers with off-the-shelf sensors and cameras that use computer vision technology to identify, detect, and track persons or objects of interest.[94] This technology is part of a software platform known as Lattice,[95] which integrates all the data collected by the towers into a centralized system that alerts agents to suspicious activity in real time. Anduril has deployed more than 300 Lattice-powered towers along the United States' southern border at a cost of around $861 million.[96]

Anduril has since parlayed its advances in autonomy and surveillance at the border into a rapidly expanding business selling AI-powered drones and munitions to the military.[97] In 2024, the company won contracts to support two major defense autonomy projects: the Air Force's multibillion-dollar Collaborative Combat Aircraft program (to develop fighter jets that can largely fly themselves)[98] and the Replicator initiative (to build fleets of cheap and disposable drones).[99] Like its surveillance towers, Anduril's drones rely on Lattice to communicate with each other and their human operators, identify and track targets for strikes, and make defensive maneuvers.

Defense procurement records also provide a glimpse into how Lattice is remaking the military's surveillance and communications systems beyond its investments in weapons autonomy. The Space Force is using the software to connect and make sense of disparate streams of surveillance data collected from space.[100] And the Army has reassigned a long-running contract to develop augmented reality headsets for soldiers from Microsoft to Anduril; the latter's prototype relies on Lattice to alert soldiers to incoming airborne threats.[101]

Other AI Contractors

Palantir's and Anduril's successes have spawned a broader ecosystem of military AI start-ups backed by billions in funding from venture capital firms, including

Lonsdale's 8VC, Andreessen's A16z, Thiel's Founders Fund, and Lux Capital, which was cofounded by the early defense tech investor Josh Wolfe.[102] Since 2020, some of these start-ups have captured major contracts in high-priority areas for the DOD, including drone and counter-drone technology. Saildrone, for example, has been working with the Navy since 2021 to develop unmanned maritime vessels that can monitor and track adversaries in harsh ocean environments and areas unable to receive GPS signals.[103] Shield AI was awarded Navy and Coast Guard contracts in 2024 for drones piloted by its AI software, Hivemind.[104] On land, the Army began working in 2022 with the self-driving software supplier Applied Intuition to test and develop unmanned ground combat vehicles.[105]

The military is also working with leading AI companies to integrate the latest advances in the technology across its operations. In 2025, OpenAI, Anthropic, xAI, and Google were awarded contracts to develop military applications of their foundation models.[106] Scale AI also won a contract to prototype large language models — a type of foundation model — in missing planning.[107] At the end of the year, the DOD launched a platform using Google's model, Gemini, to cultivate "an 'AI-first' workforce."[108] The DOD also used Anthropic's Claude in the January 2026 attack on Venezuela, and to analyze intelligence and identify targets in the February 2026 strikes on Iran.[109]

The military's reliance on AI has increased its demand for data labeling—the process of curating and categorizing raw data so that AI can be trained to interpret it. Since 2021, the Army has spent more than $100 million on Scale AI's data labeling services.[110] In 2025, a rival start-up, Enabled Intelligence, won a contract with the NGA to undertake its "largest data labeling effort to date."[111] That project, worth up to $700 million, will include services to convert the agency's vast stores of satellite and drone footage into training data for Maven systems.

Demand for online data storage is also expanding. In 2022, the DOD awarded Microsoft, Google, Amazon, and Oracle a multiyear contract to build and operate cloud computing facilities for the military, known as the Joint Warfighting Cloud Capability, or JWCC. The department has already awarded $1 billion under the contract and could spend up to $8 billion more.[112] DOD entities with intelligence missions rely on separate cloud computing infrastructure specially developed to handle data and AI tasks with higher levels of classification on behalf of the Intelligence Community. Contracts for this initiative, known as the Commercial Cloud Enterprise, were awarded in 2020 to the four JWCC contractors and IBM; they are reportedly worth tens of billions of dollars over a 15-year period.[113]

It remains to be seen whether this flurry of dealmaking will lead to meaningful competition in the defense industry, which has consolidated substantially since the 1990s.[114] This consolidation has slowed innovation and left the military vulnerable to supply chain shortages.[115] While tech companies have positioned themselves as disruptors, much of military AI spending so far has flowed to a handful of tech firms. These firms benefit even when their start-up competitors win contracts. Saildrone and Shield AI rely on Palantir for key components of their technology.[116] Anthropic is providing the military access to its foundation model through Palantir's and Amazon's systems.[117] Scale AI recently sold a 49 percent stake to Meta, which also hired Scale AI's CEO to lead its flagship AI lab.[118] These developments raise concerns that the shift to AI-driven warfare may end up replacing one form of market concentration with another.

III. Influence

The tech industry's growing share of the defense budget is the latest chapter in its long and lucrative relationship with the military. Decades before the current AI boom, the DOD was already the "developmental engine" of Silicon Valley, funding technology projects that would prove critical to the growth of today's tech giants.[119] Research it funded to help intelligence agencies better track and organize internet data led to the development of web page ranking and user tracking technologies that underpin Google search,[120] while a 2002 program to streamline military decision-making spurred the creation of Apple's virtual assistant, Siri.[121] Developments like these have propelled a trillion-dollar industry with a powerful role in the economy and politics.

Tech leaders are playing important policymaking roles, as when former Google CEO Eric Schmidt chaired the National Security Commission on Artificial Intelligence,[122] which Congress established in 2018 to advance U.S. leadership in the field. More than 100 of its recommendations were written into law on a bipartisan basis in 2021.[123] Under the second Trump administration, venture capitalist David Sacks was appointed the White House's special adviser for AI and crypto,[124] and Marc Andreessen advised on candidates for defense and intelligence posts.[125] President Trump has broadly aligned with key tech industry interests: He repealed former President Biden's executive order requiring AI companies to disclose safety testing results,[126] he sought to block states from regulating AI technology,[127] and he relaxed export controls on advanced AI chips.[128] The second Trump administration has also held multiple public events with AI industry leaders.[129] The tableau at Trump's second inauguration — at which tech industry leaders sat in the first row, in front of the president's actual cabinet — was a pointed reminder of the industry's ascendance.[130]

Traditional defense contractors continue to attract the lion's share of military contracts and spend more on lobbying, but their upstart AI competitors are asserting greater influence. In 2025, Lockheed Martin spent $11.7 million on lobbying and RTX $10.6 million — slight decreases from what they spent in 2020.[131] Meanwhile, Palantir spent $4.4 million and Anduril $1.7 million that year — about double and triple what each company spent in 2020, respectively.[132] Traditional contractors have spread the manufacturing of major weapons systems across a range of congressional districts, cementing political support.[133] Anduril may be borrowing from this playbook: The California-based company has opened factories in Mississippi and Georgia and announced plans to set up more in Ohio and Rhode Island.[134]

As AI sales to the military grow, Silicon Valley defense firms are likely to have a bigger political footprint. The cryptocurrency industry offers a glimpse into how this could unfold. Fairshake, a pro-crypto super PAC, spent lavishly to help defeat the 2024 reelection bid of Sen. Sherrod Brown (who chaired the Senate Banking Committee and sought stricter oversight of the industry)[135] and the 2024 Senate primary bid of Rep. Katie Porter (who likewise favored stricter regulation).[136] The industry has since capitalized on this influence to push for pro-crypto changes to federal laws and policies.[137] The AI industry is adopting similar tactics. In August 2025, a group of AI investors and companies created Leading the Future, a super PAC modeled after Fairshake, to oppose candidates "looking to slow down AI deployment."[138] This group includes Andreessen, his business partner Ben Horowitz, Lonsdale, OpenAI cofounder Greg Brockman, venture capitalist Ron Conway, and the AI company Perplexity.[139] Meta too has announced plans to launch its own AI-focused super PAC.[140]

Under the second Trump administration, industry proponents of military AI have become more deeply embedded in defense leadership.[141] Michael Obadal, a former senior director at Anduril, was confirmed in September 2025 as undersecretary of the Army; he is responsible for overseeing the service's business operations and acquisition strategy.[142] Obadal has said that he will recuse himself from most matters affecting Anduril's financial interests and forfeit his remaining stock in the company.[143] A few months prior, the Trump administration commissioned four industry leaders — Palantir's Sankar, along with executives from Meta, OpenAI, and Thinking Machines Lab — to serve as lieutenant colonels in a specially created detachment in the Army Reserve.[144] They will help guide the Army's AI strategy and advise soldiers on how to use the technology to enhance lethality and understand battlefield conditions.[145] Although the Army says the executives will not be involved in its contracts with the private sector, their input could lead to greater uptake of their respective companies' technologies.

This new breed of defense tech companies is reaching a turning point that will allow them to play a predictably powerful role in campaign finance and lobbying. But their influence transcends conventional measures of political

spending: Their promotion of AI as the difference between winning and losing war — and of themselves as uniquely qualified to develop and provide the technology — is pervasive in media and policy discourse.[146] This framing has contributed to a push for shortcuts in acquisition and testing alongside growing levels of government investment that the AI tech sector stands to profit immensely from. Privileging speed over caution in this way could sideline still-nascent efforts to understand how AI reshapes the legal and ethical boundaries of war and to mitigate its corresponding risks to life, liberty, and democracy.

IV. Regulatory Gaps

The government must ensure that AI adopted for military applications is effective, fairly priced, and safe in the battlefield. Likewise, it also has a responsibility to ensure that AI tech does not infringe on constitutional and human rights. But today, neither federal law nor executive policy meaningfully addresses the risks of incorporating the technology into warfighting. Instead, relevant legal and policy frameworks are undermined by numerous loopholes that reinforce secrecy and sidestep critical questions, such as how restrictions on foreign intelligence surveillance should be adapted to AI and who bears responsibility for civilian harm traceable to the technology.

A growing chorus of government leaders and tech executives have nevertheless argued that the military is bogged down in excessive regulation and bureaucracy, crippling its ability to deter and win wars.[147] Framing deregulation as a national security imperative, the Pentagon and Congress are rolling back safeguards, increasing the likelihood of fraud, waste, and abuse and risks to soldiers and civilians.

Acquisition

Fears about the United States falling behind in an AI arms race are driving an overhaul of how the military buys software and weapons.[148] In November 2025, the Pentagon launched an effort to "put the entire acquisition system and the industrial base on a wartime footing with the urgency and mandate to accept more risk."[149] A key aspect of this strategy is to slash regulations that are designed to keep costs in check and safeguard taxpayer dollars,[150] even though the Pentagon has lost hundreds of millions of dollars to contractor price gouging on spare parts, software, and other equipment.[151]

Cost and Pricing Disclosures

One regulation on the cutting-room floor is the 1962 Truth in Negotiations Act (TINA), which requires contractors to submit cost and pricing data they certify as "accurate, complete and current" for contracts beyond a certain cost point and absent adequate price competition.[152] Such data may include a detailed breakdown of labor costs, invoices of recent and comparable sales, and published catalog prices.[153] If this data turns out to be old or incorrect, under TINA the government is entitled to remedies for defective pricing, such as price adjustments.[154]

Congress established TINA after a series of revelations that federal contractors, mostly from the defense industry, were overcharging the government.[155] The risk of overcharging is particularly high when the government has few sources of information to corroborate pricing — for example, when the military relies exclusively on a single supplier for certain technologies, equipment, or parts. Certified data requirements in these situations mitigate the risk that the contractor will inflate prices to pad profits.[156]

Critics of these requirements argue that they are well-intentioned but unduly burdensome, leading to unnecessary delays. A common complaint is that expecting contractors to quantify the costs of staff training and software development creates too much paperwork that deters new market entrants.[157] In announcing its new acquisition strategy, the DOD blamed TINA for slowing down government contracts, vowing to reduce its application and leave cost and quality management to the "competitive pressures of the market."[158]

TINA's mandatory disclosures, however, level the playing field when adequate price competition is lacking, ensuring that the government has the same cost and pricing data as the contractor when negotiating the contract. Moreover, TINA simply entitles the government to see costs that contractors track and estimate during the ordinary course of business, and calls for contractors to validate this information — a nonissue for a business operating in good faith. Contractors can also claim reimbursement from the government for personnel and other costs incurred to comply with TINA.[159]

Congress has nevertheless whittled away TINA's requirements to such an extent that the vast majority of Pentagon contracts do not require certified data.[160] It has raised the threshold for mandatory certification from $100,000 per contract (the 1962 threshold) to $10 million in 2025.[161] This makes it easier to break up contracts to avoid providing certified cost and pricing data, as the spare parts supplier TransDigm Inc. did for 95 percent of its contracts between 2017 and 2019 — enabling the company to generate $20.8 million in excess profits.[162] Federal law also now exempts nontraditional defense contractors (i.e., entities that typically do not do business with the military) from certified data requirements.[163]

Commercial Items Exemption

Another loophole that has made certified data requirements the exception rather than the rule is an exemption for contracts for "commercial items."[164] The rationale is that contractors selling to a broad range of consumers and not just the government are subject to price competition, which ostensibly keeps a lid on prices. In the 1990s, however, Congress expanded the commercial item definition to cover technology developed primarily for military purposes as long as the technology can be considered "of a type" customarily used by the general public or in commercial settings.[165]

In other words, Congress extended the commercial exemption to sales of military technology and equipment for which contracting officers have few options to compare and corroborate prices.[166] This change has incentivized overcharging. Defense contractor Honeywell doubled the cost of the Chinook helicopter's engine after its designation as a commercial item.[167] Lockheed Martin and its subcontractors also used this loophole to inflate prices of spare parts for the C-130J military transport aircraft.[168]

Despite these pitfalls, the DOD has applied the commercial exemption to AI-related contracts cumulatively worth hundreds of millions of dollars, including software licenses for Palantir's Maven Smart System and the Navy's purchases of Anduril's autonomous water drones for maritime missions.[169] The Maven Smart System appears to draw on data analytics similar to technology Palantir sells to commercial customers to help them manage their supply chains,[170] and Anduril says its drones are built from off-the-shelf components.[171] But the military requires bespoke features that are rare in the commercial market, such as capabilities to handle classified information or to carry and discharge weapons. This degree of customization limits the usefulness of price comparisons with commercial offerings.

Other Transactions

Secretary Hegseth has ordered the DOD to default to one of two contracting authorities to speed up software acquisition:[172] Commercial Solutions Openings, which treats all products and services acquired under it as "commercial,"[173] and Other Transactions (OT).[174]

OT agreements have become an increasingly popular tool for prototyping AI and other emerging technologies in weapons systems. Congress established this authority as a pilot program in 1989 to encourage partnerships with nontraditional contractors such as universities to prototype new military technologies.[175] It has since expanded the authority to all components of the DOD.[176]

Notable OT agreements in the AI realm include awards totaling up to $800 million for four tech companies to develop military applications of their foundation models[177] and an Army contract worth $22 billion to develop IVAS augmented reality headsets for soldiers.[178] Another active user of OT agreements is the DIU, which oversees the military's flagship effort to mass-produce autonomous drones and has awarded more than 500 such contracts between 2017 and the beginning of 2025.[179] According to the Government Accountability Office (GAO), spending on OT agreements increased from $1.8 billion in 2016 to more than $18 billion in 2024.[180]

The features that make OT agreements attractive to contractors are also susceptible to abuse. These agreements are exempt from many of the oversight requirements that protect the government and taxpayers from fraud and waste, including certified data disclosures. Additionally, contractors are afforded more leeway to retain intellectual property rights in equipment and technology the government has paid them to develop, potentially driving up costs and lengthening repair times downstream.[181]

At the same time, defaulting to OT agreements as the preferred contracting method does little to curb abuses of market power. These agreements are exempt from statutory requirements that promote competition in government contracting[182] on the theory that such agreements are designed to attract nontraditional contractors in the first place.[183] But the majority of OT dollars have gone to defense primes.[184] Though such awards are limited to "nontraditional defense contractors," this term is defined so broadly that the primes and other large contractors frequently qualify.[185]

OT authority also does not address the problem of market concentration in the tech industry, as well-resourced firms such as Microsoft, Google, and Palantir compete for these agreements on the same footing as start-ups.[186] Outsourcing AI and data-intensive capabilities to a handful of large firms risks repeating the same mistakes the Pentagon made with legacy defense systems, many of which suffer from poor performance and equipment shortages because they rely on three suppliers at most.[187]

AI Development and Use

Recognizing the risks posed by military and national security AI, both the first Trump administration and the Biden administration sought to develop processes to ensure efficacy and guardrails to protect privacy, civil liberties, and civil rights. But these efforts have been far from sufficient.

The DOD's Responsible AI Principles

In 2020, under the first Trump administration, the DOD adopted a set of Responsible AI Principles to promote ethical and lawful uses of the technology.[188] While the princi-

ples themselves are not legally binding, the DOD may adopt them as requirements in directives or contracts.[189] They have proved difficult to enforce. In 2021, for example, the DIU synthesized these principles into its own set of Responsible Artificial Intelligence Guidelines and asked vendors to respond to questions in worksheets to assess their compliance with the principles (e.g., methods of preventing model manipulation and evaluating system performance).[190] But a 2022 DIU review found that contractors tend to omit from the worksheets sensitive information or even basic details about how their algorithms work.[191] The review also found that the DOD lacked "appropriate personnel or tools" to assess compliance and is "dependent on vendors to self-monitor."[192] In 2025, the DIU removed the guidelines from its website; it is unclear if they are still being followed.

National Security Memorandum 25

In 2024, the Biden administration built on these principles and a similar effort by the Intelligence Community[193] by issuing a national security memorandum (NSM-25), which outlines a framework for AI governance and risk management in national security.[194] The NSM stems from the 2023 Biden executive order on promoting safe, secure, and trustworthy AI, which Trump has since rescinded.[195] As of this writing, the Trump administration is still considering how to update the NSM.

The NSM applies to all uses of the technology in national security systems except autonomous and semi-autonomous weapons systems, which are governed by a separate set of rules.[196] Under this framework, the NSM seemingly applies to AI systems used to identify targets, but separate rules kick in when those systems are also mobilized to strike targets.[197]

The NSM mandates important risk management measures but provides little in the way of transparency to either the public or Congress on how the DOD will follow these protocols. Covered agencies are required to maintain an inventory of high-impact use cases but are not required to provide this information to Congress or give the public any sense of what these systems are.[198] This means that the DOD's use of AI will remain mostly secret. And, while AI oversight personnel are required to submit annual reports about their work to their agency heads, these reports need only be made available to the public to the "greatest extent practicable."[199] Agencies could employ this discretion to withhold critical information — such as risk management failures — altogether.

Although the NSM lists a handful of prohibited uses, most are narrowly scoped, leaving agencies room to sidestep safeguards. For example, it prohibits using AI to infer an individual's emotional state unless there is a "lawful and justified reason"[200] — a caveat that could be interpreted to permit uses of the technology in combat operations, even though inferring emotional states has been criticized as unreliable and pseudoscientific.[201]

AI use cases that are not prohibited but are nonetheless deemed "high impact" are subject to minimal risk management practices. These include, for example, tracking individuals for military action using just their biometric markers or classifying an individual as a terrorist or national security threat.[202] Risk management practices include impact assessments, testing and evaluation protocols, and mitigation of biases and discrimination through, for example, "appropriate training" for human operators.[203]

However, agencies can obtain waivers for these practices from their chief artificial intelligence officers (CAIOs) not only if compliance would pose "exceptionally grave damage to national security" but also if it would "increase risks to privacy, civil liberties, or safety." It is unclear how practices meant to mitigate these risks could increase such risks. Exemptions are available too if compliance would "create an unacceptable impediment to critical agency operations" — open-ended language that permits expansive discretion. Waivers are limited to one year, but CAIOs may reauthorize them indefinitely.[204] This effectively allows agencies to bypass safeguards on grounds far broader than specific, serious national security concerns.

The data-intensive nature of AI also raises privacy and civil liberties concerns that the NSM does not satisfactorily address. While foundation model developers who sell to the military stress that they only train their models on social media information that has been made public,[205] users may inadvertently disclose information they intend to keep private through their social media networks, or they may fail to keep up with changes to privacy settings.[206] Furthermore, these models could be prompted to draw inferences about the associations and locations of individuals with a social media presence in order to generate a list of potential military targets.[207] The NSM does not clarify how restrictions on foreign intelligence surveillance, particularly those that limit the collection of U.S. person information, should apply to model training or use, instead leaving it to agency discretion.[208]

These pitfalls are exacerbated by the lack of independent mechanisms to verify whether agencies are upholding the NSM's safeguards and rectifying noncompliance. Without mandatory reporting on NSM compliance to Congress or external oversight bodies such as the Privacy and Civil Liberties Oversight Board, agencies are effectively left to regulate themselves. The NSM is also silent on how agencies should remedy AI-facilitated harms to rights and safety, depriving people who are directly affected a meaningful opportunity to challenge or seek redress for such harms. And in general, civilian victims of U.S. military actions have little recourse and are forced to rely on an ad hoc system of compensation.[209] This lack of accountability can have life-or-death consequences: In

the absence of an independent process for investigating how AI-generated intelligence might contribute to lethal errors in targeting, for example, the military risks replicating those errors in future operations.

Autonomous and Semiautonomous Weapons

The DOD is fielding weapons systems that increasingly rely on AI, robotics, and related technologies to strike targets with limited human involvement. It has recognized that these systems should be subject to heightened rules, given that misfires and other failures can lead to accidental killings and other harms.[210] To "minimize the probability and consequences" of these failures, the department in 2012 established its first-ever policy directive on the "development and use of autonomous and semiautonomous functions in weapon systems," known as Department of Defense Directive 3000.09.[211] The DOD updated the directive in 2023, in part to respond to AI-driven advances in weapons autonomy.[212] Nevertheless, the policy continues to raise troubling questions about how the military mitigates the risks of AI in warfare.

Senior Review

Directive 3000.09 defines an autonomous weapons system as one that, once activated, can "select and engage targets without further intervention by an operator" (e.g., drones programmed to identify and fire on military installations without requiring operator confirmation between identification and firing).[213] In contrast, a semiautonomous system is "intended to only engage individual targets or specific target groups that *have been selected by an operator*" (e.g., drones that require operator confirmation between identification and firing).[214]

The directive does not prohibit the development and fielding of autonomous weapons systems. Instead, it requires senior DOD leaders, before development, to review whether a system's design "incorporates the necessary capabilities to allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[215] According to the Congressional Research Service, this standard does not rule out weapons lacking human-in-the-loop oversight; instead, it refers to "broader human involvement in decisions about how, when, where, and why the weapon will be employed."[216] Subsequently, before fielding the weapon, senior leaders must also verify that it can be used in accordance with the laws of war.[217]

The criteria for senior review, however, do not specify the circumstances under which autonomous weapons systems foreclose human judgment to such a degree that their deployment would conflict with the laws of war, such as the prohibition against the use of weapons that are indiscriminate by nature.[218] Battlefield conditions may cause these weapons to act in unpredictable ways — for example, by launching strikes on civilian infrastructure that is partially obscured by previous damage or poor lighting and therefore misconstrued as military targets.[219] Biases and other blind spots in training data may exacerbate these errors.[220] These failures are complicated by the black box nature of many autonomous systems, meaning that they may generate outputs that even their developers and operators struggle to understand.[221] It is critical that the directive specify minimum levels of human oversight between identification of a target and firing, particularly so that operators can correct a system's misidentification of civilian objects as military objects or its failure to prevent excessive civilian harm.[222]

The directive also authorizes the exemption of autonomous systems from senior review if the system is used to apply "non-lethal, non-kinetic force against materiel targets"[223] (e.g., directed energy weapons used to disable enemy equipment)[224] or if there is "urgent military need" (an undefined standard).[225] In 2019, the DOD disclosed that no weapons system had ever been required to undergo senior review.[226] In 2023, it declined to confirm whether this was still the case, saying that it could not comment on "individual weapons systems."[227] In 2025, Congress began requiring the department to report waivers of the directive to the congressional defense committees, including descriptions of weapons systems covered, rationales, and duration.[228] While this does not clarify or limit the scope of waivers, it at least provides a measure of transparency.

Civilian Harm

Amendments to other risk mitigation protocols appear to expand the military's tolerance for civilian harm, particularly as its leaders push to accelerate the speed of battlefield decision-making in tandem with maximizing lethality.[229] The 2012 directive required testing to "ensure" that systems were sufficiently robust to minimize failures such as "unintended engagements" with civilians,[230] whereas the 2023 directive requires only that testing "provide sufficient confidence," without specifying how this standard should be satisfied.[231] The 2012 directive also defines "unintended engagements" as the "use of force *resulting in damage* to persons or objects" that are not intended to be targets,[232] whereas the 2023 directive defines them as the "use of force against [such] persons or objects."[233] The DOD explained that this change was to clarify — not narrow — the definition.[234] Human rights experts argue, however, that the revision could allow the military to overlook civilian harm incidental to engagement with intended targets.[235]

The directive is also silent on who will be held accountable — and how — when autonomous or semiautonomous weapons systems inflict collateral damage that violates the laws of war.[236] The complex interaction between the limits of machine reasoning and human cognition requires guidance on how to apportion responsibility between operators, commanders, and commercial developers. While the DOD has a framework for investigations into civilian harm during combat operations, it does not address the role of AI-facilitated decision-making.[237] Further guidance is unlikely under the Trump administration, which has curtailed efforts across the Pentagon to mitigate civilian harm.[238]

Testing

The administration's sweeping cuts to the DOD workforce that oversees weapons testing will also impair compliance with Directive 3000.09. Secretary Hegseth halved the number of staff at the Office of the Director of Operational Test and Evaluation (DOT&E), which oversees testing of the military's major weapons systems, and ended all contractor support for the office.[239] DOT&E currently oversees 268 weapons systems — some of which have extensive AI integration, such as the Air Force's Advanced Battle Management System.[240] These cuts will make it harder for DOT&E to verify whether DOD components and their vendors are meaningfully evaluating the performance of their weapons systems and adopting appropriate mitigations.[241]

Like other weapons systems, AI-enhanced systems face complications in the battlefield that their developers may fail to anticipate. AI-powered drones that U.S. start-ups sent to the front lines of the Ukraine war, for example, have struggled to travel their advertised ranges or carry enough munitions or cargo.[242] Their operating software has also been susceptible to jamming techniques, including GPS blackouts.[243]

Testing in live-fire ranges that realistically simulate battlefield conditions ensures that the military and its contractors can make needed fixes in controlled settings, minimizing the risk of misfires, crashes, and other failures in combat. During an exercise off the coast of California, the Navy struggled to coordinate and maneuver drone boats made by BlackSea Technologies using Anduril's Lattice autonomy software, prompting a safety standdown.[244] This incident revealed problems aligning software systems created by two different contractors that Anduril said it was later able to fix.[245] Along with crashes of the company's drones in separate Army and Air Force tests, the incident also prompted Anduril to acknowledge the importance of testing that "catch[es] issues in controlled settings rather than in the field."[246]

One of the military's most expensive experiments with emerging technology illustrates another peril of subpar testing: ballooning costs. In 2021, the Army awarded a contract to Microsoft worth up to $22 billion to develop the IVAS augmented reality headset for soldiers.[247] In 2022, the DOD inspector general's audit found that program officials had not defined basic metrics for testing whether soldiers would be comfortable using the headset in the battlefield.[248] Rep. Robert Wittman revealed in a 2023 hearing that the headset "left the majority of soldiers reporting at least one physical impairment."[249] The program had at that point already cost around $1.5 billion,[250] and the Army has yet to select an effective prototype. Anduril, which had previously been tapped to integrate its AI data analytics platform into IVAS,[251] took over the program as lead contractor in 2025.[252]

AI failures in the battlefield are likely to increase unless Congress, the White House, and the DOD institute robust and enforceable guardrails on how the military acquires and uses the technology — and on how to ensure its safety and reliability. Efforts to streamline the defense acquisition process have weakened agency oversight over how contractors substantiate software prices while loosening testing and evaluation standards. Both the DOD and the White House have introduced AI-specific safeguards, but they fail to establish clear standards for the most pressing risks, including hidden biases in identifying targets and the lack of human involvement in autonomous weapons operation.[253]

V. Dangers

Determining how AI can usefully augment existing military functions requires thorough evaluation of the benefits and risks, testing in as close to real-world conditions as possible, meaningful oversight by military leaders and lawmakers, and sufficient transparency on matters of public interest — including patterns of misuse or failure. Prioritizing acquisition and adoption over guardrails could waste hundreds of millions in taxpayer dollars, arm the military with technology poorly equipped to address emerging threats, and endanger the safety and lives of soldiers and civilians alike. It could also lead to technical vulnerabilities that compromise performance and harm national security.[254]

Questionable Accuracy and Effectiveness

Persistent problems that have surfaced with AI's performance in military systems suggest that the technology may sometimes work better in laboratory settings than in real-world conditions. Key defense AI programs have suffered from high inaccuracy rates, paving the way for faulty intelligence that draws soldiers into unintended engagements or informs the mistaken targeting of civilians. For example, Bloomberg reported in 2024 that the capabilities for identifying military targets developed under Maven were only able to correctly identify a tank about 60 percent of the time in near-perfect conditions; with snow falling, accuracy plummeted to 30 percent.[255] In comparison, soldiers identified a tank accurately 84 percent of the time.[256] Air Force testing of a target recognition system in 2021 found that it was only able to correctly detect missile threats 25 percent of the time.[257] The system's accuracy broke down because it was fed sensor footage shot from a perspective different from the one it was trained on.[258]

AI can perpetuate harmful biases as well, such as when it generates images that disproportionately depict incarcerated persons, drug dealers, and terrorists as darker-skinned,[259] or when chatbot responses associate protected characteristics like gay, Black, and Muslim with anger and other negative sentiments.[260] These biases are discriminatory and harmful on their own, but they can also compromise national security: Using AI technology to create composite sketches of targets or to scour social media for security threats, for example, may produce flawed military intelligence that misidentifies innocent individuals or groups as threats while overlooking genuine indicators of illicit activity.[261]

Although the accuracy of these systems may improve with technological advances, better training data and techniques, and more rigorous testing, these problems demonstrate the inherent limitations and risks of AI. Image and video recognition technology — the bedrock of AI-based targeting systems — can be trained to perform nearly perfectly on high-quality footage, but they are more error-prone with grainy, obscured, or poorly lit images.[262] Large language models, which power intelligence-gathering tools that parse social media posts and other texts for clues about adversaries' behavior and potential threats, may misinterpret linguistic nuances (like sarcasm or parody) or overlook them (if a threat is veiled in coded language), particularly when analyzing languages other than English.[263]

Incorporating human involvement in the use of these systems — such as by giving commanders the authority to override AI-generated targets — may not be sufficient to mitigate errors. Human operators of AI systems are vulnerable to automation bias: the tendency to defer to automated outputs because operators perceive them to be more objective or rational than their own judgment.[264] Complex conflict environments can exacerbate this bias because they place commanders under immense pressure to act quickly, often with incomplete or contradictory information.[265]

These problems have come under intense scrutiny in Gaza, where the Israel Defense Forces (IDF) has acknowledged that it uses "modern data technologies" to surface potential targets for strikes from vast repositories of data it collects about Gazans.[266] According to press reports, one such tool, code-named Lavender, assigns people a score indicating how likely they are to be members of an armed group.[267] This form of predictive analysis risks flagging individuals based on unreliable proxies for suspicious activity, such as whether they are part of chat groups with other individuals who are under suspicion, or how frequently they change phone numbers or addresses.[268] To triangulate the locations of suspected militants, the IDF uses an AI system code-named Gospel to compare and analyze phone intercepts, cell phone location data, satellite footage, social networks, and other intelligence sources.[269]

The IDF has stressed that its analysts verify intelligence generated using these tools against other information sources.[270] But multiple media investigations have found that these checks are unevenly applied. Some analysts, for

example, relied only on one piece of human-derived intelligence to validate Lavender's recommendations instead of the customary two,[271] while others accepted recommendations without corroboration.[272] Inaccuracies in targeting have been compounded by underestimates of civilians in the vicinity of planned strikes.[273] These problems have raised alarm about the extent to which the IDF's methods have contributed to the high civilian death toll in Gaza.[274]

The risks of using predictive analytics in battlefield decision-making predate recent advances in AI. A U.S. intelligence program code-named SKYNET, which used AI to flag terrorism suspects from cell phone location information and other metadata collected in Pakistan, misidentified a journalist as a member of al-Qaeda because he made regular press trips to regions with known terrorist activity.[275] The U.S. government placed the journalist on a watch list of suspected terrorists.[276] This inaccuracy triggered questions about the extent to which the government relied on predictive analytics such as SKYNET to commission drone strikes,[277] particularly those that target people based on patterns of suspicious behavior without verifying their identities.[278]

Dehumanization

More fundamentally, like older forms of automation, the growing reliance on AI also makes acts of killing and destruction more abstract, potentially desensitizing military personnel to the likelihood of civilian casualties.

AI-facilitated targeting reduces people to a series of data points and turns acts of killing and destruction into a sterile and procedural task.[279] This machine-induced detachment from the moral and ethical implications of war may foster a lax or inconsistent application of safeguards to mitigate collateral harm. Former President Barack Obama acknowledged that the "machinery" of targeted killings under his watch had "started becoming too easy," giving drone operators the "illusion that it is not war."[280]

Pre-AI forms of automated warfare are instructive. Unsealed Pentagon records show, for example, that drone operators referred to imminent strikes as "play time" and to people fleeing the aftermath as "squirters."[281] This form of dehumanization coincided with rises in surveillance and intelligence lapses that led to the killing of civilians and the destruction of civilian homes and infrastructure.[282]

The Triple Black Box

The acquisition and use of military AI raises pressing questions about its effectiveness and potential for harm, yet these systems are shrouded in secrecy. Some information — including that which may reveal intelligence sources and methods — may be too sensitive for disclosure. But the military should disclose basic details about how AI systems are used, whether they have been adequately tested and proved, and the role of contractors. One way to do so would be through unclassified summaries of its use case inventories. These disclosures would go a long way toward building public trust in how the military is using a technology that many Americans already seriously doubt will be developed and used responsibly.[283]

Legal scholar and former White House associate counsel Ashley Deeks has warned that "adding black box AI into the existing black box of national security" produces a "double black box" and risks creating a doom loop of secrecy and abuse.[284] Courts almost never examine the conduct of war or covert action and surveillance.[285] Congress has few incentives to challenge the executive branch's actions in these spheres and often lacks the resources, information, and expertise to meaningfully scrutinize military operations and intelligence practices.[286] This dearth of democratic checks and balances has normalized illegal and unconstitutional action, from the bulk surveillance programs revealed by Edward Snowden to the CIA's torture of terrorism suspects.[287] AI introduces unpredictable machine-human interactions and new errors that amplify these challenges, making national security decision-making even harder to decipher and explain — and confounding efforts to hold those decision-makers accountable.[288]

Relying on proprietary AI for military activities risks expanding this double black box into a triple one. Obscure contracting relationships make it difficult to understand the AI vendor ecosystem, the prevalence of corruption and abuse, and whether public funds are being spent effectively. Public procurement databases provide basic transaction information about military AI contracts but offer few details about a contract's purpose or progress, let alone any insight into whether vendors have failed to meet the contract's specifications or deliver a viable product (or the consequences of such failures).[289] Moreover, arrangements to buy government technology through resellers do not consistently disclose the entities that originally developed the technology.[290] Classified contracts are also not included in these databases. Further complicating matters, the government sometimes removes contracts from these databases, making them hard to track. Between 2024 and 2025, for example, the Pentagon removed contracts for drone and satellite surveillance[291] and an intelligence-sharing system.[292]

The ongoing effort to fast-track AI acquisition amplifies the emphasis on secrecy. The DOD grants about half of OT agreements — the contracting vehicle it favors when prototyping emerging technologies — to groups of companies that work together to bid for large government

contracts.[293] Palantir and Anduril are reportedly creating such a consortium with other tech companies.[294] The GAO concluded that this form of contracting limits both Congress's and taxpayers' ability to understand "which consortia have received awards and the extent to which the DOD is investing in various technology areas using consortia-based OT agreements."[295] These arrangements sometimes fail to disclose all consortium partners or how awards are apportioned,[296] further obscuring companies' roles in critical military operations.

The government's limited right to access and disclose proprietary information about how vendors develop the AI it buys creates additional hurdles to oversight. Law enforcement and intelligence vendors have invoked intellectual property law and confidentiality agreements to compel agencies to withhold information about how their technologies are implicated in surveilling individuals or initiating investigations.[297] Public disclosure laws such as the Freedom of Information Act (FOIA) also establish broad exemptions for trade secrets and commercial information, making it difficult to obtain even basic information about how vendors program AI systems to make predictions and recommendations on behalf of the government.[298]

When vendors retain ownership of key elements of AI systems developed for the military or otherwise limit access to information about those elements, the military's ability to test or secure them may be undermined.[299] The decision early on in the F-35 fighter jet program to delegate maintenance to Lockheed Martin, the manufacturer, has made it difficult for the Pentagon to oversee repairs and control costs.[300] Ceding testing and maintenance of critical software to vendors risks creating similar dependencies, effectively paving the way for them to self-regulate and make risk determinations without meaningful military input or awareness.

This ceding of control may already be underway. A September 2025 Army memo detailed "critical deficiencies" in an AI-enabled battlefield communications system developed by Palantir, Anduril, Microsoft, and other contractors that make it vulnerable to "insider threats, external attacks, and data spillage."[301] The memo traced these vulnerabilities to the "black box" nature of the system, which prevented the Army from controlling what users are able to do or see. The Army says that these issues were "mitigated immediately." The integration of commercial foundation models into battle networks compounds the risk of issues like these arising. Adversaries could exploit weak points in these models' training and development pipelines — which exist outside the military's cybersecurity infrastructure — to undermine model performance and introduce security vulnerabilities.[302]

The DOD's reliance on one of its large language model vendors, Scale AI, to develop a testing and evaluation framework for military applications of the models also suggests that the department is deferring to the private sector on critical questions of accountability and evaluation of AI risks.[303] Furthermore, industry leaders have urged the DOD to permit "more mature vendors" to self-certify that their software has undergone sufficient testing and due diligence.[304] This raises the prospect that the DOD will allow Scale and other AI companies to oversee testing and inspections on key aspects of systems they provide to the military — similar to the self-regulation the Federal Aviation Administration permitted Boeing to do for the past 15 years, which experts believe played a role in the design flaws that led to two fatal plane crashes, in 2018 and 2019.[305]

The military's adoption of AI systems without adequate guardrails not only raises the risk of fraud, waste, and abuse but also leaves soldiers and civilians vulnerable to harm. Opaque procurement practices coupled with national security secrecy mean that the American public is usually the last to know when these systems are abused or fail — if they are ever informed at all.

VI. Recommendations

The military must balance the demands of speedy AI adoption with safe and effective deployment that upholds constitutional rights and international law and is subject to meaningful oversight. Regulation that upholds these principles is not antithetical to innovation. In fact, it would promote trust within the military and among the public about how AI is developed and deployed in ways that could encourage its adoption.

White House

>> Close loopholes in the national security memorandum on AI.

The White House's ongoing review of NSM-25 on AI presents an opportunity to bolster common-sense measures to ensure that the technology — particularly in connection with "high-impact" uses — is adopted and deployed in working order; is tested, proved, and documented; and does not infringe on constitutional or human rights. These measures include risk and impact assessments, test and evaluation protocols, bias mitigation safeguards, and training for human operators.

The NSM was meant to align with parallel regulations issued by the Office of Management and Budget (OMB) that govern non–national security uses of AI.[306] It is, however, weaker in several respects and should more closely track the latter. For example, while the OMB memo requires impact assessments to be supported by "specific metrics and qualitative analysis," these measures are optional under the NSM.[307] In other words, DOD components that opt out of providing evidence may be able to deploy risky and unproven technology in battlefield without rigorous justification of its utility. Waivers of these safeguards should only be granted for *specific* and *serious* national security concerns, for a maximum of one year, with a concrete plan for bringing the AI system into compliance. The NSM's transparency requirements should also be strengthened. They should, for example, require agencies to release unclassified summaries describing high-impact AI systems, links to relevant procurement records, and information on how risk management practices were implemented.[308]

Department of Defense

>> Strengthen testing of AI systems.

Rather than cut staff and spending at its main testing and evaluation arm,[309] the department should expand DOT&E's capacity to perform operational and live-fire testing across a broader range of AI-related programs, including autonomous and semiautonomous weapons programs.[310] The DOD should also ensure that the DOT&E remains independent and continues to publicly release annual unclassified reports on the results of its weapons testing.[311] And the department should leverage its existing contracting authorities to negotiate data rights to commercial systems that enable it to conduct meaningful auditing and risk monitoring.[312]

Congress

>> Codify AI safeguards.

Congress should codify and improve on the NSM's risk management framework. The Artificial Intelligence Weapons Accountability and Risk Evaluation (AWARE) Act, introduced by Sen. Peter Welch, would require the DOD to submit annual risk assessment reports.[313] It provides a starting point that lawmakers should build on to enact comprehensive safeguards.

The leaders of the House and Senate Armed Services Committees should also request that the GAO identify and review policies, directives, and other measures implemented by the DOD to protect privacy, civil rights, and civil liberties when acquiring, developing, and using AI systems, including compliance with the NSM. Additionally, lawmakers should establish a commission with civil society representation to study the privacy, security, and safety risks of intermingling commercial and military applications of foundation models and whether developing military-exclusive models would minimize these risks.[314]

>> Establish privacy protections.

Strong privacy protections provide another critical buffer against AI's potential for harm. Congress should examine how it can adapt laws governing the collection, analysis, and retention of private communications and other data, such as the Foreign Intelligence Surveillance Act, to address the privacy risks of training, developing, and using AI in national security systems.

Growing partnerships between the tech sector and the military also necessitate restrictions on the transfer of

personal data collected for advertising and other commercial purposes to the military for AI-based surveillance and targeting. A policy framework established by the Office of the Director of National Intelligence (ODNI) on how agencies should handle commercially available information recognizes that the government's acquisition and use of such data puts people's privacy and civil liberties at risk.[315] But the framework does not prohibit purchases of information that would otherwise be subject to statutory or constitutional protections, instead relying on discretionary standards that could easily turn into a box-checking exercise.[316]

ODNI's policy is no substitute for legislation — such as the bipartisan Fourth Amendment Is Not For Sale Act — that would prohibit government agencies from purchasing constitutionally or statutorily protected personal information.[317] Additionally, Congress should pass a comprehensive consumer privacy law restricting companies' collection, processing, and transfer of personal information.[318] These restrictions would not only reduce the scope of consumer data available for military use but also mitigate the risk that this information ends up in the hands of adversaries.

>> Tighten guardrails on autonomy in weapons systems.

Congress should urgently investigate the DOD's use of autonomous and semi-autonomous weapons systems; specify how their development and fielding should enable "appropriate levels of human judgment over the use of force," per DOD Directive 3000.09, in a manner consistent with the laws of war; and identify the types of systems that fail to meet this standard and therefore should be prohibited.

Congress should mandate the DOD to modify Directive 3000.09 to limit exceptions to the senior review process for fully autonomous systems based on "urgent military need," requiring that these exceptions be time-bound and limited to genuine emergencies, such as when review would cause delays that pose an imminent threat to military personnel. It should also evaluate whether to extend the process to certain classes of semiautonomous systems.

>> Strengthen pricing transparency and oversight.

Fortifying the defense acquisition process against attempts to weaken accountability and oversight is also an urgent priority.[319] Congress should lower the mandatory disclosure threshold for certified cost and pricing data to $750,000, narrow the definition of commercial items and services, and support legislation to promote competitive bidding and accountability in pricing.[320]

>> Build capacity to monitor and respond to AI risks.

To oversee AI's impact on warfighting, Congress requires independent, in-house expertise that can help legislators ask the right questions and unpack highly technical issues. Over the past several decades, budget cuts to congressional support agencies — including the elimination of the Office of Technology Assessment — have forced lawmakers to rely on industry groups and experts with a vested interest in how Congress regulates AI.[321] Building capacity for evidence-based oversight requires dedicated staffing and resources, such as the creation of a science and technology hub staffed with experts to help lawmakers make sense of technical jargon, outside research, and different viewpoints.[322]

>> Adopt campaign finance reforms.

The Brennan Center has long advocated for reforms to curb corporate and billionaire influence on policy decisions that affect their bottom lines. Congress should close long-standing loopholes in campaign finance and lobbying restrictions and establish conflict-of-interest rules that reduce the risk of major donors using money to gain access and sway policy decisions over defense matters implicating their own financial interests.[323]

Conclusion

In his farewell address to the nation, President Dwight Eisenhower recognized the importance of the military working closely with industry to safeguard national security. But he also stressed the risks of this partnership:

> In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist.[324]

The business of military AI — with its complexity and dangers both well-documented and yet unknown — makes it all the more important to heed Eisenhower's warning. The stakes could not be higher.

Appendix

TABLE A

Notable Contracts: Palantir

PURPOSE	PROCUREMENT INSTRUMENT IDENTIFIER	EFFECTIVE DATE	AGENCY	OBLIGATED (MILLIONS OF DOLLARS)	CEILING (MILLIONS OF DOLLARS)
Provide commercial software solutions, including MSS licenses[325]	W519TC25D0039	July 2025	U.S. Army	71	10,000
Expand MSS access to the Army, Air Force, Space Force, Navy, and U.S. Marine Corps[326]	W911QX24D0026	September 2024	U.S. Army Combat Capabilities Development Command (DEVCOM)	71	100
Develop MSS for AI-facilitated targeting and logistics and to enable CJADC2[327]	W911QX24D0012	June 2024	U.S. Army/ Chief Digital and Artificial Intelligence Office (CDAO)	293	1,275
Continue to support software capabilities[328]	H9243323D0001	June 2023	U.S. Special Operations Command (USSOCOM)	Unknown	463
Integrate Gotham, Palantir's "AI-powered kill chain," into USSOCOM's mission command system[329]	H924042190002	May 2021	U.S. Army/ USSOCOM	112	117
Purchase licenses for Gotham[330]	H9222216C0078	December 2016	U.S. Air Force/ USSOCOM	276	278
Provide Navy with access to Gotham[331]	N0003920F0110	February 2020	U.S. Navy	19	84
"Examine data and develop algorithms" for Secure Unclassified Network system, the military's platform for sharing sensitive intelligence and other information with other federal agencies and foreign allies[332]	W911QX19C0039	December 2019	Defense Information Systems Agency (DISA)	73	484
Develop and operate the Army Vantage platform, the Army's flagship data-sharing and analytics platform that facilitates combat logistics and readiness[333]	W15QKN209P001	December 2019	U.S. Army	550	571

Continued on next page

Continued from previous page

Create the Space C2 Data Platform[334]	FA880625FB009	May 2025	U.S. Space Force	32	359
Manage response to the Covid-19 pandemic[335]	70Z02320FPLM02200	April 2020	U.S. Coast Guard	8	8
Purchase data fusion and analytics services for DHS's investigative case management system[336]	70CTD022FR0000170	September 2022	DHS/Immigration and Customs Enforcement	139	159

TABLE B

Notable Contracts: Anduril

PURPOSE	PROCUREMENT INSTRUMENT IDENTIFIER	EFFECTIVE DATE	AGENCY	OBLIGATED (MILLIONS OF DOLLARS)	CEILING (MILLIONS OF DOLLARS)
Provide air defense capabilities — including Anvil and Roadrunner drone and missile interceptors and Pulsar drone- and IED-jamming tools — that use the AI-based Lattice operating system to identify targets[337]	H9240222D0001	January 2022	USSOCOM	906	968
Develop the Integrated Visual Augmentation System[338]	W91CRB219P002	April 2025	U.S. Army	139[339]	22,000
Provide AI-powered Counter-Small Unmanned Aircraft Systems (software and strategies to counter enemy drones and other unmanned systems, known also as C-sUAS)[340]	M6785425D0003	March 2025	U.S. Navy	54.5	2,500
Produce loitering munitions and supporting hardware[341]	N0016425CJR94	February 2025	U.S. Navy	94	94
Scale Lattice Mesh (a software capability to decentralize access to data) across multiple services and combatant commands[342]	HQ08832590001	December 2024	DOD/CDAO	33	33
Develop autonomous underwater vehicles equipped with Lattice[343]	HQ08452490015	December 2023	DOD	138	171
Integrate Lattice into the military's space surveillance network[344]	FA882321C0002	July 2021	U.S. Air Force	34	34
Provide autonomous surveillance towers that use Lattice to identify objects[345]	70B02C20D00000019	July 2020	DHS/ U.S. Customs and Border Protection	862	2,000

TABLE C

Notable Contracts in Growth Areas

PURPOSE	CONTRACTOR	PROCUREMENT INSTRUMENT IDENTIFIER	EFFECTIVE DATE	AGENCY	OBLIGATED (MILLIONS OF DOLLARS)	CEILING (MILLIONS OF DOLLARS)
Drones and counter-drone technology						
Purchase Voyager drones to conduct maritime intelligence and surveillance[346]	Saildrone	HQ08452290030	September 2022	DOD	33	54
Test and develop uncrewed surface vessels to complete essential Navy missions[347]	Saildrone	N000142492005	August 2024	U.S. Army	30	30
Develop V-BAT autonomous drone prototype for maritime missions[348]	Shield AI	N004212190022	September 2021	U.S. Navy	72	72
Integrate Hivemind into the Navy's subsonic aerial target drone platform[349]	Shield AI	N000192490020	August 2024	U.S. Navy	11	11
Deploy AI-piloted V-BAT drones for maritime intelligence, surveillance, and reconnaissance[350]	Shield AI	70Z02324D93130001	June 2024	U.S. Coast Guard	22	229
Develop autonomy software for ground vehicles[351]	Applied Intuition	W15QKN2395025	October 2022	U.S. Army/ Defense Innovation Unit	21	46
Develop autonomy software for drones as part of the DOD's Replicator initiative[352]	Applied Intuition	HQ08832490001	September 2024	CDAO	20	171
Data services						
Label data to support "geospatial intelligence, artificial intelligence and machine learning capabilities," including the NGA Maven program[353]	Enabled Intelligence	—	November 2025	National Geospatial-Intelligence Agency	–	708
Test and evaluate large language models[354]	Scale AI	SP470124D0004	September 2024	Defense Logistics Agency	5	50
Label training data for artificial intelligence and machine learning[355]	Scale AI	W911QX20C0051	September 2020	U.S. Army	106	110

TABLE D

DOD AI and AI-Related Budget Requests

FISCAL YEAR	AI (MILLIONS OF DOLLARS)	AI-RELATED (MILLIONS OF DOLLARS)	AUTONOMY (MILLIONS OF DOLLARS)
2020[356]	927	–	3,700
2021[357]	871	789 (cloud computing)	1,700
2022[358]	874	–	–
2023[359]	1,100	–	–
2024[360]	1,800	1,400 (CJADC2)	–
2025[361]	1,800	1,400 (CJADC2)	–
2026[362]	–	200 (audit automation)	13,400

TABLE E

Second Trump Administration Appointments from the Defense Tech Industry and Leading Investment Firms

NAME	APPOINTMENT	POSITION PRIOR TO APPOINTMENT
Dan Caine[363]	Joint Chiefs of Staff chairman	Venture partner, Shield Capital
Stephen Feinberg[364]	Deputy secretary of defense	CEO, Cerberus Capital Management
Jacob Helberg[365]	Undersecretary of state for economic growth, energy, and the environment	Senior adviser, Palantir
Michael Kratsios[366]	Office of Science and Technology Policy (OSTP) director	Managing director, Scale AI
Sriram Krishnan[367]	OSTP senior policy adviser for AI	Partner, A16z
Scott Kupor[368]	Office of Personnel Management director	Partner, A16z
Michael Obadal[369]	Undersecretary of the Army	Senior director, Anduril
David Sacks[370]	White House AI and crypto czar	Partner, Craft Ventures

Endnotes

1 Geneva Academy of International Humanitarian Law and Human Rights, "War Watch," accessed December 1, 2025, https://warwatch.ch/explore [https://perma.cc/G6UY-5WYU]; and Madison Schramm, "Great Power Competition: Hastening America's Decline?," Henry L. Stimson Center, August 27, 2024, https://www.stimson.org/2024/great-power-competition-hastening-americas-decline.

2 Theresa Hitchens, "AI 'Unchained': NGA's Maven Tool 'Significantly' Decreasing Time to Targeting, Agency Chief Says," *Breaking Defense,* May 22, 2025, https://breakingdefense.com/2025/05/ai-unchained-ngas-maven-tool-significantly-decreasing-time-to-targeting-agency-chief-says.

3 Defense Innovation Unit (DIU), "Replicator," accessed December 1, 2025, https://web.archive.org/web/20260302143028/https://www.diu.mil/replicator.

4 Shyam Sankar, "The Defense Reformation," Palantir Technologies, October 31, 2024, https://www.18theses.com.

5 Pete Hegseth (secretary of defense) to senior Pentagon leadership, commanders of the combatant commands, and defense agency and DOW field activity directors, Re: Transforming the Defense Acquisition System into the Warfighting Acquisition System to Accelerate Fielding of Urgently Needed Capabilities to Our Warriors, November 7, 2025, https://media.defense.gov/2025/Nov/10/2003819439/-1/-1/1/TRANSFORMING-THE-DEFENSE-ACQUISITION-SYSTEM-INTO-THE-WARFIGHTING-ACQUISITION-SYSTEM-TO-ACCELERATE-FIELDING-OF-URGENTLY-NEEDED-CAPABILITIES-TO-OUR-WARRIORS.PDF.

6 Julia Gledhill, "What You Need to Know About Pentagon and Military-Related Spending in H.R. 1," Henry L. Stimson Center, October 23, 2025, https://www.stimson.org/2025/what-you-need-to-know-about-pentagon-and-military-related-spending-in-h-r-1.

7 Heather Somerville and Brett Forrest, "How American Drones Failed to Turn the Tide in Ukraine," *Wall Street Journal*, April 10, 2024, https://www.wsj.com/world/how-american-drones-failed-to-turn-the-tide-in-ukraine-b0ebbac3.

8 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; and Sheera Frenkel and Natan Odenheimer, "Israel's A.I. Experiments in Gaza War Raise Ethical Concerns," *New York Times*, April 25, 2025, https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html.

9 Sheera Frenkel, "Israel Deploys Expansive Facial Recognition Program in Gaza," *New York Times*, March 27, 2024, https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html.

10 U.S. Department of Defense (DOD), *Department of Defense 2018 Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*, February 14, 2019, 3, https://stratml.us/pdfs/DODAIS.pdf.

11 See DOD, "Transcript: Background Briefing on FY 2026 Defense Budget," June 26, 2025, https://www.defense.gov/News/Transcripts/Transcript/Article/4228828/background-briefing-on-fy-2026-defense-budget. Table D in this report's appendix outlines the department's AI, AI-related, and autonomy budget requests between fiscal years 2020 and 2025 and how the relevant budget categories have evolved during this period.

12 Billy Mitchell, "Air Force Selects AI-Enabled Predictive Maintenance Program as System of Record," *DefenseScoop*, May 10, 2023, https://defensescoop.com/2023/05/10/air-force-selects-ai-enabled-predictive-maintenance-program-as-system-of-record.

13 Beth Reece, "DLA Applying AI to Supply Chain Risk Management, Warfighter Readiness," Defense Logistics Agency, March 13, 2025, https://www.dla.mil/About-DLA/News/News-Article-View/Article/4117309/dla-applying-ai-to-supply-chain-risk-management-warfighter-readiness.

14 See, e.g., David Vergun, "AI Could Speed Background Investigations," DOD, April 8, 2019, https://www.defense.gov/News/News-Stories/Article/Article/1808113/ai-could-speed-background-investigations (on using AI to speed up security clearances); Matthew Olay, "Senior Special Ops Leader Highlights AI's Usefulness Beyond Battlefield," DOD, June 3, 2025, https://www.defense.gov/News/News-Stories/Article/Article/4205349/senior-special-ops-leader-highlights-ais-usefulness-beyond-battlefield (on using AI to plan budgets); and Devon Bistarkey, "AI-Powered Agile Talent Identification Systems Supports Joint Force," DOD, July 25, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3849739/ai-powered-agile-talent-identification-systems-supports-joint-force (on using AI to match candidates with short-term assignments).

15 John R. Hoehn and Nishawn S. Smagh, "Intelligence, Surveillance, and Reconnaissance Design for Great Power Competition," Congressional Research Service, June 4, 2020, 2, https://www.congress.gov/crs_external_products/R/PDF/R46389/R46389.3.pdf.

16 Elliot Jones, "What Is a Foundation Model?," Ada Lovelace Institute, July 17, 2023, https://www.adalovelaceinstitute.org/resource/foundation-models-explainer.

17 See Chief Digital and Artificial Intelligence Office (CDAO), "Task Force Lima: Executive Summary," December 2024, https://www.ai.mil/Portals/137/Documents/Resources%20Page/2024-12-TF%20Lima-ExecSum-TAB-A.pdf; and James O'Donnell, "Phase Two of Military AI Has Arrived," *MIT Technology Review*, April 15, 2025, https://www.technologyreview.com/2025/04/15/1115078/phase-two-of-military-ai-has-arrived.

18 Government Accountability Office (GAO), *Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems*, February 2022, 17, https://www.gao.gov/assets/gao-22-104765.pdf.

19 DIU, "Replicator."

20 Kelley M. Sayler, "Army's Integrated Visual Augmentation System (IVAS): Background and Issues for Congress," Congressional Research Service, September 11, 2025, https://www.congress.gov/crs-product/IF13022.

21 Ashley Roque, "Anduril Gets Green Light from Army to Take Over Microsoft's IVAS Project: Exec," *Breaking Defense*, April 15, 2025, https://breakingdefense.com/2025/04/anduril-gets-green-light-from-army-to-take-over-microsofts-ivas-project-exec.

22 U.S. Army Public Affairs, "U.S. Army Awards Enterprise Service Agreement to Enhance Military Readiness and Drive Operational Efficiency," July 31, 2025, https://www.army.mil/article/287506/u_s_army_awards_enterprise_service_agreement_to_enhance_military_readiness_and_drive_operational_efficiency.

23 John A. Tirpak, "USAF Plans $28.48 Billion over 5 Years to Develop New Advanced Fighters, Drone Escorts," *Air & Space Forces Magazine*, March 16, 2024, https://www.airandspaceforces.com/usaf-2025-ngad-cca-five-year-budget.

24 Sen. Kevin Cramer, "Senate Passes President Trump's One Big Beautiful Bill Act, Advancing Agenda for a Strong, Prosperous America," news release, July 1, 2025, https://www.cramer.senate.gov/news/press-releases/senate-passes-president-trumps-one-big-beautiful-bill-act-advancing-agenda-for-a-strong-prosperous-america; and Mike Stone and Marisa Taylor, "Exclusive: Musk's SpaceX Is Frontrunner to Build Trump's Golden Dome Missile Shield,"

Reuters, April 17, 2025, https://www.reuters.com/business/aerospace-defense/musks-spacex-is-frontrunner-build-trumps-golden-dome-missile-shield-2025-04-17.

25 DOD, "Contracts for Dec. 7, 2022," accessed February 5, 2026, https://www.defense.gov/News/Contracts/Contract/Article/3239197/contracts-for-dec-7-2022.

26 Frank Konkel, "CIA Awards Secret Multibillion-Dollar Cloud Contract," *Nextgov/FCW*, November 20, 2020, https://www.nextgov.com/modernization/2020/11/exclusive-cia-awards-secret-multibillion-dollar-cloud-contract/170227.

27 Matthew Olay, "Senior Officials Outline President's Proposed FY26 Defense Budget," DOD, June 26, 2025, https://www.defense.gov/News/News-Stories/Article/Article/4227847/senior-officials-outline-presidents-proposed-fy26-defense-budget.

28 Peter Hegseth to senior Pentagon leadership, commanders of the combatant commands, and defense agency and DOD field activity directors, Re: Artificial Intelligence Strategy for the Department of War, January 9, 2026, https://media.defense.gov/2026/Jan/12/2003855671/-1/-1/0/ARTIFICIAL-INTELLIGENCE-STRATEGY-FOR-THE-DEPARTMENT-OF-WAR.PDF.

29 For example, the National Security Agency, the National Reconnaissance Office, the Defense Intelligence Agency, and the National Geospatial-Intelligence Agency all run AI programs.

30 Frank Bajak, "Pentagon's AI Initiatives Accelerate Hard Decisions on Lethal Autonomous Weapons," Associated Press, November 25, 2023, https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942.

31 Robert Work (deputy secretary of defense) to secretaries of the military departments et al., Re: Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven), April 26, 2017, https://nsarchive.gwu.edu/document/18583-national-security-archive-department-defense.

32 Jack Poulson, "Easy as PAI (Publicly Available Information)," Tech Inquiry, September 10, 2021, 1, 19, https://web.archive.org/web/20250630091658/https://techinquiry.org/EasyAsPAI/resources/EasyAsPAI.pdf; and Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html. After facing intense public scrutiny, Google ultimately decided not to renew its Project Maven contract in 2018. The DOD subsequently shielded key details about Google's involvement from public disclosure. See Sam Biddle, "Pentagon Says All of Google's Work on Drones Is Exempt from the Freedom of Information Act," *Intercept*, March 25, 2019, https://theintercept.com/2019/03/25/google-project-maven-pentagon-foia.

33 Katrina Manson, "US Used AI to Help Find Middle East Targets for Airstrikes," Bloomberg, February 26, 2024, https://www.bloomberg.com/news/articles/2024-02-26/us-says-it-used-ai-to-help-find-targets-it-hit-in-iraq-syria-and-yemen; and David E. Sanger, "In Ukraine, New American Technology Won the Day. Until It Was Overwhelmed," *New York Times*, April 25, 2024, https://www.nytimes.com/2024/04/23/us/politics/ukraine-new-american-technology.html.

34 Defense Acquisition University, "Program of Record (POR)," accessed February 4, 2026, https://www.dau.edu/acquipedia-article/program-record-por; and Jaspreet Gill, "Now That Maven Is a Program of Record, NGA Looks at LLMs, Data Labeling," *Breaking Defense*, November 16, 2023, https://breakingdefense.com/2023/11/now-that-maven-is-a-program-of-record-nga-looks-at-llms-data-labeling.

35 Poulson, "Easy as PAI," 24–26; and Katrina Manson, "AI Warfare is Already Here," Bloomberg Businessweek, February 28, 2024, https://www.bloomberg.com/features/2024-ai-warfare-project-maven.

36 The National Geospatial-Intelligence Agency reportedly splits responsibilities for Maven with the CDAO, which develops Maven-related capabilities outside geospatial intelligence, and the Office of the Undersecretary of Defense for Intelligence and Security, which performs oversight. See Brandi Vincent, "Amid a High-Stakes Transition, Questions Linger About Project Maven's Future Management," *DefenseScoop*, September 9, 2022, https://defensescoop.com/2022/09/09/amid-a-high-stakes-transition-project-mavens-future-management-remains-unclear.

37 Palantir Technologies, "Maven Smart System: The Foundational AI-Enabled Software Platform for CJADC2," 2025, https://assets.ctfassets.net/xrfr7uokpv1b/25muZs93DY5XOUBtuh68yn/b40d9784f69917219f972890ceede986/Maven_One_Pager.pdf; and Hitchens, "AI 'Unchained.'"

38 Joseph P. Lyddane, "138th Field Artillery Brigade Incorporates Artificial Intelligence," Defense Visual Information Distribution Service, February 29, 2024, https://www.dvidshub.net/news/464998/138th-field-artillery-brigade-incorporates-artificial-intelligence; and Emelia S. Probasco, *Building the Tech Coalition: How Project Maven and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense*, Center for Security and Emerging Technology, August 2024, 3–4, https://cset.georgetown.edu/wp-content/uploads/CSET-Building-the-Tech-Coalition-1.pdf.

39 United States Air Force Academy, "Combatant Commands Research Guide," McDermott Library, accessed January 27, 2026, https://usafa.libguides.com/combatantcommands/overview.

40 Brandi Vincent, "'Growing Demand' Sparks DOD to Raise Palantir's Maven Contract to More than $1B," *DefenseScoop*, May 23, 2025, https://defensescoop.com/202480000005/05/23/dod-palantir-maven-smart-system-contract-increase.

41 Vincent, "'Growing Demand' Sparks DOD to Raise Palantir's Maven Contract."

42 John R. Hoehn et al., "Defense Primer: What Is Command and Control?," Congressional Research Service, November 29, 2021, https://www.congress.gov/crs_external_products/IF/PDF/IF11805/IF11805.2.pdf.

43 Jon Harper, "Pentagon Getting Ready to Onboard New Vendors and Applications for CJADC2 Tech," *DefenseScoop*, May 31, 2024, https://defensescoop.com/2024/05/31/pentagon-onboard-new-vendors-cjadc2-tech-palantir-open-digar.

44 Nishawn S. Smagh, "Defense Capabilities: Joint All Domain Command and Control," Congressional Research Service, April 6, 2020, https://www.congress.gov/crs_external_products/IF/PDF/IF11493/IF11493.1.pdf.

45 John R. Hoehn, "Joint All-Domain Command and Control (JADC2)," Congressional Research Service, January 21, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11493/14.

46 Peter Hegseth to senior Pentagon leadership, Re: Army Transformation and Acquisition Reform, April 30, 2025, 1–2, https://media.defense.gov/2025/May/01/2003702281/-1/-1/1/ARMY-TRANSFORMATION-AND-ACQUISITION-REFORM.PDF (directing the secretary of the army to "enable AI-driven command and control at Theater, Corps, and Division headquarters by 2027").

47 Sayler, "Army's Integrated Visual Augmentation System."

48 Frederick Shear, "IVAS' Campaign of Learning Ensures Development, Production and Fielding Remain on Track," U.S. Army, March 14, 2023, https://www.army.mil/article/264773/ivas_campaign_of_learning_ensures_development_production_and_fielding_remain_on_track.

49 Jon Harper, "Anduril Integrates AI Tech into Army IVAS Headsets," *DefenseScoop*, September 19, 2024, https://defensescoop.com/2024/09/19/ivas-anduril-microsoft-lattice-integration-army.

50 Jennifer DiMascio, "U.S. Air Force Collaborative Combat Aircraft (CCA)," Congressional Research Service, November 28, 2025, https://crsreports.congress.gov/product/pdf/IF/IF12740.

51 Gregory C. Allen and Isaac Goldston, *The Department of Defense's Collaborative Combat Aircraft Program: Good News, Bad News, and Unanswered Questions*, Center for Strategic and International Studies, August 6, 2024, https://www.csis.org/analysis/department-defenses-collaborative-combat-aircraft-program-good-news-bad-news-and.

52 DIU, "Replicator"; and Savannah Wooten, *Deadly and Imminent: The Pentagon's Mad Dash for Silicon Valley's AI Weapons*, Public Citizen, November 22, 2024, https://www.citizen.org/article/deadly-and-imminent-report.

53 See DIU, "Who We Are/Our Mission," accessed December 1, 2025, https://www.diu.mil/about; and DOD, "CDAO and DIU Launch New Effort Focused on Accelerating DOD Adoption of AI Capabilities," news release, December 11, 2024, https://www.defense.gov/News/Releases/Release/Article/3996199/cdao-and-diu-launch-new-effort-focused-on-accelerating-dod-adoption-of-ai-capab.

54 Shelby Holiday et al., "U.S. Military Is Struggling to Deploy AI Weapons," *Wall Street Journal*, September 26, 2025, https://www.wsj.com/politics/national-security/pentagon-ai-weapons-delay-0f560d7e.

55 DIU, "DIU and DAWG Launch Autonomous Vehicle Orchestrator Prize Challenge," January 13, 2026, https://www.diu.mil/latest/diu-and-dawg-launch-autonomous-vehicle-orchestrator-prize-challenge.

56 Katrina Manson, "OpenAI Tapped for Voice Control Tech in US Drone Swarm Trial," Bloomberg, February 13, 2026, https://www.bloomberg.com/news/articles/2026-02-13/openai-tapped-for-voice-control-tech-in-us-drone-swarm-challenge.

57 Dan Sabbagh, "'It Is Impossible to Outrun Them': How Drones Transformed War in Ukraine," *Guardian*, January 4, 2025, https://www.theguardian.com/world/2025/jan/04/it-is-impossible-to-outrun-them-how-drones-transformed-war-in-ukraine. See also Marc Santora et al., "A Thousand Snipers in the Sky: The New War in Ukraine," *New York Times*, March 3, 2025, https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html.

58 Hegseth to senior Pentagon leadership, Re: Army Transformation and Acquisition Reform, 1. General James Rainey, the commanding general of Army Futures Command, estimated that the Army currently employs 90 percent crewed aircraft and 10 percent unmanned aircraft, and said that it hopes to flip that percentage over the coming years. Chris Panella, "What the US Army Is Flying Is Around 90% Crewed, 10% Drone. Leaders Want to Flip That," *Business Insider*, July 3, 2025, https://www.businessinsider.com/us-army-sec-general-flying-crewed-uncrewed-2025-7.

59 CDAO, "CDAO Announces Partnerships with Frontier AI Companies to Address National Security Mission Areas," news release, July 14, 2025, https://www.ai.mil/Latest/News-Press/PR-View/Article/4242822/cdao-announces-partnerships-with-frontier-ai-companies-to-address-national-secu [https://perma.cc/Y8F8-LUHE].

60 CDAO, "Artificial Intelligence Rapid Capabilities Cell," December 11, 2024, https://www.ai.mil/Portals/137/Documents/Resources%20Page/2024-12-CDAO-Artificial-Intelligence-Rapid-Capabilities-Cell.pdf [https://perma.cc/6P3X-LNS9].

61 Dave Lawler and Maria Curi, "Musk's xAI and Pentagon Reach Deal to Use Grok in Classified Systems," Axios, February 23, 2026, https://www.axios.com/2026/02/23/ai-defense-department-deal-musk-xai-grok.

62 Amrith Ramkumar et al., "Pentagon Used Anthropic's Claude in Maduro Venezuela Raid," *Wall Street Journal*, February 15, 2026, https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17; and Sheera Frenkel and Julian E. Barnes, "Defense Dept. and Anthropic Square Off in Dispute Over A.I. Safety," *New York Times*, February 18, 2026, https://www.nytimes.com/2026/02/18/technology/defense-department-anthropic-ai-safety.html.

63 Hegseth to senior Pentagon leadership et al., Re: Artificial Intelligence Strategy for the Department of War, 3.

64 AI tools enable the government to piece together discrete and seemingly unconnected data points about individuals to expose their locations, movements, associations, and habits at scale, undermining a central aim of the Fourth Amendment "to place obstacles in the way of a too permeating police surveillance." *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (citing *United States v. Di Re*, 332 U.S. 581, 595 (1948)) (holding that the government's warrantless acquisition of "deeply revealing" location information violates the Fourth Amendment).

65 See, e.g., Neil Davison, "A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law," *United Nations Office of Disarmament Affairs Occasional Papers*, no. 30 (November 2017): 5–18, https://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf.

66 See, e.g., DOD and Deloitte Consulting LLP, delivery order, FA487718F0258, August 31, 2018, https://www.usaspending.gov/award/CONT_AWD_FA487718F0258_9700_GS00Q14OADU113_4732 [https://perma.cc/ZLG6-VAMF] (DOD contract with commercial data broker Venntel); DOD and Systems & Technology Research LLC, definitive contract, FA865016C1830, September 23, 2016, https://www.usaspending.gov/award/CONT_AWD_FA865016C1830_9700_-NONE-_-NONE- [https://perma.cc/7RCU-S5YL] (DOD contract with commercial data broker X-Mode Social); Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020, https://www.vice.com/en/article/us-military-location-data-xmode-locate-x (explaining how the DOD purchases location data from X-Mode); and Joseph Cox, "How an ICE Contractor Tracks Phones Around the World," *Vice*, December 3, 2020, https://www.vice.com/en/article/ice-dhs-fbi-location-data-venntel-apps (explaining how government agencies purchase sensitive information from Venntel). See also Charlie Savage, "N.S.A. Buys Americans' Internet Data Without Warrants, Letter Says," *New York Times*, January 25, 2024, https://www.nytimes.com/2024/01/25/us/politics/nsa-internet-privacy-warrant.html.

67 See Emile Ayoub and Elizabeth Goitein, "Closing the Data Broker Loophole," Brennan Center for Justice, February 13, 2024, https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole; and Joseph Cox, "Homeland Security Uses AI Tool to Analyze Social Media of U.S. Citizens and Refugees," *Vice*, May 17, 2023, https://www.vice.com/en/article/dhs-uses-ai-tool-babel-x-babel-street-social-media-citizens-refugees.

68 Office of the Director of National Intelligence Senior Advisory Group, Panel on Commercially Available Information, *Report to the Director of National Intelligence*, January 27, 2022, https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf. See also Cox, "Homeland Security Uses AI Tool to Analyze Social Media."

69 Ayoub and Goitein, "Closing the Data Broker Loophole." The DOD's Defense Intelligence Agency has argued that Fourth Amendment protections do not apply when the government purchases information like location data for intelligence purposes. See Defense Intelligence Agency, "Clarification of Information Briefed During DIA's 1 December Briefing on CTD," January 15, 2021, https://int.nyt.com/data/documenttools/dni-to-wyden-on-commercially-available-smartphone-locational-data/5d9f9186c07993b6/full.pdf.

70 Jai Vipra and Sarah Myers West, "Computational Power and AI," AI Now Institute, September 27, 2023, https://ainowinstitute.org/

publication/policy/compute-and-ai.

71 DOD, *DoD Cloud Strategy*, December 2018, 1, https://media.defense.gov/2019/feb/04/2002085866/-1/-1/1/dod-cloud-strategy.pdf.

72 DOD, *DoD Cloud Strategy*, 1.

73 DOD, "Contracts for Dec. 7, 2022."

74 See, e.g., Courtney Albon, "Space Force Awards ULA, SpaceX $1 Billion for Seven Launches," *Air & Space Forces Magazine*, October 3, 2025, https://www.airandspaceforces.com/space-force-awards-ula-spacex-1-billion-for-seven-launches.

75 See, e.g., Silicon Valley Defense Group, "SVDG NatSec100 2025 Edition," accessed December 1, 2025, https://natsec100.org; Andreessen Horowitz, "American Dynamism," accessed December 1, 2025, https://a16z.com/american-dynamism; Founders Fund, "Portfolio," accessed December 1, 2025, https://foundersfund.com/portfolio; and Lizette Chapman, "The 10 Defense Tech Startups to Watch in 2025," Bloomberg, January 16, 2025, https://www.bloomberg.com/features/2025-tech-defense-startups-to-watch.

76 Palantir Technologies, "Palantir Reports Q3 2025 U.S. Comm Revenue Growth of 121% Y/Y and Revenue Growth of 63% Y/Y; Guides Q4 Revenue to 61% Y/Y and U.S. Comm Revenue to 121% Y/Y; Raises FY 2025 Revenue Guidance to 53% Y/Y, Crushing Consensus Expectations," news release, November 3, 2025, https://investors.palantir.com/news-details/2025/Palantir-Reports-Q3-2025-U-S--Comm-Revenue-Growth-of-121-YY-and-Revenue-Growth-of-63-YY-Guides-Q4-Revenue-to-61-YY-and-U-S--Comm-Revenue-to-121-YY-Raises-FY-2025-Revenue-Guidance-to-53-YY-Crushing-Consensus-Expectations; and Jessica E. Lessin, "'We'll Double Revenue This Year': Anduril's CEO on Growth, Shutdowns and Space War," *The Information*, October 3, 2025, https://www.theinformation.com/articles/double-revenue-year-andurils-ceo-growth-shutdowns-space-war.

77 CNBC, "Palantir Technologies Inc," accessed February 6, 2026, https://www.cnbc.com/quotes/PLTR [https://perma.cc/4ZTM-PWL3]; and Jason Ma, "SpaceX and Palantir Now Have Bigger Valuations than Top Aerospace-Defense Stocks as the Military Eyes Transformation," *Fortune*, December 7, 2024, https://fortune.com/2024/12/07/spacex-palantir-valuation-market-cap-pentagon-contractor-rtx-lockheed-boeing-northrop.

78 Kate Clark and Becky Peterson, "Thrive Capital, A16Z to Lead Anduril Investment at $60 Billion Valuation," Wall Street Journal, March 3, 2026, https://www.wsj.com/business/entrepreneurship/thrive-capital-a16z-to-lead-anduril-investment-at-60-billion-valuation-2de8922e?st=aSy71N; and Ari Levy, "Anduril Raises Funding at $30.5 Billion Valuation in Round Led by Founders Fund, Chairman Says," CNBC, June 5, 2025, https://www.cnbc.com/2025/06/05/anduril-valuation-founders-fund.html.

79 Andy Greenberg, "How a 'Deviant' Philosopher Built Palantir, a CIA-Funded Data-Mining Juggernaut," *Forbes*, August 14, 2013, https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut.

80 Greenberg, "How a 'Deviant' Philosopher Built Palantir"; and The Lord of the Rings Wiki, "Palantíri Usage," accessed December 1, 2025, https://lotr.fandom.com/wiki/Palant%C3%ADri.

81 Palantir Technologies, "Board of Directors," accessed December 1, 2025, https://investors.palantir.com/governance/board-of-directors.

82 Palantir Technologies, "About Palantir: Answers to Frequently Asked Questions About Palantir," *Palantir Blog*, August 21, 2025, https://blog.palantir.com/about-palantir-ddddb78aec29.

83 Palantir Technologies, "Palantir Foundry: The Ontology-Powered Operating System for the Modern Enterprise," accessed December 1, 2025, https://www.palantir.com/platforms/foundry. See also U.S. Securities and Exchange Commission, Form 10-K for Palantir Technologies Inc., Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 for the Fiscal Year Ended December 31, 2024, 4, https://investors.palantir.com/files/2024%20FY%20PLTR%2010-K.pdf (stating that key Palantir platforms "enable institutions to transform massive amounts of information into an integrated data asset that reflects their operations").

84 Palantir Technologies, "Gotham," accessed December 1, 2025, https://www.palantir.com/platforms/gotham. See also Imke Stock, "Missing Link: Power Center Palantir — a Software Controls Organization," Heise Online, June 29, 2025, https://www.heise.de/en/background/Missing-link-Power-center-Palantir-a-software-controls-organizations-10463503.html; and #Hash, "The Problem with Palantir," April 2, 2025, https://hash.ai/blog/the-problem-with-palantir.

85 For list of key contracts with each branch, see table A in this report's appendix.

86 U.S. Army Public Affairs, "U.S. Army Awards Enterprise Service Agreement to Enhance Military Readiness."

87 Aaron Mehta, "Palantir Wins Contract for Army TITAN Next-Gen Targeting System," *Breaking Defense*, March 6, 2024, https://breakingdefense.com/2024/03/palantir-wins-contract-for-army-titan-next-gen-targeting-system; and Lizette Chapman et al., "Silicon Valley Is Coming for the Pentagon's $1 Trillion Budget," Bloomberg, May 8, 2025, https://www.bloomberg.com/graphics/2025-silicon-valley-targets-pentagon-budget (describing Titan as a mobile command post that integrates multiple data streams to identify unmanned weapons and provide real-time assessments on the battlefield). The Brennan Center was unable to locate a public procurement record for the Titan contract.

88 See Vincent, "'Growing Demand' Sparks DOD to Raise Palantir's Maven Contract." See also table A in this report's appendix.

89 Jason Koebler, "Inside a Powerful Database ICE Uses to Identify and Deport People," *404 Media*, April 9, 2025, https://www.404media.co/inside-a-powerful-database-ice-uses-to-identify-and-deport-people.

90 See, e.g., Brennan Center for Justice, "Brennan Center for Justice v. New York Police Department," August 6, 2021, https://www.brennancenter.org/our-work/court-cases/brennan-center-justice-v-new-york-police-department; and Mary Pat Dwyer, "LAPD Documents Reveal Use of Social Media Monitoring Tools," Brennan Center for Justice, September 8, 2021, https://www.brennancenter.org/our-work/analysis-opinion/lapd-documents-reveal-use-social-media-monitoring-tools.

91 Steven Levy, "Inside Palmer Luckey's Bid to Build a Border Wall," *Wired*, June 11, 2018, https://www.wired.com/story/palmer-luckey-anduril-border-wall.

92 Jeremy Stern, "American Vulcan," *Tablet*, accessed December 1, 2025, https://www.tabletmag.com/feature/american-vulcan-palmer-luckey-anduril.

93 Levy, "Inside Palmer Luckey's Bid to Build a Border Wall"; and U.S. Customs and Border Protection, "CBP's Autonomous Surveillance Towers Declared a Program of Record Along the Southwest Border," news release, July 2, 2020, https://www.cbp.gov/newsroom/national-media-release/cbp-s-autonomous-surveillance-towers-declared-program-record-along.

94 Anduril Industries, "President Biden Demanded 'High-Tech Capacity' for Border Security. Anduril's Towers Are Delivering It," *Anduril Blog*, September 16, 2021, https://blog.anduril.com/president-biden-demanded-high-tech-capacity-for-border-security-805b7b5664b5.

95 Anduril Industries, "Mission Autonomy," accessed December 1, 2025, https://www.anduril.com/mission-autonomy.

96 This figure reflects the total cost that USAspending.gov recorded for the relevant DHS contract as of January 22, 2026. See DHS and

Anduril Industries Inc., indefinite delivery/indefinite quantity contract, 70B02C20D00000019, July 2, 2020, https://www.usaspending.gov/award/CONT_IDV_70B02C20D00000019_7014 [https://perma.cc/82WR-QFEZ]. See also Anduril Industries, "Anduril Deploys 300th Autonomous Surveillance Tower (AST), Advancing Capability for Border Security," September 25, 2024, https://www.anduril.com/article/anduril-deploys-300th-autonomous-surveillance-tower-ast-advancing-capability-for-border-security.

97 See table B in this report's appendix.

98 DiMascio, "U.S. Air Force Collaborative Combat Aircraft"; and Jason Levin, "Anduril's YFQ-44A Begins Flight Testing for the Collaborative Combat Aircraft Program," Anduril Industries, October 30, 2025, https://www.anduril.com/article/anduril-yfq-44a-begins-flight-testing-for-the-collaborative-combat-aircraft-program.

99 Brandi Vincent, "Army Moves to Rapidly Field Anduril's Ghost-X Drones via Replicator," *DefenseScoop*, October 17, 2024, https://defensescoop.com/2024/10/17/replicator-ghost-x-drones-anduril-army; and Courtney Albon, "Pentagon Picks Programmers to Connect Its Replicator Drone Swarms," *Defense News*, November 20, 2024, https://www.defensenews.com/pentagon/2024/11/20/pentagon-picks-programmers-to-connect-its-replicator-drone-swarms.

100 Theresa Hitchens, "Anduril Could Receive up to $100M for Space Surveillance Network Upgrade," *Breaking Defense*, November 21, 2024, https://breakingdefense.com/2024/11/anduril-could-receive-up-to-100m-for-space-surveillance-network-upgrade.

101 Roque, "Anduril Gets Green Light from Army to Take Over Microsoft's IVAS Project."

102 Mark Sullivan, "Meet the VC Trying to Reintroduce the Pentagon to Silicon Valley," *Fast Company*, November 5, 2021, https://www.fastcompany.com/90692208/josh-wolfe-lux-capital-vc-pentagon-silicon-valley-defense-tech. According to Crunchbase, 8VC has participated in 28 funding rounds in start-ups coded as "military" and "national security" in its database; A16z has participated in 26 rounds, Founders Fund in 22 rounds, and Lux Capital in 16 rounds. In comparison, Lockheed Martin Ventures, the venture capital arm of Lockheed Martin, has participated in 3 rounds, though many of its other investments not coded as such are in technologies that have potential military applications. See also Chris Metinko, "A16z and Founders Fund Lead the Way in Defense Venture Capital," Crunchbase News, August 20, 2024, https://news.crunchbase.com/venture/a16z-founders-fund-lead-defense-vc-anduril-helsing.

103 See table C in this report's appendix; and Saildrone, "Saildrone Overcomes Denied and Spoofing Environments to Expand Middle East Ops," March 25, 2025, https://www.saildrone.com/news/saildrone-overcomes-denied-and-spoofing-environments-to-expand-middle-east-ops. According to Crunchbase, Lux Capital has led more funding rounds (five) for Saildrone than any other VC firm.

104 See table C in this report's appendix; Shield AI, "Shield AI Awarded Contract to Integrate Hivemind AI Pilot onto Eighth Aircraft: The Kratos BQM-177A," news release, August 19, 2024, https://shield.ai/shield-ai-awarded-contract-to-integrate-hivemind-ai-pilot-onto-eighth-aircraft-the-kratos-bqm-177a; and Shield AI, "Shield AI's V-BAT Selected for $198 Million Contract to Provide U.S. Coast Guard with Maritime Unmanned Aircraft System Services," news release, July 1, 2024, https://shield.ai/shield-ais-v-bat-selected-for-198-million-contract-to-provide-u-s-coast-guard-with-maritime-unmanned-aircraft-system-services. According to Crunchbase, A16z has led more funding rounds (six) for Shield AI than any other VC firm.

105 See table C in this report's appendix; and Applied Intuition Defense, "Army Selects Applied Intuition to Accelerate Autonomy Development for Robotic Combat Vehicle (RCV)," November 14, 2022, https://www.appliedintuitiondefense.com/blog/army-selects-applied-intuition-for-robotic-combat-vehicle. According to Crunchbase, Lux Capital has led more funding rounds (seven) for Applied Intuition than any other VC firm.

106 CDAO, "CDAO Announces Partnerships with Frontier AI Companies."

107 DIU, "DIU's Thunderforge Project to Integrate Commercial AI-Powered Decision-Making for Operational and Theater-Level Planning," March 5, 2025, https://www.diu.mil/latest/dius-thunderforge-project-to-integrate-commercial-ai-powered-decision-making [https://perma.cc/9VK8-TTUF]. According to Crunchbase, Y Combinator has led the highest number of funding rounds (five) for Scale AI.

108 CDAO, "The War Department Unleashes AI on New GenAI.mil Platform," news release, December 9, 2025, https://www.ai.mil/Latest/News-Press/PR-View/Article/4355177/the-war-department-unleashes-ai-on-new-genaimil-platform.

109 Reed Albergotti, "Palantir Partnership Is at Heart of Anthropic, Pentagon Rift," Semafor, February 17, 2026, https://www.semafor.com/article/02/17/2026/palantir-partnership-is-at-heart-of-anthropic-pentagon-rift; and Marcus Weisgerber et al., "U.S. Strikes in Middle East Use Anthropic, Hours After Trump Ban," *Wall Street Journal*, February 28, 2026, https://www.wsj.com/livecoverage/iran-strikes-2026/card/u-s-strikes-in-middle-east-use-anthropic-hours-after-trump-ban-ozNO0iCIZpfpL7K7EIJ2.

110 USAspending.gov, "Keyword Search W911QX20C0051," accessed December 1, 2025, https://www.usaspending.gov/keyword_search/W911QX20C0051 [https://perma.cc/FCL4-NC6X]; and Scale AI, "Data Labeling: The Authoritative Guide," accessed December 1, 2025, https://scale.com/guides/data-labeling-annotation-guide.

111 Katrina Manson, "Scale AI Loses to Smaller Startup in Bid for US Intel Work," Bloomberg, November 24, 2025, https://www.bloomberg.com/news/articles/2025-11-24/scale-ai-loses-to-smaller-upstart-in-bid-for-us-intel-work; and National Geospatial-Intelligence Agency (NGA), "NGA Announces $708M Data Labeling RFP," news release, September 30, 2024, https://www.nga.mil/news/NGA_announces_$708M_data_labeling_RFP.html.

112 Jon Harper, "Pentagon Awards Nearly $1B in JWCC Task Orders," *DefenseScoop*, August 7, 2024, https://defensescoop.com/2024/08/07/pentagon-awards-nearly-1b-jwcc-task-orders. The Pentagon is reportedly seeking to expand its cloud computing access in its upcoming JWCC Next contract. Jon Harper, "Pentagon Officials Gearing Up for JWCC Next Enterprise Cloud Program Solicitation," *DefenseScoop*, August 7, 2025, https://defensescoop.com/2025/08/07/jwcc-next-enterprise-cloud-program-dod-solicitation-plans.

113 Billy Mitchell, "CIA Quietly Awards C2E Cloud Contract Possibly Worth Billions," *FedScoop*, November 20, 2020, https://fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract.

114 DOD, *State of Competition Within the Defense Industrial Base*, Office of the Under Secretary of Defense for Acquisition and Sustainment, February 2022, https://media.defense.gov/2022/feb/15/2002939087/-1/-1/1/state-of-competition-within-the-defense-industrial-base.pdf.

115 DOD, *State of Competition Within the Defense Industrial Base*.

116 Justin Katz, "Saildrone, Palantir Partner to Use AI to Streamline USV Manufacturing, Operations," *Breaking Defense*, March 13, 2025, https://breakingdefense.com/2025/03/saildrone-palantir-partner-to-use-ai-to-streamline-usv-manufacturing-operations; and Shield AI, "Shield AI and Palantir Technologies Deepen Strategic Partnership and Announce Deployment of Warp Speed," news release, December 5, 2024, https://shield.ai/shield-ai-and-palantir-technologies-deepen-strategic-partnership-and-announce-deployment-of-warp-speed.

117 Palantir Technologies, "Anthropic and Palantir Partner to Bring Claude AI Models to AWS for U.S. Government Intelligence and Defense Operations," Business Wire, November 7, 2024, https://www.businesswire.com/news/home/20241107699415/en/Anthropic-

and-Palantir-Partner-to-Bring-Claude-AI-Models-to-AWS-for-U.S.-Government-Intelligence-and-Defense-Operations.

118 Janakiram MSV, "Meta Invests $14 Billion in Scale AI to Strengthen Model Training," *Forbes*, June 23, 2025, https://www.forbes.com/sites/janakirammsv/2025/06/23/meta-invests-14-billion-in-scale-ai-to-strengthen-model-training.

119 Jeannette Estruth, "The Real Developmental Engine," *Drift*, February 22, 2023, https://www.thedriftmag.com/the-real-developmental-engine.

120 Jeff Nesbit, "Google's True Origin Partly Lies in CIA and NSA Research Grants for Mass Surveillance," *Quartz*, January 28, 2025, https://qz.com/1145669/googles-true-origin-partly-lies-in-cia-and-nsa-research-grants-for-mass-surveillance.

121 Defense Advanced Research Projects Agency, "Innovation Timeline," accessed December 1, 2025, https://www.darpa.mil/about/innovation-timeline.

122 National Security Commission on Artificial Intelligence (NSCAI), *Final Report: National Security Commission on Artificial Intelligence*, March 2021, https://assets.foleon.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf; and Kate Conger and Cade Metz, "'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive," *New York Times*, November 3, 2021, https://www.nytimes.com/2020/05/02/technology/eric-schmidt-pentagon-google.html.

123 See Bipartisan Artificial Intelligence Task Force, *Bipartisan House Task Force Report on Artificial Intelligence*, 118th Congress, December 2024, 40, https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf.

124 David Warrington (counsel to the president) to David O. Sacks (special adviser for AI and crypto), Re: Limited Waiver Pursuant to 18 U.S.C. § 208(b)(1) Regarding A.I. Assets, June 2025, https://www.whitehouse.gov/wp-content/uploads/2025/06/David-Sacks.pdf.

125 Cat Zakrzewski and Jacqueline Alemany, "Elon Musk Isn't the Only Tech Leader Helping Shape the Trump Administration," *Washington Post*, January 13, 2025, https://www.washingtonpost.com/politics/2025/01/13/andreessen-tech-industry-trump-administration-doge.

126 Initial Rescissions of Harmful Executive Orders, Exec. Order No. 14148, 90 Fed. Reg. 8237 (January 20, 2025), https://www.govinfo.gov/app/details/FR-2025-01-28/2025-01901.

127 Ensuring a National Policy Framework for Artificial Intelligence, Exec. Order No. 14365, 90 Fed. Reg. 58499 (December 11, 2025), https://www.govinfo.gov/app/details/FR-2025-12-16/2025-23092.

128 Steve Kopack, "Trump Says He Will Allow Nvidia to Sell Some AI Chips in China," NBC News, December 8, 2025, https://www.nbcnews.com/business/corporations/trump-nvidia-h200-chips-ai-china-rcna248107.

129 See, e.g., The White House, "President Trump, Tech Leaders Unite to Power American AI Dominance," September 5, 2025, https://www.whitehouse.gov/articles/2025/09/president-trump-tech-leaders-unite-american-ai-dominance; and Cecilia Kang and Cade Metz, "Trump Announces $100 Billion A.I. Initiative," *New York Times*, January 21, 2025, https://www.nytimes.com/2025/01/21/technology/trump-openai-stargate-artificial-intelligence.html.

130 Edward Helmore, "Trump Inauguration: Zuckerberg, Bezos and Musk Seated in Front of Cabinet Picks," *Guardian*, January 20, 2025, https://www.theguardian.com/us-news/2025/jan/20/trump-inauguration-tech-executives.

131 OpenSecrets, "Client Profile: Lockheed Martin," accessed January 22, 2026, https://www.opensecrets.org/federal-lobbying/clients/summary?id=D000000104; and OpenSecrets, "Client Profile: RTX Corp," accessed January 22, 2026, https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2025&id=D000072615.

132 OpenSecrets, "Client Profile: Palantir Technologies," accessed January 22, 2026, https://www.opensecrets.org/federal-lobbying/clients/summary?id=D000055177; and OpenSecrets, "Client Profile: Anduril Industries," accessed January 22, 2026, https://www.opensecrets.org/federal-lobbying/clients/summary?id=D000073362. Notably, Lockheed Martin, RTX, Palantir, and Anduril all spent more on lobbying in 2024 than in 2025.

133 Mandy Smithberger, "Never the Pentagon: How the Military-Industrial Complex Gets Away with Murder in Contract After Contract," Project On Government Oversight, January 21, 2020, https://www.pogo.org/analysis/never-the-pentagon.

134 Anduril Industries, "Anduril Expands Solid Rocket Motor Production Facility," June 9, 2024, https://www.anduril.com/article/anduril-expands-solid-rocket-motor-production-facility; Anduril Industries, "Anduril Expands into New Atlanta Office, Research, Development and Production Facility," March 12, 2023, https://www.anduril.com/article/anduril-expands-into-new-atlanta-office-research-development-and-production-facility; Cade Metz and Eric Lipton, "A.I. Military Start-Up Anduril Plans $1 Billion Factory in Ohio," *New York Times*, January 16, 2025, https://www.nytimes.com/2025/01/16/technology/anduril-factory-columbus-ohio.html; and Anduril Industries, "Anduril to Open Large Scale Production Facility for Autonomous Underwater Vehicles," June 16, 2024, https://www.anduril.com/article/anduril-to-open-large-scale-production-facility-for-autonomous-underwater-vehicles.

135 Tony Romm, "In Critical Ohio Senate Race, Crypto Cash Looks to Tip the Scales," *Washington Post*, September 23, 2024, https://www.washingtonpost.com/business/2024/09/20/ohio-senate-race-crypto-cash.

136 Shane Goldmacher, "Crypto PAC Jumps into Senate Race, Opposing Katie Porter in California," *New York Times*, February 13, 2024, https://www.nytimes.com/2024/02/13/us/politics/crypto-pac-katie-porter-senate.html.

137 Fredreka Schouten, "The Crypto Industry Plowed Tens of Millions into the Election. Now, It's Looking for a Return on That Investment," CNN, November 17, 2024, https://www.cnn.com/2024/11/17/politics/crypto-industry-donald-trump-reelection; and David Yaffe-Bellany and Robert Jimison, "Crypto Industry Reaches Milestone with Passage of First Major Bill," *New York Times*, July 17, 2025, https://www.nytimes.com/2025/07/17/technology/crypto-industry-milestone-legislation.html.

138 Amrith Ramkumar and Brian Schwartz, "Silicon Valley Launches Pro-AI PACs to Defend Industry in Midterm Elections," *Wall Street Journal*, August 25, 2025, https://www.wsj.com/politics/silicon-valley-launches-pro-ai-pacs-to-defend-industry-in-midterm-elections-287905b3?3.

139 Leading the Future, "AI Industry Launches 'Leading the Future' to Drive U.S. AI Leadership, Economic Growth, National Security, and Innovation," PR Newswire, August 25, 2025, https://www.prnewswire.com/news-releases/ai-industry-launches-leading-the-future-to-drive-us-ai-leadership-economic-growth-national-security-and-innovation-302537548.html.

140 Tyler Katzenberger and Christine Mui, "Meta to Launch California Super PAC Focused on AI," *Politico*, August 26, 2025, https://www.politico.com/news/2025/08/26/exclusive-meta-to-launch-california-super-pac-focused-on-ai-00524989.

141 For a more comprehensive list of second Trump administration officials with a background in the defense industry and related investment firms, see table E in this report's appendix.

142 DOD, "Hon. Michael A. Obadal, Under Secretary of the Army," accessed December 1, 2025, https://api.army.mil/e2/c/downloads/2025/09/22/1618c0bb/michael-obadal-bio.pdf [https://perma.cc/JZX9-Q3JF].

143 Meghann Myers, "Senators Question Army Undersecretary

Nominee on Transformation Plan," *Defense One*, May 8, 2025, https://www.defenseone.com/policy/2025/05/senators-question-army-undersecretary-nominee-transformation-plan/405168; Sen. Elizabeth Warren to Michael Obadal (nominee, undersecretary of the U.S. Army), May 7, 2025, https://www.warren.senate.gov/imo/media/doc/letter_from_senator_warren_to_mike_obadal_on_ethics_commitments.pdf; and Danica Irvine (alternate designated agency ethics official, DOD) to U.S. Office of Government Ethics, August 18, 2025, https://extapps2.oge.gov/201/Presiden.nsf/PAS+Index/22D2862F18C6328885258C6F002C8B8D/$FILE/Obadal%2C%20Michael%20%20AMENDED%20finalEA.pdf.

144 Steven Levy, "What Big Tech's Band of Execs Will Do in the Army," *Wired*, June 20, 2025, https://www.wired.com/story/what-lt-col-boz-and-big-techs-enlisted-execs-will-do-in-the-army.

145 Levy, "What Big Tech's Band of Execs Will Do in the Army."

146 See, e.g., Alexander C. Karp and Nicholas W. Zamiska, "New Weapons Will Eclipse Atomic Bombs. Their Builders Ask Themselves This Question," *Washington Post*, June 25, 2024, https://www.washingtonpost.com/opinions/2024/06/25/ai-weapon-us-tech-companies; Peter Thiel, "Good for Google, Bad for America," *New York Times*, August 1, 2019, https://www.nytimes.com/2019/08/01/opinion/peter-thiel-google.html; and Stern, "American Vulcan." See also NSCAI, *Final Report: National Security Commission on Artificial Intelligence*, 2; and Sharon Goldman, "Former Google CEO Eric Schmidt's AI Expo Serves Up Visions of War, Robotics, and LLMs for Throngs of Tech Execs, Defense Officials, and Fresh Recruits," *Fortune*, June 4, 2025, https://fortune.com/2025/06/04/eric-schmidt-ai-expo-washington-dc-openai-tesla-drones-military.

147 See DOD, *Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom*, November 10, 2025, 2, https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF; Sankar, "Defense Reformation"; and Anduril Industries, "Rebooting the Arsenal of Democracy: Anduril Mission Document," June 4, 2022, https://www.anduril.com/article/rebooting-the-arsenal-of-democracy-anduril-mission-document.

148 See NSCAI, *Final Report: National Security Commission on Artificial Intelligence*; Sankar, "Defense Reformation"; and Anduril Industries, "Rebooting the Arsenal of Democracy."

149 DOD, *Acquisition Transformation Strategy*, 2.

150 DOD, *Acquisition Transformation Strategy*, 25.

151 See, e.g., DOD Inspector General, *Summary of DoD Office of Inspector General Spare-Parts Pricing Audits: Additional Guidance Is Needed*, March 31, 2015, https://media.defense.gov/2015/Mar/31/2001713486/-1/-1/1/DODIG-2015-103.pdf; U.S. Attorney's Office, Eastern District of Virginia, "VMware and Carahsoft Agree to Pay $75.5 Million to Settle Claims That They Concealed Commercial Pricing and Overcharged the Government," news release, June 30, 2015, https://media.defense.gov/2015/Jun/30/2001711737/-1/-1/1/VMwareCarahsoftPR.pdf; U.S. Department of Justice, "Dell and Iron Bow Agree to Pay $4.3M to Resolve False Claims Act Allegations Relating to Submitting Non-Competitive Bids to the Army," news release, November 19, 2024, https://www.justice.gov/archives/opa/pr/dell-and-iron-bow-agree-pay-43m-resolve-false-claims-act-allegations-relating-submitting-non; and DOD Inspector General, *Audit of the Business Model for TransDigm Group Inc. and Its Impact on Department of Defense Spare Parts Pricing*, December 13, 2021, https://media.defense.gov/2021/Dec/27/2002914678/-1/-1/1/DODIG-2022-043%20508.PDF.

152 Truth in Negotiations Act, Pub. L. 87-653, 76 Stat. 528 (1962), https://www.congress.gov/87/statute/STATUTE-76/STATUTE-76-Pg528.pdf. See 10 U.S.C. § 3702; and 48 C.F.R. § 215.402.

153 Defense Acquisition University, "Cost/Pricing Data," accessed December 1, 2025, https://www.dau.edu/glossary/cost/pricing-data.

154 GAO, *Federal Contracting: Implementation of Changes to Cost or Pricing Data Requirements*, April 14, 2022, 7, https://www.gao.gov/assets/gao-22-105307.pdf.

155 Ward T. Williams, "The Truth-in-Negotiations Act: The Need for Both Truth and Fairness," *Villanova Law Review* 16, no. 1 (1970), https://digitalcommons.law.villanova.edu/vlr/vol16/iss1/6.

156 Amos Toh and Julia Gledhill, "How Acquisition Reform Could Make Military AI More Expensive and Less Safe," *Lawfare*, October 9, 2025, https://www.lawfaremedia.org/article/how-acquisition-reform-could-make-military-ai-more-expensive-and-less-safe.

157 John F. Wharton and Tate Nurkin, "Why Is US Defense Acquisition Falling Behind? Blame the TINA Paradox," Atlantic Council, August 10, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/why-is-us-defense-acquisition-falling-behind-blame-the-tina-paradox.

158 DOD, *Acquisition Transformation Strategy*, 25.

159 48 C.F.R. § 31.205-6.

160 See GAO, *Federal Contracting*, 7–8.

161 Truth in Negotiations Act, Pub. L. 87-653; and National Defense Authorization Act for Fiscal Year 2026, Pub. L. 119-60, § 1804 (2025), https://www.congress.gov/119/bills/s1071/BILLS-119s1071enr.pdf.

162 House Committee on Oversight and Government Reform, Democrats, "Ahead of Hearing, Oversight Committee Releases New Information on Price Gouging by TransDigm in DOD Contracts," news release, January 19, 2022, https://oversightdemocrats.house.gov/news/press-releases/ahead-of-hearing-oversight-committee-releases-new-information-on-price-gouging; and DOD Inspector General, *Audit of the Business Model for TransDigm Group Inc.* See also Sen. Elizabeth Warren and Rep. John Garamendi to Lloyd Austin (secretary of defense), November 29, 2023, 2, https://www.warren.senate.gov/imo/media/doc/2023.11.29%20Follow%20up%20Letter%20to%20DoD%20re%20Cost%20or%20Pricing%20Data.pdf.

163 National Defense Authorization Act for 2026, § 1826.

164 48 C.F.R. § 2.101.

165 Federal Acquisition Streamlining Act of 1994 (FASA), Pub. L. 103-355 (1994), https://www.congress.gov/bill/103rd-congress/senate-bill/1587/text; and National Defense Authorization Act for Fiscal Year 1996, Pub. L. 104-106, 110 Stat. 202, Div. D — Federal Acquisition Reform (1996), https://www.congress.gov/104/plaws/publ106/PLAW-104publ106.pdf.

166 Richard C. Loeb, *Caveat Emptor: Reversing the Anti-Competitive and Over-Pricing Policies That Plague Government Contracting*, American Economic Liberties Project, June 2020, 8, https://www.economicliberties.us/wp-content/uploads/2020/06/Working-Paper-Series-on-Corporate-Power_4.pdf.

167 Office of Elizabeth Warren, "At Hearing, Defense Contractor Agrees with Warren: Legal Loopholes Should Not Lead to Price-Gouging the Military," news release, January 28, 2025, https://www.warren.senate.gov/newsroom/press-releases/at-hearing-defense-contractor-agrees-with-warren-legal-loopholes-should-not-lead-to-price-gouging-the-military; and DOD and Honeywell International Inc., indefinite delivery/indefinite quantity contract, W58RGZ20D0098, September 28, 2020, https://www.usaspending.gov/award/CONT_IDV_W58RGZ20D0098_9700 [https://perma.cc/US5X-VTEP].

168 DOD Inspector General, *Acquisition: Contracting for and Performance of the C-130J Aircraft*, July 23, 2024, 11, https://media.defense.gov/2004/Jul/23/2001713142/-1/-1/1/04-102.pdf.

169 DOD and Palantir USG Inc., indefinite delivery/indefinite quantity contract, W911QX24D0026, September 18, 2024, https://www.usaspending.gov/award/CONT_IDV_W911QX24D0026_9700 [https://perma.cc/8H4W-DQ6N]; Anduril Industries, "DIU Awards Anduril Contract to Innovate New Capabilities for Undersea Warfare," February 7, 2024, https://www.anduril.com/article/diu-awards-

anduril-contract-to-innovate-new-capabilities-for-undersea-warfare; and DOD and Anduril Industries Inc., definitive contract, N0016425CJR94, February 11, 2025, https://www.usaspending.gov/award/CONT_AWD_N0016425CJR94_9700_-NONE-_-NONE- [https://perma.cc/3DC2-QCSH].

170 Palantir Technologies, "Supply Chain Risk Management," accessed December 1, 2025, https://www.palantir.com/offerings/supply-chain-risk-management.

171 Anduril Industries, "Anduril to Open Large Scale Production Facility."

172 Pete Hegseth to senior Pentagon leadership, commanders of combatant commands, and defense agency and DOD field activity directors, Re: Directing Modern Software Acquisition to Maximize Lethality, March 6, 2025, https://media.defense.gov/2025/Mar/07/2003662943/-1/-1/1/DIRECTING-MODERN-SOFTWARE-ACQUISITION-TO-MAXIMIZE-LETHALITY.PDF.

173 Defense Acquisition University, "Commercial Solutions Opening (DFARS 212.70)," accessed January 29, 2026, https://aaf.dau.edu/aaf/contracting-cone/defense-cso. Contracts for commercial items are also exempt from cost accounting standards criteria that prevent vendors from charging the Pentagon for costs unrelated to government contracts. See 48 C.F.R. § 12.214.

174 Defense Acquisition University, "Other Transactions," accessed January 29, 2026, https://aaf.dau.edu/aaf/contracting-cone/ot.

175 GAO, *Other Transaction Agreements: DOD Can Improve Planning for Consortia Awards*, September 20, 2022, 4, https://www.gao.gov/assets/gao-22-105357.pdf.

176 GAO, *Other Transaction Agreements*, 4–5.

177 CDAO, "CDAO Announces Partnerships with Frontier AI Companies."

178 Sayler, "Army's Integrated Visual Augmentation System."

179 DIU, "Replicator"; and DIU, "Advancing DoD Operations with Software Acquisition Reform," March 7, 2025, https://www.diu.mil/latest/advancing-dod-operational-capabilities-with-software-acquisition-reform [https://perma.cc/D977-RGYJ].

180 GAO, *Other Transaction Agreements: Improved Contracting Data Would Help DOD Assess Effectiveness*, September 3, 2025, https://www.gao.gov/products/gao-25-107546.

181 GAO, *Weapon System Sustainment: DOD Can Improve Planning and Management of Data Rights*, September 29, 2025, https://www.gao.gov/assets/gao-25-107468.pdf.

182 10 U.S.C. § 4022.

183 David H. Carpenter and Alexandra G. Neenan, "Defense Primer: Other Transactions (OTs)," Congressional Research Service, December 19, 2024, https://www.congress.gov/crs-product/IF12856.

184 Scott Amey, "Other Transactions: Do the Rewards Outweigh the Risks?," Project On Government Oversight, March 15, 2019, https://www.pogo.org/reports/other-transactions-do-the-rewards-outweigh-the-risks; and Austin Gray, "OTAs, Defense Tech, and the Path to Revenue," Substack, October 11, 2024, https://austinegray.substack.com/p/otas.

185 Amey, "Other Transactions."

186 Microsoft qualified for nontraditional defense contractor (NDC) status in 2021 when it was awarded the IVAS OT agreement; Google qualified in 2025 when it was awarded a foundation model OT agreement; and Palantir qualified in 2024 when it was awarded a CJADC2-related OT agreement. Deborah Bach, "U.S. Army to Use HoloLens Technology in High-Tech Headsets for Soldiers," Microsoft, June 8, 2021, https://news.microsoft.com/source/features/digital-transformation/u-s-army-to-use-hololens-technology-in-high-tech-headsets-for-soldiers; CDAO, "CDAO Announces Partnerships with Frontier AI Companies"; and Palantir Technologies, "Palantir Selected by Chief Digital and Artificial Intelligence Office (CDAO) to Participate in Scaling Data Analytics and AI Capabilities Across the Department of Defense in Support of CJADC2 Strategy," news release, May 30, 2024, https://investors.palantir.com/news-details/2024/Palantir-Selected-by-Chief-Digital-and-[...]-the-Department-of-Defense-in-Support-of-CJADC2-Strategy.

187 DOD, *State of Competition Within the Defense Industrial Base*; and Susannah Glickman, "The War over Defense Tech," *New York Review*, October 4, 2025, https://www.nybooks.com/online/2025/10/04/the-war-over-defense-tech ("Using [Palantir's software] as the 'data backbone' for a vast and complicated system makes it distinctly costly and burdensome to switch software in the future, not to mention to train and retrain its users.").

188 DOD, "DOD Adopts Ethical Principles for Artificial Intelligence," news release, February 24, 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence.

189 See, e.g., DOD, Directive 3000.09: Autonomy in Weapon Systems, January 25, 2023, § 1.2(f), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf. See also DOD Responsible AI Working Council, *U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway*, June 2022, 25–28, https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF.

190 DIU, "Responsible AI Guidelines: Operationalizing DoD's Ethical Principles for AI," accessed January 27, 2026, https://www.diu.mil/responsible-ai-guidelines [https://perma.cc/PH7F-EK8V?type=image]; and David Vergun, "Defense Innovation Unit Publishes 'Responsible AI Guidelines,'" DOD, November 18, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2847598/defense-innovation-unit-publishes-responsible-ai-guidelines.

191 DIU, *Responsible Artificial Intelligence: 2022 in Review*, May 1, 2023, 5, https://s3.us-gov-west-1.amazonaws.com/publicdocs.diu.mil/RAI_Guidelines_-_2022_in_Review.pdf [https://perma.cc/2A2C-5DAR].

192 DIU, *Responsible Artificial Intelligence*, 5.

193 Office of the Director of National Intelligence (ODNI), "Principles of Artificial Intelligence Ethics for the Intelligence Community," July 23, 2020, https://www.dni.gov/files/ODNI/documents/Principles_of_AI_Ethics_for_the_Intelligence_Community.pdf.

194 Joseph R. Biden Jr., National Security Memorandum/NSM-25, Re: Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence, October 24, 2024, https://www.govinfo.gov/content/pkg/DCPD-202400945/pdf/DCPD-202400945.pdf; and The White House, *Framework to Advance AI Governance and Risk Management in National Security*, October 24, 2024, https://data.aclum.org/storage/2025/01/WhiteHouse_ai_gov_wp-content_uploads_2024_10_NSM-Framework-to-Advance-AI-Governance-and-Risk-Management-in-National-Security.pdf [https://perma.cc/DV6L-73NB].

195 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, Exec. Order No. 14110, 88 Fed. Reg. 75191 (October 30, 2023), § 4.8, https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf; and Removing Barriers to American Leadership in Artificial Intelligence, Exec. Order No. 14179, 90 Fed. Reg. 8741 (January 31, 2025), https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence.

196 White House, *Framework to Advance AI Governance and Risk Management*, 4; and DOD, Directive 3000.09 (2023).

197 See, e.g., Tristan Greene, "Report: Palantir Took Over Project Maven, the Military AI Program Too Unethical for Google," The Next Web, December 11, 2019, https://thenextweb.com/news/report-palantir-took-over-project-maven-the-military-ai-program-too-unethical-for-google ("The limited, unclassified information available makes it appear as though the project stops just short of functioning as an AI weapons system capable of firing on self-designated targets."). But see Jon Harper, "Marine Corps to Receive New Smart Sensor System for MQ-9 Reaper Drones," *DefenseScoop*, April 29, 2025, https://defensescoop.com/2025/04/29/marine-corps-mq-9-reaper-drones-smart-sensor-system (describing MQ-9 Reaper drones outfitted with AI to "find, fix, track and target targets of interest").

198 White House, *Framework to Advance AI Governance and Risk Management*, 8.

199 White House, *Framework to Advance AI Governance and Risk Management*, 12.

200 White House, *Framework to Advance AI Governance and Risk Management*, 3.

201 Lisa Feldman Barrett et al., "Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements," *Psychological Science in the Public Interest* 20, no. 1 (July 2019): 1–68, https://doi.org/10.1177/1529100619832930.

202 White House, *Framework to Advance AI Governance and Risk Management*, 3. Note that AI use is presumed to be "high-impact" only if "the AI use controls or significantly influences the outcomes" of these activities.

203 White House, *Framework to Advance AI Governance and Risk Management*, 5–7.

204 White House, *Framework to Advance AI Governance and Risk Management*, 7.

205 See Jesus Jiménez, "Worried About Meta Using Your Instagram to Train Its A.I.? Here's What to Know," *New York Times*, September 26, 2024, https://www.nytimes.com/article/meta-ai-scraping-policy.html.

206 Rachel Levinson-Waldman et al., "Social Media Surveillance by the U.S. Government," Brennan Center for Justice, January 7, 2022, https://www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

207 Heidy Khlaaf et al., "Mind the Gap: Foundation Models and the Covert Proliferation of Military Intelligence, Surveillance, and Targeting," arXiv:2410.14831 (October 18, 2024): 6–7, https://doi.org/10.48550/arXiv.2410.14831.

208 White House, *Framework to Advance AI Governance and Risk Management*, 9.

209 Connor Echols, "Victims of US Military Violence Are Getting Stiffed," Responsible Statecraft, December 15, 2023, https://responsiblestatecraft.org/drone-strike-civilian-casualties.

210 United States, "Human-Machine Interaction in the Development, Deployment and Use of Emerging Technologies in the Area of Lethal Autonomous Weapons Systems," paper presented at a meeting of a group of governmental experts of the high contracting parties to the United Nations Convention on Certain Conventional Weapons (CCW), second session, Geneva, August 28, 2018, https://documents.un.org/doc/undoc/gen/g18/261/55/pdf/g1826155.pdf.

211 DOD, Directive 3000.09: Autonomy in Weapon Systems, November 21, 2012, 1, https://ogc.osd.mil/Portals/99/autonomy_in_weapon_systems_dodd_3000_09.pdf.

212 DOD, "DoD Announces Update to DoD Directive 3000.09, 'Autonomy in Weapon Systems,'" news release, January 25, 2023, https://www.defense.gov/News/Releases/Release/article/3278076/dod-announces-update-to-dod-directive-300009-autonomy-in-weapon-systems.

213 DOD, Directive 3000.09 (2023), 22. Note that this definition still holds even if an operator can override operation of the system. The point is that a system has the *capability* to select and engage targets without further human intervention.

214 DOD, Directive 3000.09 (2023), 23 (emphasis added).

215 DOD, Directive 3000.09 (2023), § 4.1(c)(1).

216 Kelley M. Sayler, "Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems," Congressional Research Service, January 2, 2025, https://www.congress.gov/crs-product/IF11150.

217 DOD, Directive 3000.09 (2023), § 4.1(d)(1).

218 International Committee of the Red Cross, *Autonomous Weapon Systems and International Humanitarian Law: Selected Issues*, October 2025, https://www.icrc.org/sites/default/files/media_file/2025-10/ICRC-Position_Paper-Autonomous_Weapon_Systems_and_IHL-Selected_issues_Oct2025.pdf.

219 Elke Schwarz, "Delegating Moral Responsibility in War: Lethal Autonomous Weapons Systems and the Responsibility Gap," in *The Routledge Handbook on Responsibility in International Relations*, ed. Hannes Hansen-Magnusson and Antje Vetterlein (Routledge, 2021), 177–91, esp. 184, https://www.taylorfrancis.com/chapters/edit/10.4324/9780429266317-13/delegating-moral-responsibility-war-elke-schwarz.

220 Schwarz, "Delegating Moral Responsibility in War," 184–85.

221 See Abi Olvera, "Why Nobody Can See Inside AI's Black Box," Bulletin of the Atomic Scientists, January 27, 2025, https://thebulletin.org/2025/01/why-nobody-can-see-inside-ais-black-box.

222 These criteria reflect the principles of distinction and proportionality under the laws of war. DOD, *Law of War Manual*, updated July 2023, 60–65, 374–376, https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF; and International Committee of the Red Cross, *Autonomous Weapon Systems and International Humanitarian Law*.

223 DOD, Directive 3000.09 (2023), § 1(2)(d)(4).

224 DOD, Directive 3000.03E: DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy, August 31, 2018, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300003p.pdf?ver=2017-09-27-.

225 DOD, Directive 3000.09 (2023), § 4.2.

226 Sydney J. Freedberg Jr., "Fear and Loathing in AI: How the Army Triggered Fears of Killer Robots," *Breaking Defense*, March 6, 2019, https://breakingdefense.com/2019/03/fear-loathing-in-ai-how-the-army-triggered-fears-of-killer-robots.

227 Human Rights Watch and Harvard Law School International Human Rights Clinic (IHRC), *Background Briefing: Review of the 2023 US Policy on Autonomy in Weapons Systems*, February 2023, 3 https://www.hrw.org/sites/default/files/media_2023/02/DoDrobots_2.13.2023_Final_0.pdf.

228 National Defense Authorization Act for 2026, § 1061. See also Amos Toh, "The Good, Bad and Really Weird AI Provisions in the Annual US Defense Policy Bill," Tech Policy Press, December 15, 2025, https://www.techpolicy.press/the-good-bad-and-really-weird-ai-provisions-in-the-annual-us-defense-policy-bill.

229 Amanda Miller, "AI Algorithms Deployed in Kill Chain Target Recognition," *Air & Space Forces Magazine*, September 21, 2021, https://www.airandspaceforces.com/ai-algorithms-deployed-in-kill-chain-target-recognition; Hegseth to senior Pentagon leadership et al., Re: Directing Modern Software Acquisition to Maximize Lethality.

230 DOD, Directive 3000.09 (2012), § 4(a)(1), enclosure 2.

231 DOD, Directive 3000.09 (2023), §§ 1.2(a)(1), 2.3(h), 2.5(b), 2.9(b)(3), and 3(d).

232 DOD, Directive 3000.09 (2012), 15 (emphasis added).

233 DOD, Directive 3000.09 (2023), 23.

234 Human Rights Watch and IHRC, *Background Briefing*, 5.

235 Human Rights Watch and IHRC, *Background Briefing*, 5.

236 See generally DOD, Directive 3000.09 (2023). See also DOD, *Law of War Manual*.

237 See generally DOD, Instruction 3000.17: Civilian Harm Mitigation and Response, December 21, 2023, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/300017p.pdf.

238 John Ismay and Azmat Khan, "Hegseth Cuts Pentagon Work on Preventing Civilian Harm," *New York Times*, March 4, 2025, https://www.nytimes.com/2025/03/04/us/politics/hegseth-pentagon-civilian-harm.html; Nick Turse, "Pete Hegseth Is Gutting Pentagon Programs That Reduce Civilian Casualties," *Intercept*, April 15, 2025, https://theintercept.com/2025/04/15/pete-hegseth-pentagon-civilian-casualties-harm; and Nick Turse, "U.S. Military Command That Attacked Venezuela Gutted Its Civilian Harm Team," *Intercept*, January 13, 2026, https://theintercept.com/2026/01/13/civilian-harm-venezuela-airwars-southcom.

239 DOT&E previously had 94 personnel (82 civilians and 12 military); it currently has 45 personnel (30 civilian and 15 military). Pete Hegseth to senior Pentagon leadership, Re: Reorganization of the Office of the Director of Operational Test and Evaluation, May 27, 2025, https://media.defense.gov/2025/May/28/2003725153/-1/-1/1/MEMORANDUM-DIRECTING-REORGANIZATION-OF-THE-OFFICE-OF-THE-DIRECTOR-OF-OPERATIONAL-TEST-AND-EVALUATION.PDF; and Dan Grazier, "Gutting Military Testing Office May Be the Deadliest Move Yet," Henry L. Stimson Center, June 4, 2025, https://www.stimson.org/2025/gutting-military-testing-office-may-be-the-deadliest-move-yet.

240 Office of the Director of Operational Test and Evaluation, "T&E Oversight List," May 9, 2025, https://www.dote.osd.mil/Portals/97/pub/reports/oversight/TE%20Oversight%20List%2020250508%20www%20extract.pdf.

241 See Mark Thompson, "Army Prematurely Pushes Black Hawk Replacement into Production," *Responsible Statecraft*, June 5, 2025, https://responsiblestatecraft.org/army-black-hawk.

242 Somerville and Forrest, "How American Drones Failed to Turn the Tide in Ukraine."

243 Somerville and Forrest, "How American Drones Failed to Turn the Tide in Ukraine"; and Shelby Holliday et al., "'We Do Fail . . . a Lot': Defense Startup Anduril Hits Setbacks with Weapons Tech," *Wall Street Journal*, November 27, 2025, https://www.wsj.com/business/anduril-industries-defense-tech-problems-52b90cae.

244 Holliday et al., "'We Do Fail . . . a Lot.'"

245 Holliday et al., "'We Do Fail . . . a Lot'"; and Anduril Industries, "How Defense Technology Actually Gets Built," November 24, 2025, https://www.anduril.com/news/how-defense-technology-actually-gets-built.

246 Anduril Industries, "How Defense Technology Actually Gets Built."

247 Gina Heeb, "Microsoft Wins $22 Billion Army Contract for Augmented Reality Headsets," *Forbes*, March 31, 2021, https://www.forbes.com/sites/ginaheeb/2021/03/31/microsoft-wins-22-billion-army-contract-for-augmented-reality-headsets.

248 DOD Inspector General, *Audit of the Army's Integrated Visual Augmentation System*, April 20, 2022, 7, https://media.defense.gov/2022/Apr/22/2002981953/-1/-1/1/DODIG-2022-085.PDF (finding a lack of effectiveness metrics such as "clear measures of user acceptance levels [among soldiers]").

249 Side effects included "disorientation, dizziness, eye strain, heads [*sic*] and motion sickness, nausea, neck strain, and tunnel vision." *Fiscal Year 2024 Army Modernization Programs: Hearing on National Defense Authorization Act for Fiscal Year 2024 and Oversight of Previously Authorized Programs Before the Subcomm. on Tactical Air and Land Forces, H. Comm. on Armed Services*, 118th Cong. (2023) (opening statement of Representative Robert J. Wittman, subcommittee chairman), https://www.govinfo.gov/content/pkg/CHRG-118hhrg52421/html/CHRG-118hhrg52421.htm.

250 *Fiscal Year 2024 Army Modernization Programs* (opening statement of Representative Robert J. Wittman); and Department of the Army and Microsoft Corporation and Anduril Industries Inc., other transaction IDV, ID W91CRB219P002, accessed December 1, 2025, https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=W91CRB219P002+9700 [https://perma.cc/6GAN-RG4D].

251 Harper, "Anduril Integrates AI Tech into Army IVAS Headsets."

252 Patrick Tucker, "With IVAS Takeover, Anduril Looks to Build Out Human-Machine 'Ecosystem,'" *Defense One*, February 13, 2025, https://www.defenseone.com/business/2025/02/ivas-takeover-anduril-looks-build-out-human-machine-ecosystem/403009.

253 The Trump administration's executive order directing agencies to purchase "ideologically neutral" AI has raised censorship concerns and could undermine model performance. See Amos Toh, "How Trump's AI Policy Could Compromise the Technology," Brennan Center for Justice, August 1, 2025, https://www.brennancenter.org/our-work/analysis-opinion/how-trumps-ai-policy-could-compromise-technology. However, listening sessions between industry and the government in response to the executive order may provide an opportunity to identify and mitigate national security risks associated with unwanted model behavior. See U.S. Chief Information Officers Council, "AI Transparency Listening Session with the White House Office of Management and Budget," September 26, 2025, https://www.cio.gov/news/ai-transparency-listening-session.

254 The commercial AI models that the DOD relies on to classify and analyze data for targeting and other military operations are serviced by company engineers and housed on company infrastructure that may also become the targets of foreign adversaries. Khlaaf et al., "Mind the Gap," 8; and Mieke Eoyang, "Military AI Needs Guardrails — Not to Slow It Down, but to Keep It Useful," *Defense One*, September 29, 2025, https://www.defenseone.com/ideas/2025/09/military-ai-needs-guardrailsnot-slow-it-down-keep-it-useful/408452.

255 Saleha Mohsin, "Inside Project Maven, the US Military's AI Project," Bloomberg, February 29, 2024, https://www.bloomberg.com/news/newsletters/2024-02-29/inside-project-maven-the-us-military-s-ai-project.

256 Mohsin, "Inside Project Maven."

257 Patrick Tucker, "This Air Force Targeting AI Thought It Had a 90% Success Rate. It Was More Like 25%," *Defense One*, December 9, 2021, https://www.defenseone.com/technology/2021/12/air-force-targeting-ai-thought-it-had-90-success-rate-it-was-more-25/187437.

258 Tucker, "This Air Force Targeting AI Thought It Had a 90% Success Rate."

259 Leonardo Nicoletti and Dina Bass, *Humans Are Biased. Generative AI Is Even Worse*, Bloomberg Technology, June 9, 2023, https://www.bloomberg.com/graphics/2023-generative-ai-bias.

260 Anna Woorim Chung, "How Automated Tools Discriminate Against Black Language," MIT Center for Civic Media, January 24, 2019, https://civic.mit.edu/index.html%3Fp=2402.html; and Andrew Myers, "Rooting Out Anti-Muslim Bias in Popular Language Model GPT-3," Stanford University Human-Centered Artificial Intelligence, July 22, 2021, https://hai.stanford.edu/news/rooting-out-anti-muslim-bias-popular-language-model-gpt-3.

261 Other government agencies have found that social media monitoring tools have failed to reliably identify security threats, even though the role of bias in these failures is unclear. Department of Homeland Security, "Social Media," in *USCIS Presidential Transition Records*, 2020, 198–99, https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf; and Faiza Patel et al., *Social Media Monitoring*, Brennan Center for Justice, March 11, 2020, https://www.brennancenter.org/our-work/research-reports/social-media-monitoring.

262 Patrick Groher et al., *Face Recognition Technology Evaluation (FRTE)*, National Institute of Standards and Technology, January 9, 2026, 10–13, https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf (finding that facial recognition algorithms are "increasingly tolerant" to low-quality images but these continue to be responsible for "declines in accuracy"); and Frenkel, "Israel Deploys Expansive Facial Recognition Program in Gaza."

263 Dwoskin, "Israel Built an 'AI Factory' for War" (noting that an internal audit found that IDF AI systems "for processing the Arabic language had inaccuracies, failing to understand key slang words and phrases"). See also Harsha Panduranga and Emil Mella Pablo, "Federal Government Social Media Surveillance, Explained," Brennan Center for Justice, February 9, 2022, https://www.brennancenter.org/our-work/research-reports/federal-government-social-media-surveillance-explained; and Gabriel Nicholas and Aliya Bhatia, *Lost in Translation: Large Language Models in Non-English Content Analysis*, Center for Democracy & Technology, May 2023, https://cdt.org/wp-content/uploads/2023/05/non-en-content-analysis-primer-051223-1203.pdf.

264 Elke Schwarz, "Autonomous Weapons Systems, Artificial Intelligence, and the Problem of Meaningful Human Control," *The Philosophical Journal of Conflict and Violence* 5, no. 1 (2021): 64, https://doi.org/10.22618/TP.PJCV.20215.1.139004.

265 Neil Renic and Elke Schwarz, "Crimes of Dispassion: Autonomous Weapons and the Moral Challenge of Systematic Killing," *Ethics & International Affairs* 37, no. 3 (Fall 2023): 336–37, https://doi.org/10.1017/S0892679423000291.

266 Israel Defense Forces, "The IDF's Use of Data Technologies in Intelligence Processing," June 18, 2024, https://www.idf.il/210062.

267 Dwoskin, "Israel Built an 'AI Factory' for War"; Frenkel and Odenheimer, "Israel's A.I. Experiments in Gaza War"; Bethan McKernan and Harry Davies, "'The Machine Did It Coldly': Israel Used AI to Identify 37,000 Hamas Targets," *Guardian*, April 3, 2024, https://www.theguardian.com/world/2024/apr/03/israel-gaza-ai-database-hamas-airstrikes; and Yuval Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine*, April 3, 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza.

268 Dwoskin, "Israel Built an 'AI Factory' for War."

269 Patrick Kingsley et al., "Israel Loosened Its Rules to Bomb Hamas Fighters, Killing Many More Civilians," *New York Times*, December 26, 2024, https://www.nytimes.com/2024/12/26/world/middleeast/israel-hamas-gaza-bombing.html; Dwoskin, "Israel Built an 'AI Factory' for War"; and Harry Davies et al., "'The Gospel': How Israel Uses AI to Select Bombing Targets in Gaza," *Guardian*, December 1, 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

270 Israel Defense Forces, "IDF's Use of Data Technologies."

271 Dwoskin, "Israel Built an 'AI Factory' for War."

272 Dwoskin, "Israel Built an 'AI Factory' for War"; Kingsley et al., "Israel Loosened Its Rules to Bomb Hamas Fighters"; and McKernan and Davies, "'Machine Did It Coldly.'"

273 Dwoskin, "Israel Built an 'AI Factory' for War"; and Davies et al., "'The Gospel.'"

274 Dwoskin, "Israel Built an 'AI Factory' for War"; and Kingsley et al., "Israel Loosened Its Rules to Bomb Hamas Fighters." The U.S. State Department concluded that military operations in Gaza had killed 21,000 Palestinians and injured more than 56,000 by the end of 2023. U.S. Department of State, *2023 Country Reports on Human Rights Practices: Israel, West Bank and Gaza*, April 22, 2024, https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/israel-west-bank-and-gaza.

275 U.S. National Security Agency, *SKYNET: Courier Detection via Machine Learning*, June 5, 2012, https://www.eff.org/files/2015/06/01/20150508-intercept-skynet-courier-detection.pdf; Hadas Gold, "Report: U.S. Marked Al Jazeera Journalist a Terrorist," *Politico*, May 8, 2015, https://www.politico.com/blogs/media/2015/05/report-us-marked-al-jazeera-journalist-a-terrorist-206825; and Cora Currier et al., "U.S. Government Designated Prominent Al Jazeera Journalist as 'Member of Al Qaeda,'" *Intercept*, May 8, 2015, https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list.

276 Christian Grothoff and J. M. Porup, "The NSA's SKYNET Program May Be Killing Thousands of Innocent People," *Ars Technica*, February 16, 2016, https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people; and Mike Murphy, "There May Be a Big Flaw in the U.S. Government's AI System to Identify Terrorists in Pakistan," *Quartz*, July 21, 2022, https://qz.com/617619/there-may-be-a-big-flaw-in-the-us-governments-ai-system-to-identify-terrorists-in-pakistan.

277 See Grothoff and Porup, "NSA's SKYNET Program." But see Martin Robbins, "Has a Rampaging AI Algorithm Really Killed Thousands in Pakistan?," *Guardian*, February 18, 2016, https://www.theguardian.com/science/the-lay-scientist/2016/feb/18/has-a-rampaging-ai-algorithm-really-killed-thousands-in-pakistan.

278 Scott Shane, "Drone Strikes Reveal Uncomfortable Truth: U.S. Is Often Unsure About Who Will Die," *New York Times*, April 23, 2015, https://www.nytimes.com/2015/04/24/world/asia/drone-strikes-reveal-uncomfortable-truth-us-is-often-unsure-about-who-will-die.html.

279 Renic and Schwarz, "Crimes of Dispassion."

280 "President Obama Reflects on the Drone Program and 'The Illusion That It Is Not War,'" *The Late Show with Stephen Colbert*, December 1, 2020, https://www.youtube.com/watch?v=V-Q8MFjlQ2Y.

281 Azmat Khan, "The Civilian Casualty Files: Hidden Pentagon Records Reveal Patterns of Failure in Deadly Airstrikes," *New York Times*, December 18, 2021, https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html.

282 Khan, "Civilian Casualty Files."

283 Colleen McClain et al., *How the U.S. Public and AI Experts View Artificial Intelligence*, Pew Research Center, April 3, 2025, https://www.pewresearch.org/internet/2025/04/03/how-the-us-public-and-ai-experts-view-artificial-intelligence.

284 Ashley Deeks, "The Double Black Box: AI Inside the National Security Ecosystem," *Just Security*, August 14, 2024, https://www.justsecurity.org/98555/the-double-black-box-ai-inside-the-national-security-ecosystem. See also Ashley S. Deeks, *The Double Black Box: National Security, Artificial Intelligence, and the Struggle for Democratic Accountability* (Oxford University Press, 2025), https://doi.org/10.1093/9780197520932.003.0001.

285 Shirin Sinnar, "Courts Have Been Hiding Behind National Security for Too Long," Brennan Center for Justice, August 11, 2021, https://www.brennancenter.org/our-work/analysis-opinion/courts-have-been-hiding-behind-national-security-too-long.

286 Katherine Yon Ebright, *Secret War*, Brennan Center for Justice, November 3, 2022, 12–13, https://www.brennancenter.org/our-work/research-reports/secret-war (explaining how Congress lacks

expertise, information, and resources to exercise effective oversight over certain key operations, in part because of the DOD's failures to comply with reporting requirements).

287 See Barton Gellman, "Edward Snowden, After Months of NSA Revelations, Says His Mission's Accomplished," *Washington Post*, December 23, 2013, https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html; and Select Comm. on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program Together with Foreword by Chairman Feinstein and Additional and Minority Views, S. Rep. No. 113–288 (December 9, 2014), https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-crpt-113srpt288.pdf.

288 See Olvera, "Why Nobody Can See Inside AI's Black Box."

289 The two main databases the Brennan Center relied on for its research were USASpending.gov and the Federal Procurement Data System (FPDS). The government shut down FPDS on February 25, 2026. Joseph Cox, "The Government Just Made It Harder to See What Spy Tech It Buys," 404 Media, February 26, 2026, https://www.404media.co/the-government-just-made-it-harder-to-see-what-spy-tech-it-buys. Certain contracting vehicles, like OT agreements, are excluded from USASpending.gov and were only made available on FPDS. The shutdown further frustrates the public's ability to account for government procurement practices.

290 See, e.g., DOD and ECS Federal LLC, definitive contract, W911QX18C0037, September 28, 2018, https://www.usaspending.gov/award/CONT_AWD_W911QX18C0037_9700_-NONE-_-NONE-/ [https://perma.cc/TJ2D-KMCE].

291 Jack Poulson, "Pentagon Confirms Erasure of Project Maven–Related Contract Records," *All-Source Intelligence*, November 5, 2024, https://jackpoulson.substack.com/p/pentagon-confirms-erasure-of-project (citing Federal Acquisition Regulation 4.606(c) and (d) as bases for contract deletion).

292 The DOD has deleted official records of the following contract from USAspending.gov and the FPDS; the only publicly available record is a copy that Tech Inquiry made before the deletion: Tech Inquiry, Procurement Records for W911QX19C0039, accessed December 1, 2025, https://techinquiry.org/?text=W911QX19C0039&guard= (site currently discontinued, on file with Tech Inquiry) .

293 See Gray, "OTAs, Defense Tech, and the Path to Revenue"; and GAO, *Other Transaction Agreements: DOD Can Improve Planning for Consortia Awards*.

294 Tabby Kinder and George Hammond, "Palantir and Anduril Join Forces with Tech Groups to Bid for Pentagon Contracts," *Financial Times*, December 22, 2024, https://www.ft.com/content/6cfdfe2b-6872-4963-bde8-dc6c43be5093.

295 GAO, *Other Transaction Agreements: DOD Can Improve Planning for Consortia Awards*, 43.

296 Silicon Valley Defense Group, *NATSEC100 Report: 2024 Edition*, July 2024, 16, https://sdvg-serving.s3.us-east-2.amazonaws.com/SVDG+NATSEC100+2024+Report.pdf.

297 See, e.g., Carey Shenkman et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Center for Democracy & Technology, December 9, 2021, 42, https://cdt.org/insights/report-legal-loopholes-and-data-for-dollars-how-law-enforcement-and-intelligence-agencies-are-buying-your-data-from-brokers.

298 32 C.F.R. § 1662.21; and Deepa Vardarajan, "Business Secrecy Expansion and FOIA," *UCLA Law Review* 68, no. 2 (August 2021): 468, https://www.uclalawreview.org/wp-content/uploads/securepdfs/2021/11/Varadarajan-68-2.pdf.

299 #Hash, "Problem with Palantir" ("Without open code, the government relies on vendor assurances that known and unknown vulnerabilities are being patched."); and Chloe Autio et al., *A Snapshot of Artificial Intelligence Procurement Challenges*, The Gov Lab, June 2023, 18, https://files.thegovlab.org/a-snapshot-of-ai-procurement-challenges-june2023.pdf.

300 See GAO, *F-35 Aircraft: DOD and the Military Services Need to Reassess the Future Sustainment Strategy*, September 21, 2023, https://www.gao.gov/products/gao-23-105341.

301 Mark Pomerleau, "Army Says It's Mitigated 'Critical' Cybersecurity Deficiencies in Early NGC2 Prototype," *Breaking Defense*, October 1, 2025, https://breakingdefense.com/2025/10/army-says-its-mitigated-critical-cybersecurity-deficiencies-in-early-ngc2-prototype; and Mike Stone, "Anduril and Palantir Battlefield Communication System Has Deep Flaws, Army Memo Says," Reuters, October 3, 2025, https://www.reuters.com/business/aerospace-defense/anduril-palantir-battlefield-communication-system-has-deep-flaws-army-memo-says-2025-10-03.

302 Khlaaf et al., "Mind the Gap," 8–9.

303 Brandi Vincent, "Scale AI to Set the Pentagon's Path for Testing and Evaluating Large Language Models," *DefenseScoop*, February 20, 2024, https://defensescoop.com/2024/02/20/scale-ai-pentagon-testing-evaluating-large-language-models.

304 Whitney M. McNamara et al., *Commission on Software-Defined Warfare: Final Report*, Atlantic Council, March 2025, 10, https://www.atlanticcouncil.org/wp-content/uploads/2025/03/Commission-on-Software-Defined-Warfare-Final-Report.pdf.

305 Freddy Brewster, "The Hole in Boeing's Inspection Program," *Lever*, February 7, 2024, https://www.levernews.com/the-hole-in-boeings-inspection-program.

306 Russell T. Vought (director, OMB) to heads of executive departments and agencies, Re: Accelerating Federal Use of AI Through Innovation, Governance, and Public Trust, April 3, 2025, https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-21-Accelerating-Federal-Use-of-AI-through-Innovation-Governance-and-Public-Trust.pdf; and Vought to heads of executive departments and agencies, Re: Driving Efficient Acquisition of Artificial Intelligence in Government, April 3, 2025, https://www.whitehouse.gov/wp-content/uploads/2025/02/M-25-22-Driving-Efficient-Acquisition-of-Artificial-Intelligence-in-Government.pdf.

307 Vought to heads of executive departments and agencies, April 3, 2025, "Re: Accelerating Federal Use of AI Through Innovation, Governance, and Public Trust," 16; and White House, *Framework to Advance AI Governance and Risk Management*, 5 (stating that AI risk and impact assessment should include "the intended purpose for the AI and its expected benefit, supported by metrics or qualitative analysis, *as appropriate*" (emphasis added)).

308 See Faiza Patel and Patrick C. Toomey, "Bringing Transparency to National Security Uses of Artificial Intelligence," *Just Security*, April 4, 2024, https://www.justsecurity.org/94113/bringing-transparency-to-national-security-uses-of-artificial-intelligence.

309 Matthew Olay, "Hegseth Orders Civilian Workforce Realignment in DOD, Reopens DRP," DOD, March 29, 2025, https://www.defense.gov/News/News-Stories/Article/Article/4138965/hegseth-orders-civilian-workforce-realignment-in-dod-reopens-drp.

310 DOD, Instruction 5000.98: Operational Test and Evaluation and Live Fire Test and Evaluation, December 9, 2024, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500098p.PDF?ver=InJ_BDOOVcUHyurlNv_FAg%3d%3d.

311 See Dan Grazier and Julia Gledhill, *Build a More Effective Military Force: Strengthen Oversight and Transparency to Protect Against Military Waste*, Henry L. Stimson Center, November 2024, 3, https://www.stimson.org/wp-content/uploads/2024/11/More-Effective-Military-Force_GrazierGledhill_FINAL.pdf; Project On Government Oversight, "Coalition Calls for Transparency in DOT&E's Annual Weapons Testing Report," February 9, 2022, https://www.

pogo.org/policy-letters/coalition-calls-for-transparency-in-dot-es-annual-weapons-testing-report; and Valerie Insinna, "Top Oversight Dems to Pentagon: Stop 'Hiding' Info on Weapons Programs from Public," *Breaking Defense*, February 23, 2022, https://breakingdefense.com/2022/02/top-oversight-dems-to-pentagon-stop-hiding-info-on-weapons-programs-from-public.

312 Brennan Center for Justice et al., "Comment Submitted to the Office of Management and Budget on Federal Procurement of Artificial Intelligence," April 29, 2024, 8–9, https://www.brennancenter.org/our-work/research-reports/comment-submitted-office-management-and-budget-federal-procurement.

313 AWARE Act of 2024, S. 5239, 118th Congress (2024), https://www.congress.gov/bill/118th-congress/senate-bill/5239.

314 See Khlaaf et al., "Mind the Gap."

315 See ODNI, "ODNI Releases IC Policy Framework for Commercially Available Information," news release, May 8, 2024, https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3815-odni-releases-ic-policy-framework-for-commercially-available-information.

316 See ODNI, "ODNI Releases IC Policy Framework for Commercially Available Information"; and Emile Ayoub, "Assessing the Intelligence Community's Policy Framework for Commercially Available Information," *Just Security*, May 24, 2024, https://www.justsecurity.org/96015/commercially-available-information.

317 See Ayoub and Goitein, "Closing the Data Broker Loophole"; Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Congress (2023), https://www.congress.gov/bill/118th-congress/house-bill/4639; and Fourth Amendment Is Not For Sale Act, S. 2576, 118th Congress (2023), https://www.congress.gov/bill/118th-congress/senate-bill/2576.

318 See Ayoub and Goitein, "Closing the Data Broker Loophole"; and Emile Ayoub, "We're Nearing a Point of No Return on Data Privacy. Congress Must Act," *Hill*, May 23, 2024, https://thehill.com/opinion/technology/4680104-were-nearing-a-point-of-no-return-on-data-privacy-congress-must-act.

319 Bills that would weaken defense acquisition guardrails have been introduced in the Senate and the House. See Fostering Reform and Government Efficiency in Defense Act, S. 5618, 118th Congress (2024), https://www.congress.gov/bill/118th-congress/senate-bill/5618/text; and Streamlining Procurement for Effective Execution and Delivery and National Defense Authorization Act for Fiscal Year 2026, H.R. 3838, 119th Congress (2025), https://www.congress.gov/bill/119th-congress/house-bill/3838/text. See also Christopher Preble et al., "Testing Assumptions About US Foreign Policy in 2025," Henry L. Stimson Center, February 14, 2025, https://www.stimson.org/2025/testing-assumptions-about-us-foreign-policy-in-2025.

320 Transparency in Contracting Act of 2025, S. 2809, 119th Congress (2025), https://www.congress.gov/bill/119th-congress/senate-bill/2809; and Stop Pentagon Price Gouging Act, S. 2049, 118th Congress (2023), https://www.congress.gov/bill/118th-congress/senate-bill/2049.

321 See, e.g., Brendan Bordelon, "Key Congress Staffers in AI Debate Are Funded by Tech Giants Like Google and Microsoft," *Politico*, December 3, 2023, https://www.politico.com/news/2023/12/03/congress-ai-fellows-tech-companies-00129701.

322 Maya Kornberg and Martha Kinsella, *Building Science and Technology Expertise in Congress*, Brennan Center for Justice, November 6, 2023, https://www.brennancenter.org/our-work/policy-solutions/building-science-and-technology-expertise-congress.

323 Daniel I. Weiner et al., "Nine Solutions for Political Corruption," Brennan Center for Justice, January 20, 2026, https://www.brennancenter.org/our-work/research-reports/nine-solutions-political-corruption; and Adriana Navarro et al., "Lobbyists Exploit Massive Loophole to Wine and Dine Lawmakers, Aides at Fancy Getaways," *Politico*, September 22, 2024, https://www.politico.com/news/2024/09/22/lobbyists-flout-ethics-rules-free-trips-00176749.

324 Farewell address by President Dwight D. Eisenhower, January 17, 1961, National Archives and Records Administration, College Park, MD, https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address; and Final TV Talk 1/17/61 (1), box 38, Speech Series, Papers of Dwight D. Eisenhower as President, 1953–61, Eisenhower Library, Abilene, KS.

325 Department of Defense and Palantir USG Inc., indefinite delivery/indefinite quantity contract, W519TC25D0039, July 31, 2025, https://www.usaspending.gov/award/CONT_IDV_W519TC25D0039_9700 [https://perma.cc/QS7Z-QDGZ]; and U.S. Army Public Affairs, "U.S. Army Awards Enterprise Service Agreement to Enhance Military Readiness."

326 Department of Defense and Palantir USG Inc., W911QX24D0026; DOD, "Contracts for Sept. 18, 2024," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/3910169; Katrina Manson, "Palantir Wins $100 Million US Contract for AI Targeting Tech," Bloomberg, September 19, 2024, https://www.bloomberg.com/news/articles/2024-09-19/palantir-wins-100-million-us-contract-for-ai-targeting-tech; and Palantir Technologies, "Palantir Expands Maven Smart System AI/ML Capabilities to Military Services," news release, September 20, 2024, https://investors.palantir.com/news-details/2024/Palantir-Expands-Maven-Smart-System-AIML-Capabilities-to-Military-Services. In September 2025, the Marine Corps announced a contract with Palantir for access to MSS. The Brennan Center was unable to locate any public record of the contract ID, ceiling or obligated amounts as of January 22, 2026. See U.S. Marine Corps, "Marine Corps Partners with Chief Digital and Artificial Intelligence Office and Defense Innovation Unit for Enterprise CJADC2 Capability Acceleration of Palantir System," news release, September 10, 2025, https://www.marines.mil/News/Press-Releases/Press-Release-Display/Article/4305728/marine-corps-partners-with-chief-digital-and-artificial-intelligence-office-and.

327 Department of the Army and Palantir USG Inc., indefinite delivery contract/indefinite delivery vehicle, W911QX24D0012, accessed January 22, 2026, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=W911QX24D0012&x=18&y=12 [https://perma.cc/CXG4-67AB]; DOD, "Contracts for May 21, 2025," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/4194643; Vincent, "'Growing Demand' Sparks DOD to Raise Palantir's Maven Contract"; Palantir Technologies, "Palantir Selected by Chief Digital and Artificial Intelligence Office (CDAO) to Participate in Scaling Data Analytics and AI Capabilities"; and Jon Harper, "Palantir Lands $480M Army Contract for Maven Artificial Intelligence Tech," *DefenseScoop*, May 29, 2024, https://defensescoop.com/2024/05/29/palantir-480-million-army-contract-maven-smart-system-artificial-intelligence.

328 The Brennan Center was unable to locate a record of this contract on USAspending.gov or the FPDS. Contract information is drawn from the DOD's June 2023 contract announcements: DOD, "Contracts for Jun. 5, 2023," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/3417409/contracts-for-jun-5-2023. See also Palantir Technologies, "US Special Operations Command Awards Contract to Palantir," news release, June 5, 2023, https://investors.palantir.com/news-details/2023/US-Special-Operations-Command-Awards-Contract-to-Palantir.

329 U.S. Special Operations Command and Palantir Technologies Inc., other transaction IDV, H924042190002, accessed January 22, 2026, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=H924042190002&x=35&y=14 [https://perma.cc/85J8-PUZN]; Palantir Technologies, "Palantir Awarded $111m Contract to Provide

Mission Command Platform for the United States Special Operations Command," May 28, 2021, https://www.palantir.com/newsroom/press-releases/palantir-ussocom-award-mission-command-platform; and Palantir Technologies, "Gotham."

330 Department of Defense and Palantir Technologies Inc., definitive contract, H9222216C0078, May 24, 2026, https://www.usaspending.gov/award/CONT_AWD_H9222216C0078_9700_-NONE-_-NONE- [https://perma.cc/6XPC-6AQ3]; and DOD, "Contracts for May 25, 2016," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/781719.

331 Department of Defense and Palantir Technologies Inc., blanket purchase agreement call, N0003920F0110, February 10, 2020, https://www.usaspending.gov/award/CONT_AWD_N0003920F0110_9700_N6600119A0044_9700 [https://perma.cc/TM27-A9LK]. Shortly after this agreement, *The Washington Post* reported that Palantir had sealed its first major deal with the U.S. Navy. It appears, however, that the February 2020 agreement is different from the one reported. Aaron Gregg, "Palantir Seals Its First Major U.S. Navy Deal as Raytheon Is Passed Over," *Washington Post*, March 5, 2020, https://www.washingtonpost.com/business/2020/03/05/palantir-first-navy-contract.

332 The DOD has deleted official records of this contract; the only publicly available record is a copy that Tech Inquiry made before the deletion: Tech Inquiry, Procurement Records for W911QX19C0039. The prime awardee for this contract is ECS Federal. See Ross Wilkers, "ECS Keeps $484M Army Unclassified Network Contract," *Washington Technology*, September 30, 2019, https://www.washingtontechnology.com/2019/09/ecs-keeps-484m-army-unclassified-network-contract/327093.

333 Department of the Army and Palantir USG Inc., other transaction IDV, W15QKN209P001, accessed January 22, 2026, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=W15QKN209P001&x=0&y=0 [https://perma.cc/38UB-Q322]; Palantir Technologies, "Palantir Expands Army Vantage Partnership with $618.9M Contract," news release, December 18, 2024, https://investors.palantir.com/news-details/2024/Palantir-Expands-Army-Vantage-Partnership-with-618.9M-Contract/; and DOD, "PEO EIS ARDAP Army Data Platform 2.0 RFI," notice ID no. ADP_RFI_11_30_23, December 1, 2023, https://sam.gov/opp/6cf58173525446d09c1bb74ac14a7a24/view.

334 Department of Defense and Palantir USG Inc., delivery order, FA880625FB009, June 16, 2025, https://www.usaspending.gov/award/CONT_AWD_FA880625FB009_9700_FA880623D0015_9700 [https://perma.cc/5CN6-YVJS]; and U.S. Space Force, "Space Systems Command Advances Space C2 Dominance Decision Making Through Data Platform Program," news release, May 16, 2025, https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/4188469/space-systems-command-advances-space-c2-dominance-decision-making-through-data.

335 Department of Homeland Security and Palantir Technologies Inc., blanket purchase agreement call, 70Z02320FPLM02200, April 6, 2020, https://www.usaspending.gov/award/CONT_AWD_70Z02320FPLM02200_7008_N6600119A0044_9700 [https://perma.cc/MAD3-RLC6]; and Palantir Technologies, "U.S. Coast Guard Renews Partnership with Palantir to Fight COVID-19," news release, May 6, 2021, https://www.palantir.com/newsroom/press-releases/us-coast-guard-renews-partnership-with-palantir-to-fight-covid-19.

336 Department of Homeland Security and Palantir Technologies Inc., delivery order, 70CTD022FR0000170, September 26, 2022, https://www.usaspending.gov/award/CONT_AWD_70CTD022FR0000170_7012_GS35F0086U_4730 [https://perma.cc/BC66-KX6L]; and Koebler, "Inside a Powerful Database ICE Uses to Identify and Deport People."

337 Department of Defense and Anduril Industries, indefinite delivery/indefinite quantity contract, H9240222D0001, January 20, 2022, https://www.usaspending.gov/award/CONT_IDV_H9240222D0001_9700 [https://perma.cc/VAJ3-DMTY]; Jackson Barnett, "Anduril Nabs $1B Contract for Anti-Drone Work with SOCOM," *DefenseScoop*, January 20, 2022, https://defensescoop.com/2022/01/20/anduril-nabs-1b-contract-for-anti-drone-work-with-socom; DOD, "Contracts for Jan. 20, 2022," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/2906241; and Colin Demarest, "Anduril Touts Pulsar Jammers That Rapidly Adapt to Changing Threats," *C4ISRNet*, May 6, 2024, https://www.c4isrnet.com/electronic-warfare/2024/05/06/anduril-touts-pulsar-jammers-that-rapidly-adapt-to-changing-threats.

338 Department of the Army and Microsoft Corporation and Anduril Industries Inc., W91CRB219P002; and Roque, "Anduril Gets Green Light from Army to Take Over Microsoft's IVAS Project."

339 A portion of this amount was obligated to Microsoft, the previous contractor.

340 Department of Defense and Anduril Industries Inc., indefinite delivery/indefinite quantity contract, M6785425D0003, March 7, 2025, https://www.usaspending.gov/award/CONT_IDV_M6785425D0003_9700 [https://perma.cc/4LP9-ZNUP]; and Anduril Industries, "Anduril Awarded 10-Year $642M Program of Record to Deliver CUAS Systems for U.S. Marine Corps," March 12, 2025, https://www.anduril.com/news/anduril-awarded-10-year-642m-program-of-record-to-deliver-cuas-systems-for-u-s-marine-corps.

341 Department of Defense and Anduril Industries Inc., N0016425CJR94.

342 Immediate Office of the Secretary of Defense and Anduril Industries Inc., other transaction agreement, HQ08832590001, accessed February 6, 2026, https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=HQ08832590001+9700 [https://perma.cc/K9VC-VURJ]; and Anduril Industries, "CDAO Awards Anduril Production Agreement to Deliver Edge Data Mesh," December 2, 2024, https://www.anduril.com/news/cdao-awards-anduril-production-agreement-to-deliver-edge-data-mesh.

343 Immediate Office of the Secretary of Defense and Anduril Industries Inc., other transaction agreement, HQ08452490015, accessed January 22, 2026, https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=HQ08452490015+9700 [https://perma.cc/4MNA-VN3Z]. This contract is likely with the DIU. See Anduril Industries, "DIU Awards Anduril Contract to Innovate New Capabilities for Undersea Warfare"; and Megan Eckstein, "Pentagon Tech Hub Hires Anduril to Get Large Underwater Drone to Navy," *DefenseNews*, February 8, 2024, https://www.defensenews.com/unmanned/2024/02/08/pentagon-tech-hub-hires-anduril-to-get-large-underwater-drone-to-navy.

344 Department of Defense and Anduril Industries Inc., definitive contract, FA882321C0002, July 26, 2021, https://www.usaspending.gov/award/CONT_AWD_FA882321C0002_9700_-NONE-_-NONE- [https://perma.cc/QUS3-AYD9]; DOD, "Contracts for July 12, 2023," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/3456563; DOD, "Contracts for Nov. 15, 2024," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/3966753; and Anduril Industries, "Anduril Awarded Program of Record Contract to Modernize Space Surveillance Network," November 20, 2024, https://www.anduril.com/article/anduril-awarded-program-of-record-space-surveillance-network.

345 Department of Homeland Security and Anduril Industries Inc., 70B02C20D00000019; and Anduril Industries, "Anduril Deploys 300th Autonomous Surveillance Tower."

346 Immediate Office of the Secretary of Defense and Saildrone Inc., other transaction agreement, HQ08452290030, accessed January 22, 2026, https://www.fpds.gov/ezsearch/fpdsportal?indexName=awardfull&templateName=1.5.3&s=FPDS.

GOV&q=HQ08452290030+&x=0&y=0 [https://perma.cc/PHL9-Z2WX]; and DIU, "Saildrone Inc — Persistent Maritime ISR," accessed January 22, 2026, https://www.diu.mil/solutions/portfolio/catalog/a0Tt0000009EnAHEA0-a0ht000000AQtkPAAT [https://perma.cc/NHL4-T4JU].

347 Department of the Navy and Saildrone Inc., other transaction agreement, N000142492005, accessed January 22, 2026, https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=N000142492005+9700 [https://perma.cc/8NNM-N2AP]; and Devin Coldewey, "Saildrone's First Aluminum Surveyor Autonomous Vessel Splashes Down for Navy Testing," *TechCrunch*, March 6, 2024, https://techcrunch.com/2024/03/06/saildrones-first-aluminum-surveyor-autonomous-vessel-splashes-down-for-navy-testing.

348 Department of the Navy and Martin UAV LLC, other transaction IDV, N004212190022, accessed January 22, 2026, https://www.fpds.gov/ezsearch/fpdsportal?s=FPDS.GOV&templateName=1.5.3&indexName=awardfull&q=N004212190022+9700+ [https://perma.cc/H883-B464]; Shield AI, "Martin UAV Kicks Off MTUAS Increment 2 Effort with Naval Air Warfare Center Aircraft Division," news release, November 16, 2021, https://shield.ai/martin-uav-kicks-off-mtuas-increment-2-effort-with-naval-air-warfare-center-aircraft-division; and Anna Miskelley, "BRIEFER: Shield AI V-BAT," *Defense and Security Monitor*, February 10, 2025, https://dsm.forecastinternational.com/2025/02/10/briefer-shield-ai-v-bat.

349 Department of the Navy and Shield AI Inc., other transaction agreement, N000192490020, accessed February 6, 2026, https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=N000192490020+9700 [https://perma.cc/F2ZC-WTFB]; and Naval Air Systems Command, "Navy Partners with Shield AI to Enhance Autonomy in Naval Aviation," August 27, 2024, https://www.navair.navy.mil/news/Navy-partners-Shield-AI-enhance-autonomy-naval-aviation/Tue-08272024-1237.

350 Department of Homeland Security and Shield AI Inc., indefinite delivery/indefinite quantity contract, 70Z02324D93130001, June 26, 2024, https://www.usaspending.gov/award/CONT_IDV_70Z02324D93130001_7008 [https://perma.cc/5MKJ-5G44]; and Shield AI, "Shield AI's V-BAT Selected for $198 Million Contract to Provide U.S. Coast Guard with Maritime Unmanned Aircraft System Services."

351 Department of the Army and Applied Intuition Inc., other transaction IDV, W15QKN2395025, accessed January 22, 2026, https://www.fpds.gov/ezsearch/fpdsportal?s=FPDS.GOV&templateName=1.5.3&indexName=awardfull&q=W15QKN2395025+9700+ [https://perma.cc/ZLH6-C35A]; and Applied Intuition Defense, "Army Selects Applied Intuition to Accelerate Autonomy Development for Robotic Combat Vehicle."

352 Immediate Office of the Secretary of Defense and Applied Intuition Inc., other transaction agreement, HQ08832490001, accessed January 22, 2026, https://www.fpds.gov/ezsearch/search.do?indexName=awardfull&templateName=1.5.3&s=FPDS.GOV&q=HQ08832490001+9700+ [https://perma.cc/9YNM-3Q7T]; and Courtney Albon, "Applied Intuition Acquires AI Software Firm EpiSci," *DefenseNews*, February 6, 2025, https://www.defensenews.com/air/2025/02/06/applied-intuition-acquires-ai-software-firm-episci.

353 US intelligence agency contracts — including their contract IDs and obligated and ceiling amounts — are generally not reported on public government procurement websites. This ceiling amount is drawn from the National Geospatial-Intelligence Agency's press release. NGA, "NGA Announces $708M Data Labeling RFP"; Enabled Intelligence, "Enabled Intelligence Awarded NGA's $708 Million SEQUOIA Contract for AI/ML Data Labeling-as-a-Service," news release, November 24, 2025, https://enabledintelligence.net/press/enabled-intelligence-awarded-ngas-708-million-sequoia-contract-for-ai-ml-data-labeling-as-a-service; and Manson, "Scale AI Loses to Smaller Startup in Bid for US Intel Work."

354 Department of Defense and Scale AI Inc., indefinite delivery/indefinite quantity contract, SP470124D0004, September 27, 2024, https://www.usaspending.gov/award/CONT_IDV_SP470124D0004_9700 [https://perma.cc/Q6W6-Z3ZU]. It is unclear whether this agreement is linked to Scale AI's testing and evaluation partnership with CDAO. Scale AI, "Scale AI Partners with DoD's Chief Digital and Artificial Intelligence Office (CDAO) to Test and Evaluate LLMs," February 20, 2024, https://scale.com/blog/scale-partners-with-cdao-to-test-and-evaluate-llms.

355 Department of Defense and Scale AI Inc., definitive contract, W911QX20C0051, September 29, 2020, https://www.usaspending.gov/award/CONT_AWD_W911QX20C0051_9700_-NONE-_-NONE- [https://perma.cc/C9M6-FSWS]; and DOD, "Contracts for Sept. 29, 2020," accessed January 22, 2026, https://www.defense.gov/News/Contracts/Contract/Article/2365695/#SCALEAI092920.

356 DOD, "DOD Releases Fiscal Year 2020 Budget Proposal," news release, March 12, 2019, https://www.defense.gov/News/Releases/Release/Article/1782623/dod-releases-fiscal-year-2020-budget-proposal.

357 DOD, "DOD Releases Fiscal Year 2021 Budget Proposal," news release, February 10, 2020, https://www.defense.gov/News/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal.

358 DOD, "The Department of Defense Releases the President's Fiscal Year 2022 Defense Budget," news release, May 28, 2021, https://www.defense.gov/News/Releases/Release/Article/2638711/the-department-of-defense-releases-the-presidents-fiscal-year-2022-defense-budg.

359 In its news release, the DOD did not report specific budget request figures for AI, AI-related, or autonomy categories for FY 2023. DOD, "The Department of Defense Releases the President's Fiscal Year 2023 Defense Budget," news release, March 28, 2022, https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg. The FY 2023 defense budget overview, however, notes that the budget request for AI was $1.1 billion. Office of the Undersecretary of Defense (Comptroller)/Chief Financial Officer, *Defense Budget Overview: United States Department of Defense Fiscal Year 2023 Budget Request*, April 2022, 4–7, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.

360 DOD, "Department of Defense Releases the President's Fiscal Year 2024 Defense Budget," news release, March 13, 2023, https://www.defense.gov/News/Releases/Release/Article/3326875/department-of-defense-releases-the-presidents-fiscal-year-2024-defense-budget; and Jon Harper, "Pentagon Requesting More Than $3B for AI, JADC2," *DefenseScoop*, March 13, 2023, https://defensescoop.com/2023/03/13/pentagon-requesting-more-than-3b-for-ai-jadc2.

361 DOD, "Department of Defense Releases the President's Fiscal Year 2025 Defense Budget," news release, March 11, 2024, https://www.defense.gov/News/Releases/Release/Article/3703410/department-of-defense-releases-the-presidents-fiscal-year-2025-defense-budget; and Brandi Vincent, "Why the Pentagon Didn't Request Higher Funding for AI in Fiscal 2025," *DefenseScoop*, March 11, 2024, https://defensescoop.com/2024/03/11/pentagon-ai-budget-request-2025.

362 Senior Defense Official and Senior Military Official, "Transcript: Background Briefing on FY 2026 Defense Budget."

363 Jon Harper, "Lt. Gen. Caine, Trump's Nominee for Joint Chiefs Chairman, Is Gung-Ho About Commercial Tech," *DefenseScoop*, April 1, 2025, https://defensescoop.com/2025/04/01/dan-caine-joint-

chiefs-chairman-trump-entrepreneur-commercial-technology. See also Andrew deGrandpre and Kelsey Ables, "Dan Caine Confirmed by Senate to Become Trump's Joint Chiefs Chairman," *Washington Post*, April 11, 2025, https://www.washingtonpost.com/national-security/2025/04/11/dan-caine-joint-chiefs-trump.

364 Anastasia Obis, "Feinberg Says His Private Equity Background Positions Him to Fix Pentagon," Federal News Network, February 25, 2025, https://federalnewsnetwork.com/defense-main/2025/02/feinberg-says-his-private-equity-background-positions-him-to-fix-pentagon; and Nomination of Stephen Feinberg, PN12-16, 119th Congress (2025), https://www.congress.gov/nomination/119th-congress/12/16.

365 Eric Bazail-Eimil, "Trump Picks China Hawk to Be Top State Department Economic Policy Official," *Politico*, December 10, 2024, www.politico.com/live-updates/2024/12/10/congress/trump-picks-china-hawk-helberg-to-be-top-state-department-economic-policy-official-00193683. See also Nomination of Jacob Helberg, PN12-21, 119th Congress (2025), https://www.congress.gov/nomination/119th-congress/12/21.

366 Filip Timotija, "Senate Confirms Michael Kratsios to Lead White House Science, Tech Office," *Hill*, March 25, 2025, https://thehill.com/policy/technology/5213986-senate-confirms-michael-kratsios-white-house-science-tech-office.

367 Kyle Wiggers, "Sriram Krishnan Named Trump's Senior Policy Advisor for AI," *TechCrunch*, December 22, 2024, https://techcrunch.com/2024/12/22/sriram-krishnan-named-trumps-senior-policy-advisor-for-ai.

368 U.S. Office of Personnel Management, "OPM Director Scott Kupor," accessed January 22, 2026, https://www.opm.gov/about-us/who-we-are/opm-director-scott-kupor. See also Nomination of Scott Kupor, PN12-24, 119th Congress (2025), https://www.congress.gov/nomination/119th-congress/12/24.

369 Jon Harper, "Trump Nominates Anduril Executive, Former Special Operations Office to Be Army Undersecretary," *DefenseScoop*, March 11, 2025, https://defensescoop.com/2025/03/11/trump-nominates-michael-obadal-army-undersecretary-anduril. See also Nomination of Michael Obadal, PN26-35, 119th Congress (2025), https://www.congress.gov/nomination/119th-congress/26/35.

370 Julia Shapero, "Who Is David Sacks, Trump's Crypto and AI Chief?," *Hill*, December 6, 2024, https://thehill.com/policy/technology/5026959-venture-capitalist-david-sacks-white-house.

ABOUT THE AUTHORS

▶ **Amos Toh** is senior counsel and manager in the Brennan Center's Liberty and National Security Program. He was previously the senior researcher on artificial intelligence and human rights at Human Rights Watch, where he led investigations into AI's impact on public services and platform work. Between 2015 and 2019, he served as legal adviser to the United Nations special rapporteur on the right to freedom of opinion and expression.

▶ **Emile Ayoub** is senior counsel in the Brennan Center's Liberty and National Security Program. His work focuses on surveillance and the impact of technology on civil rights and civil liberties. His research and commentary have been featured in outlets such as Bloomberg, *The Washington Post*, and *The Intercept*. Ayoub is a graduate of the University of California, Los Angeles, and the University of California, Irvine School of Law.

ACKNOWLEDGMENTS

The Brennan Center extends deep gratitude to supporters of our work, who made this report and all our work possible. See them at brennancenter.org/supporters.

The authors would like to thank the Brennan Center's Faiza Patel, John Kowal, and Michael Waldman for their leadership and invaluable guidance, comments, and suggestions; Matthew Ruppert, Melanie Geller, Kaitlyn Rentala, and Naz Balkam for research, cite-checking, and editing; Benjamin Nyblade and Jia Zhang for their analysis and visualizations of defense procurement data; and Marcelo Agudo and Julian Brookes for their expert guidance in communicating our findings to policymakers and a broader audience.

We are also grateful to Jack Poulson for his meticulous research, reporting, and expertise on defense procurement and to Meredith Berger, Julia Gledhill, William Hartung, Heidy Khlaaf, Elisa Miller, Sarah Myers West, and Daniel Weiner for their thoughtful review and feedback on drafts of this report.

BRENNAN CENTER FOR JUSTICE

Brennan Center for Justice at New York University School of Law
120 Broadway // 17th Floor // New York, NY 10271
brennancenter.org