Tech Scouting
Future at Your Fingertips

Booz Allen®

TOP 10 EMERGING TECHNOLOGIES FOR THE DOD AND NATIONAL SECURITY

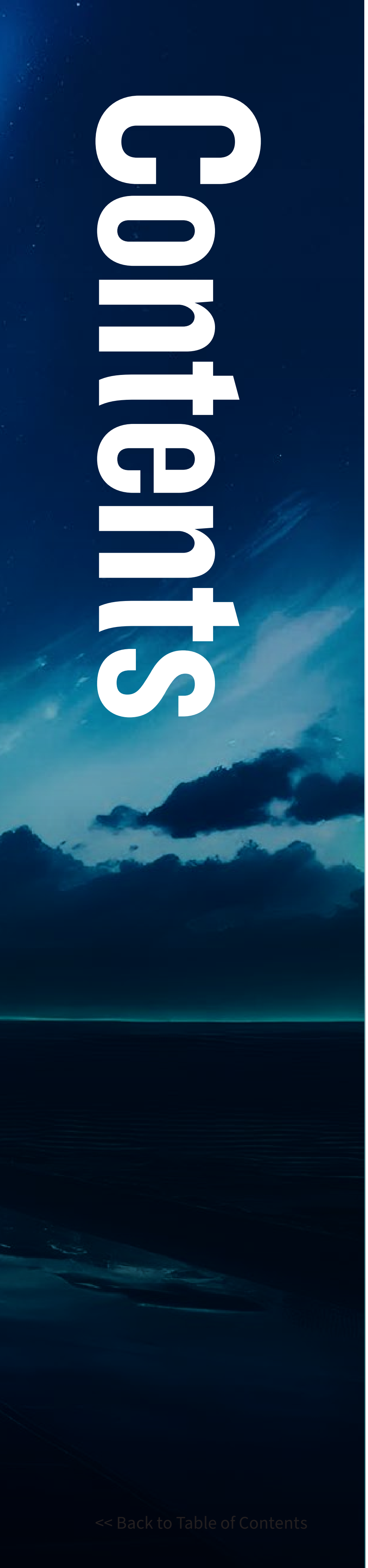
MAY 2024

Velocity **Magazine: Special Edition Report**

"The world order is shifting and the greatest technological competition of our lifetimes is upon us. To maintain technological supremacy in the midst of Great Power Competition with China, the U.S. defense and national security sector has a duty to foster and integrate the U.S.'s greatest strength: our commercial tech industry."

–Brian MacCarthy
Senior Vice President,
Head of Booz Allen Tech Scouting and Ventures

Contents



<< Back to Table of Contents

> **The technology innovation strategies of the Cold War and counterterrorism eras focused on research and development (R&D) of large-scale hardware and weapons systems. As today’s threat environment shifts, the U.S. needs a more strategic approach to successfully harness the technologies of the future.**
>
> **– Susan Penfield**
> Chief Technology Officer, Booz Allen Hamilton

In a time of escalating global tension, technological innovation provides an essential lever for both defense and deterrence. With powerful disruptions coming into focus almost daily, nations that quickly develop, integrate, and deploy emerging technology to support high-stakes national defense missions can expect to dominate the current and future battlefield.

But what does it take to realize a technological asymmetric advantage? The technology innovation strategies of the Cold War and counterterrorism eras focused on research and development (R&D) of large-scale hardware and weapons systems. As today's threat environment shifts, the U.S. needs a more strategic approach to successfully harness the technologies of the future.

For the Department of Defense (DOD) and Intelligence Community (IC), addressing this challenge increasingly means rapidly identifying, adopting, prototyping, and fielding dual-use commercial technology. Fortunately, the resources DOD needs are already at its fingertips: The U.S. is home to far and away the largest, most dynamic, and most innovative technology ecosystem in the world. It is one of our nation's most valuable resources, yet one that is severely underutilized by DOD—to its detriment. A further challenge is the need to make hard choices: prioritizing which of the many powerful technologies and innovative companies to develop and field.

Booz Allen Tech Scouting is releasing *Top 10 Emerging Technologies for the DOD and National Security* to call attention to the technologies our research says should be prioritized in the near term. With tech sectors advancing in all directions and with defense buying power declining (or at least uncertain), DOD must spend its limited resources wisely and in the most impactful ways possible. This means not just prioritizing technology areas, but also placing big bets on winning commercial partners rather than diluting funding across so many players that none can make it through the Valley of Death.

Here we explore 10 dual-use technologies—from autonomous swarms and post-quantum cryptography to space domain awareness tech and more—that we see as critical for our defense clients to harness over the next several years, as well as the key trends defense leaders should be aware of as the landscape continues to evolve. In addition, we highlight promising emerging startups that are disrupting legacy systems and could usher in a new future, both for commercial and military applications.

Booz Allen has been honored to serve as a close advisor to DOD for decades. Today, I invite you to explore this report and join us in assessing exactly how emerging technology can support your enduring mission of keeping the nation secure.

Thank you,

Susan Penfield

Chief Technology Officer
Booz Allen Hamilton

Introduction & Methodology

Introduction

Emerging technology is a critically important aspect of modern defense and deterrence—a field being disrupted daily, as evidenced in recent global conflicts. In Eastern Europe, Ukraine's integration and use of innovative commercial technology—such as drones, artificial intelligence (AI), and cyber tools—enabled an initial level playing field that not many imagined possible during the Russian military buildup. A few years earlier, in 2020, Azerbaijan's decisive victory over Armenia was the first war to be won primarily by robotic systems rather than humans, according to military analyst John Antal. Moreover, Israel's victory over Hamas in 2021 was the first war to be won via the asymmetric advantage provided by AI, and the conflict in Gaza that started in 2023 continues to be characterized by AI as well as information warfare in the cognitive domain.

There are many technical lessons to be learned from these campaigns, some of which we will unpack in the subsequent technology sections. **However, the most important lesson from these conflicts may be that success in modern warfare goes to those who rapidly exploit emerging technologies into combat operations.** Ukraine, Azerbaijan, and Israel have all prioritized agility and flexibility in acquiring and deploying new technology, which have proved to be key factors in battlefield success and resiliency.

As the U.S. studies these conflicts and evaluates its global military standing and strategic objectives, China looms as a daunting competitor with technological prowess and outsized ambition. As a state power, China strives to reorganize the world order and advance its economic and political interests globally—an outcome which threatens U.S. primacy and is a dramatic shift from the recent counterterrorism era. To bolster its capabilities and influence, China has invested in a multitude of emerging technologies—including AI, autonomy, and hypersonics—with the innovation largely being driven by civil-military fusion, intellectual property (IP) theft, and state-driven directives and priorities.

As a result, the U.S. is facing a type of threat it has not seen since the Cold War: a near-peer technological competitor. As tensions rise and both sides participate in an emerging technological arms race to deter escalation, the U.S. must field the most impactful new technologies into its defense systems to create the most capable military force possible. The question remains: What are those technologies, and how do the U.S. Department of Defense (DOD) and national security agencies identify them in the context of their very specific mission needs?

DOD has always understood the need to ingest and understand high-fidelity information from a variety of sources to improve high-stakes decision making. **Today, the need for that type of pervasive intelligence extends beyond the battlefield and into the commercial market. Much of the best technologies in the world are currently developed by and for the private sector, and U.S. entrepreneurs and investors work together to create what is likely the country's greatest global competitive advantage: technological innovation at speed.** In many cases, it is this dual-use innovation of fielding commercial technology for software-defined military operations (rather than singular billion-dollar hardware or weapon systems) that holds the promise of unlocking new capabilities that scale and deter global conflict. The reality is that the technology and acquisition strategies deployed during the Cold War and counter-terrorism eras, which largely focused on internal defense research and development (R&D) reliant on defense prime contractors, are not sufficient to adequately transform the U.S. military to deter and defend against today's constantly evolving threats.

Therefore, it is in DOD's best interest to fully harness the power of private sector innovation. Unfortunately, understanding and adopting novel technology for force transformation is complex—it requires proficiency in both technology and mission innovation, two sometimes disparate ecosystems spanning from the Pentagon to Silicon Valley and many places in between. Making things more difficult, emerging technology ecosystems are riddled with uncertainty, instability, and hype—all sworn enemies of traditional defense acquisition cycles. And the consequences of these choices are huge: Public and private investment decisions today will determine which enabling technologies warfighters have to protect the U.S. in tomorrow's conflicts.

To meet the challenges of the modern battlefield, these ecosystems must form a high-functioning partnership, one that is well informed on the threats, the strategic imperatives to address them, and the opportunities for technology to provide new asymmetric advantages. **It is for these reasons that Booz Allen's Tech Scouting exists: to actively monitor the technology landscape and guide government agencies through the intricate patchwork of people, companies, and investors that power the startup market.** In partnership with U.S. federal clients, we find and vet emerging and transformational capabilities that are best positioned to advance the nation's security and competitive advantage across the technology ecosystem.

The goal of this report is to highlight the emerging dual-use technologies that will be increasingly significant and impactful for DOD and the battlefield over the next one to three years. We aim to do that by:

- Providing clarity on the underlying technologies
- Helping defense stakeholders make sense of and prioritize the ever-expanding labyrinth of emerging technologies, ecosystems, and nomenclature
- Illuminating how the emerging trends and associated early innovators may have major implications in the future battlespace

By weeding through the noise of constant technology updates and new entrants to the ecosystem, our hope is to arm defense stakeholders with the vetted and reliable information necessary to harness emerging technology. Booz Allen has been a trusted advisor to DOD for 110 years, and the goal has always been the same: to support U.S. federal clients' most critical missions. We believe these technologies to be essential in that endeavor.

Methodology

Highlighting Ecosystems

INITIAL SCOPING: To start our analysis, we reviewed public DOD and other federal agency reports outlining emerging technology priorities. For example, DOD Chief Technology Officer (CTO) Heidi Shyu's *Critical Technologies* report highlights 14 critical and emerging technologies for the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]). The Defense Information Systems Agency (DISA) publishes technology watchlists as well. **These stated priorities, in conjunction with insight from Booz Allen Tech Scouting, mission experts, federal client requests, and venture analysis created a starting menu of technology areas from which to select topics.**

From there, we broke down umbrella terms into better-defined ecosystems. For example, it is challenging to find someone who disagrees with "Trusted AI and Autonomy" being a pillar of OUSD(R&E)'s tech list—but what type of AI? On which systems? For what use case?

There are many right answers, but our goal was to help readers understand the specific technologies and use cases at hand by creating manageable bounds for the ecosystems. "Generative AI for Software Development" and "Autonomous Swarms" are presumably easier to understand on a granular level than AI and autonomy in general. **Research was conducted by using subscription-based tools, open-source intelligence, and networks of subject matter experts (SMEs) both inside and outside Booz Allen.**

DOWN-SELECTION: We down-selected ecosystems as we analyzed projected impact and time to inflection for our list of technologies. **We spoke with more than 20 Booz Allen executives, technical advisors, and SMEs to curate thoughts, experiences, and client/mission knowledge on the sub-ecosystems, capturing tech definitions, maturity levels, and mission relevance.** These themes were then quantified in a standardized survey (included in the appendix) addressing five base criteria: Technology Readiness Level (TRL), defense impact, defense implementation speed, commercial impact, and market momentum. The results for each ecosystem are highlighted in the executive summary page for each section.

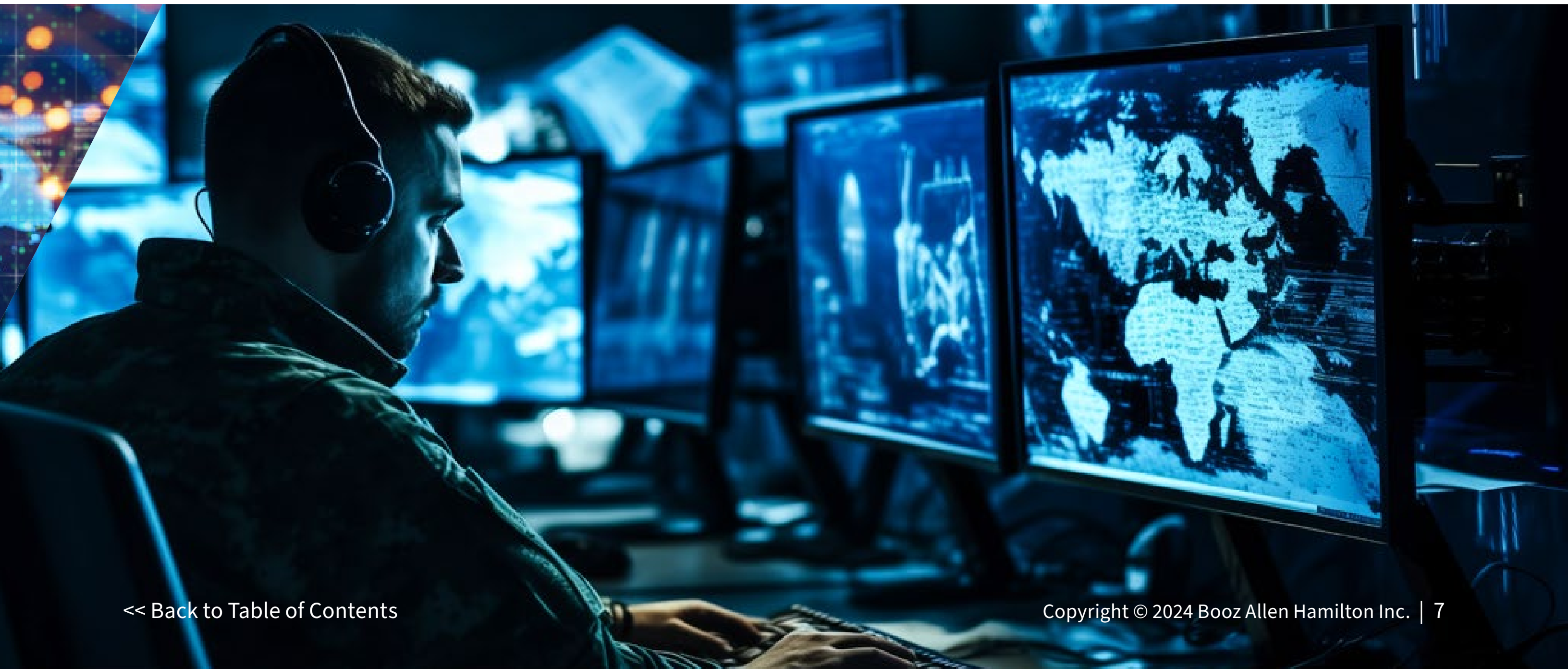
Through this analysis, technologies emerged which:

- Fall under DOD's stated priorities
- Are novel and disruptive
- Are projected to provide significant defense impact in the next one to three years

We gave preference to ecosystems with dual-use capabilities (public and private sector applications), which often attract more startups that are rapidly innovating and attracted to steady cash flow. However, certain technologies, such as hypersonics, were deemed important enough to the defense space to include even without significant private sector traction. **The ecosystems included are non-exhaustive—our team believes the highlighted technologies will have important future impact but are not representative of every technological trend of significance in the years to come.**

In addition, not every technology included in this list is brand new—much of the innovative process deals with overcoming hurdles to adoption, and tech that may be more mature in the private sector can still be novel for governmental mission and impact. Of note, PitchBook charts and compound annual growth rate (CAGR) values were calculated solely for pure-play companies rather than investments from large, diversified conglomerates like the Big Tech players. Therefore, this data is likely an underrepresentation and sampling of the true investment and growth values. Finally, most ecosystems experienced down years in funding from 2022–2023, which reflects the broader industry and the result of higher interest rates and other macroeconomic conditions following the post-COVID boom rather than investor disillusion or tech pessimism.

In our diligence, we often used generative AI as an example of an ecosystem that reached a major inflection point in 2022–2023. While it falls under DOD's stated priority of fielding "trusted AI," the generative AI subcategory caught DOD (along with most of the world) by surprise when OpenAI's ChatGPT burst onto the scene in late 2022. As a result, DOD is now racing to strategize and field this new technology, which will undoubtedly have an outsized impact on future capabilities. While not



<< Back to Table of Contents

every ecosystem will evolve at this scale or exponential pace, we believe the inflection points for the technologies in this report to be similar, and therefore, worth evaluating today.

The primary purpose of each section is to focus on the impact a fully integrated technology could have on DOD, including trend analyses to speak to the evolving aspect of the technology and what makes it compelling. Visual aids and charts emphasize key points, and we highlight non-exhaustive lists of emerging innovators, which may be of interest to government customers. Technologies are listed alphabetically and not by order of importance.

HIGHLIGHTING STARTUPS

Tech Scouting regularly highlights emerging startups for U.S. federal clients. Due to varying requirements and criteria, there is no exact scorecard for evaluation. Instead, our team looks holistically at factors such as:

- Technical merit and differentiation
- Leadership acumen and experience
- Commercial traction
- Investor backing
- Foreign influence
- U.S. government (USG) traction

Selecting an appropriate partner or commercial off-the-shelf (COTS) solution for a defense mission is inherently driven by an organization's specific requirements and scenarios. In our analysis, we aimed to highlight companies that address some of those key requirements and scenarios, but these are not the only applicable companies or necessarily the best ones for the reader's use cases.

The company highlights do not represent absolute market leaders. Rather, they represent a distribution of compelling startups that are cutting edge in their respective fields—their capabilities are novel, futuristic, and a sampling of what is possible.

We highlighted domestic, earlier-stage startups that fit the initial criteria to be innovation partners for defense customers. Factors such as product TRL, dual-use potential, projected market size, and information availability were also used as benchmarks.

SUMMARY

Emerging technology is a key element in the future of warfare, and the aim of this report is to be an introductory roadmap for those trying to understand it. Our assertions are based on technology research and mission knowledge curated from inside Booz Allen and out, from conversations with leaders from Washington, DC, to Silicon Valley. Some of the ecosystems highlighted in this report will be more impactful than others—extrapolation and prediction are no friends of accuracy. However, an objective of this report is to reinforce that those things are not only okay but necessary. DOD's only choice is to move fast and integrate emerging technology, be willing to divest where necessary, double down on success, welcome fresh opinions, and move urgently toward a future that hinges on innovation. We hope this report aids in that endeavor.

Methodology for Selecting the 10 Highlighted Technologies

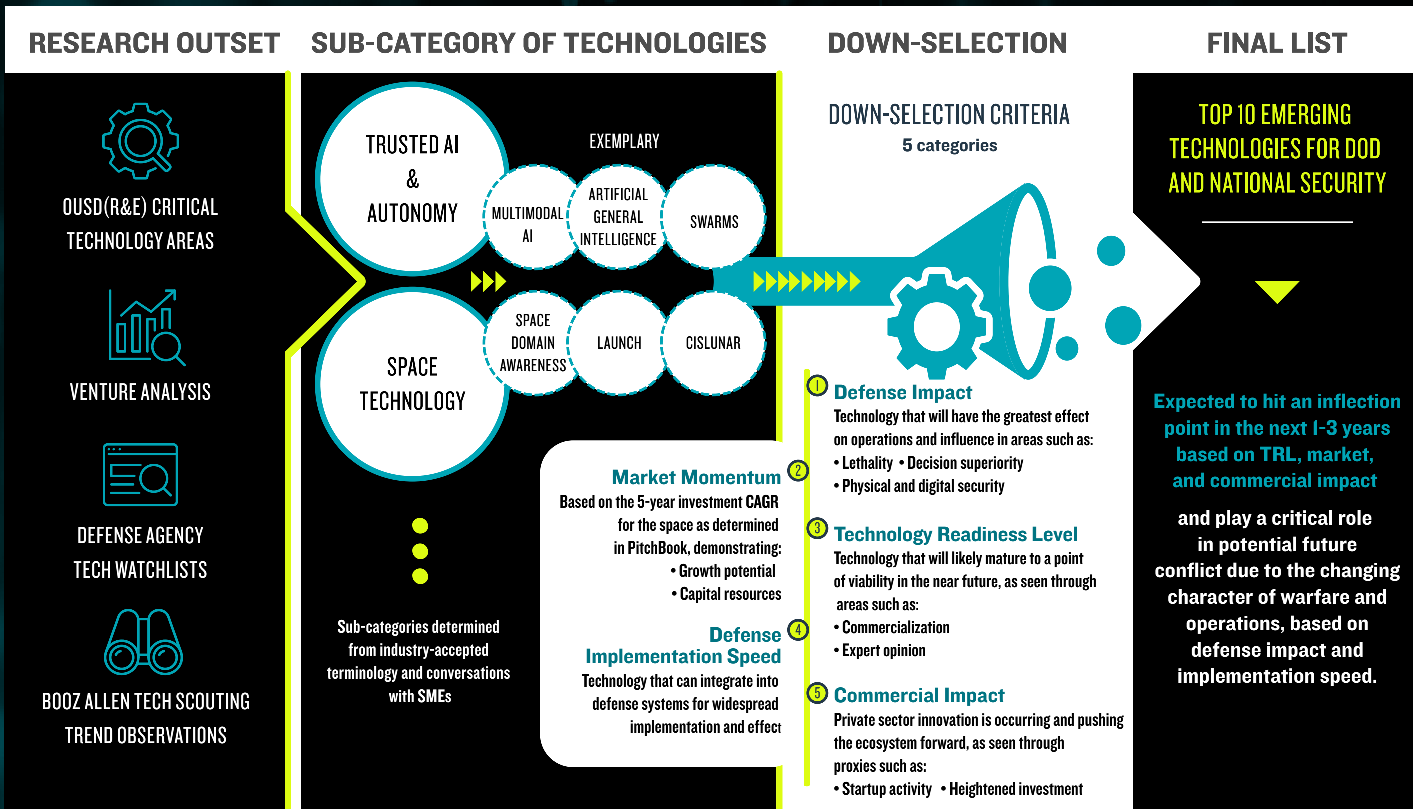


Figure 1: *The methodology above was used to down-select to 10 highlighted technology ecosystems. This list is exemplary and non-exhaustive. Qualitative and quantitative data were used to derive insights, with input from both Booz Allen internal and external experts.*

<< Back to Table of Contents

Report Guide

Booz Allen believes that evaluating and integrating emerging technology empowers U.S. federal clients to meet the evolving challenges that confront our nation. This report identifies 10 emerging technology ecosystems we believe to be critical for defense clients to adopt and harness in the near- to mid-term. Analysis includes an ecosystem definition, technical breakdown, strategic insight, and a look at potential outcomes.

HOW SHOULD I USE THIS REPORT?

This report is intended to inform strategy, direct technology research and integration, shape technology roadmaps, identify leading companies and disruption, and support U.S. federal clients in exploring potential use cases when targeting mission requirements.

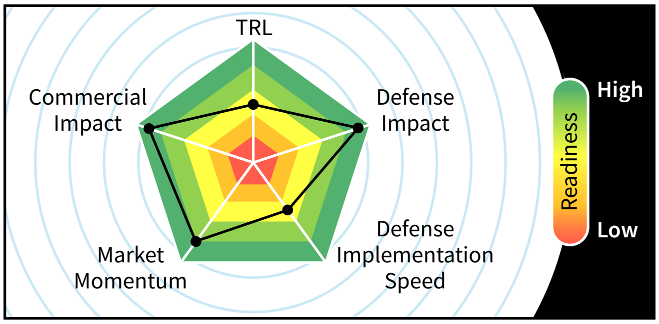
WHAT'S INCLUDED IN EACH TECHNOLOGY SECTION?

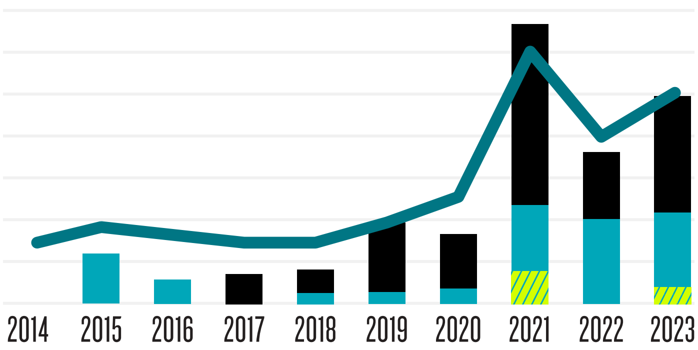
- **Summary page:** A quick look at the key points for each technology
- **Narrative analysis:** A written summary of the technology, including its definition, technical breakdown, strategic insight, and future impact
- **Company highlights:** Profiles of emerging, generally early-stage startups in the space

WHAT ARE THE RADAR CHARTS?

Radar and investment analysis charts, along with other intermixed graphics, are included to shed light on the technology's maturity, growth, implementation speed, projected impact, and market trends.

Radar chart values were derived from surveys distributed to Booz Allen experts. For the survey language and definitions, see page 76 in the appendix. For a side-by-side comparison of tech ecosystem radar charts, visit page 77.





WHAT ARE THE INVESTMENT CHARTS?

Investment charts show global, pure-play market growth using PitchBook search terms. Figures are proxies and inexact, often skewing downward because they do not include the large defense primes or Big Tech players (for which data on specific technology investments is not available). Due to low interest rates and the injection of government money, investment numbers tend to spike from 2020 to 2022.

Definitions of acronyms appearing in the investment charts are:

- IPO: Initial public offering
- M&A: Mergers and acquisitions
- PIPE: Private investment in public equity
- VC: Venture capital

 |

Emerging Technology Areas

Technologies are listed alphabetically and not in order of importance.

AI Accelerator Chips

These semiconductor chips are designed specifically for speeding up AI/ML computations and lowering their energy requirements, which are especially critical when running AI and LLM applications at the edge.

Alternative Position, Navigation, and Timing

Vulnerabilities in existing GPS-based PNT technologies have created a need for more secure, robust alternatives.

Autonomous Swarms

Multiple robots with local processing, communication, and sensing capabilities can be interconnected and programmed to react to the environment autonomously in a disaggregated but synchronized fashion.

Generative AI Software Development

The use of specially designed AI/ML to review, edit, and write software can offload all or much of the task of coding from humans, as well as potentially reduce bugs and security flaws.

High-Density Energy Storage

New chemistries have paved the way for next-gen batteries with significantly higher energy density, allowing for much greater energy output in smaller form factors.

Hypersonics

Vehicles that fly five times faster than the speed of sound can enable quicker access to space, rapid military response over long ranges, and faster commercial air travel.

Multimodal AI

AI systems that ingest and analyze numerous data types in tandem can better interpret context and deliver more accurate insights.

Non-Kinetic Counter-UAS

This subset of c-UAS focuses on disabling small- and medium-sized drone threats using effectors such as radio frequency jamming, cyber takeover, or directed energy.

Post-Quantum Cryptography

New mathematical algorithms for public-key encryption must be defined and implemented today to resist attacks from quantum computers in the future.

Space Domain Awareness Tech

The monitoring of active satellites and debris is key to maintaining the situational awareness and safety of the space operating environment.

<< Back to Table of Contents

1. AI Accelerator Chips

> **The global race for AI is on with decisive implications from the boardroom to the battlefield. The ground upon which this race will be won is the next generation of chips powering breakthrough AI capability at the edge.**
>
> **– Zach Beecher**
> America's Frontier Fund

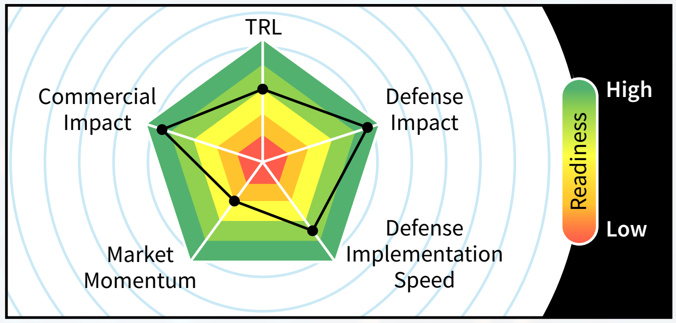
Executive Summary

Definition: AI accelerator chips ("AI chips") are specialized microelectronic hardware devices that speed up and optimize the processing of AI/machine learning (ML) software models. This function is especially critical for large language models (LLMs) and AI at the edge, where current graphics processing units (GPUs) are extremely expensive and limited in their compute efficiency. Here, we focus on beyond-GPU architectures for our analysis.

Technology: AI chips come in several varieties, typically with a tradeoff between the power efficiency and speed with which they can run their operations and the flexibility in the models they can run. Custom von Neumann and non-von Neumann application-specific integrated circuits (ASICs) and photonic data transmission links are experiencing a renaissance in innovation and will likely revolutionize the AI industry.

Strategic Insight: The pace of AI progress might depend on new chip designs and supply chains. Moreover, in the face of rising geopolitical tensions over Taiwan—where most AI chips are produced—the U.S. Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act represents a key effort to reinstate U.S. leadership in semiconductors. DOD can leverage this and other funding to pursue next-generation devices that will greatly enhance tactical decision making and military resiliency in the field.

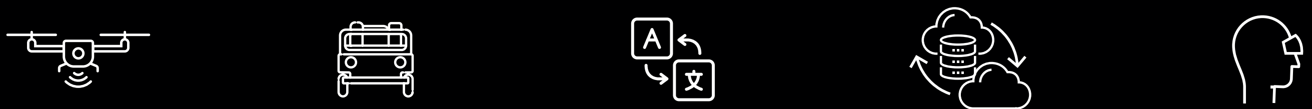
Future: In the near term, edge applications could undergo major disruption, such as high-fidelity computer vision (CV) on unmanned aerial systems (UASs) or real-time translation using natural language processing (NLP) in head-mounted displays. Ultimately, as chips become ever more "brain-like," their abilities will begin to rival the human brain, and even highly complex models like LLMs could be run in low size, weight, and power (SWaP) environments.



Essential Hardware for Computing at the Tactical Edge

AI chips are computing chips that speed up the processing of AI/ML applications. While traditional central processing units (CPUs) are ideally suited for sequential, high-precision calculations, AI chips are designed for the kind of low-precision matrix math that characterizes the deep learning models needed to power critical, dual-use applications, such as autonomous vehicles, big data analysis and visualization, and generative chatbots. In particular, AI chips are essential for running AI models at the edge—a large and growing need for DOD.

USE CASES



Computer Vision at the Edge | Autonomous Vehicles | Real-Time Language Translation | Power-Efficient Data Centers | Battlefield Augmented Reality

<< Back to Table of Contents

Technology: By far the most widely used type of AI chip today is the GPU. While GPUs are far superior to CPUs for running AI algorithms, they are, at their core, general-purpose processors designed to support a variety of applications. More targeted AI chips are being explored for still better performance. Among chips with von Neumann architectures (i.e., distinct computing, control, and memory functions), field programmable gate arrays (FPGAs) and custom ASICs are better suited to performing AI/ML calculations than GPUs, though they offer less flexibility to train and run diverse algorithms.

Even for these more advanced chips, the high cost and slow speed of moving data pose daunting barriers to efficiency. While ASICs optimize for efficient compute, they do not solve for the "von Neumann bottleneck"—the energy cost of data transfer associated with von Neumann architectures. In the long term, innovations in architecture, such as in-memory computing (IMC) or alternatives to electrical data movement, will be necessary to achieve the levels of energy efficiency required for advanced AI functions. One option, photonics, presents an attractive new approach to data transfer—both on- and off-chip—given its added benefits of speed, bandwidth, and low heat generation.

Strategic Insight: The geopolitical importance of AI chips cannot be overstated. In the ongoing Great Power Competition with China, advanced-node semiconductor devices—and the AI algorithms they enable—are the linchpin to the military and economic goals of both the People's Republic of China (PRC) and the U.S. Acutely aware of AI's national security implications, both countries are pouring billions of private and public investment dollars into AI chip hardware. Notably, U.S. export restrictions on advanced AI chips have so far stymied Chinese AI development. Meanwhile, the advanced-node foundry capabilities of Taiwan Semiconductor Manufacturing Company (TSMC), producer of feature-dense AI chips, have raised the stakes of conflict in the Taiwan Straits. In fact, indicative of AI chips' importance and Taiwanese tensions, both India and the U.K. have announced the creation of their own national AI chip stockpiles.

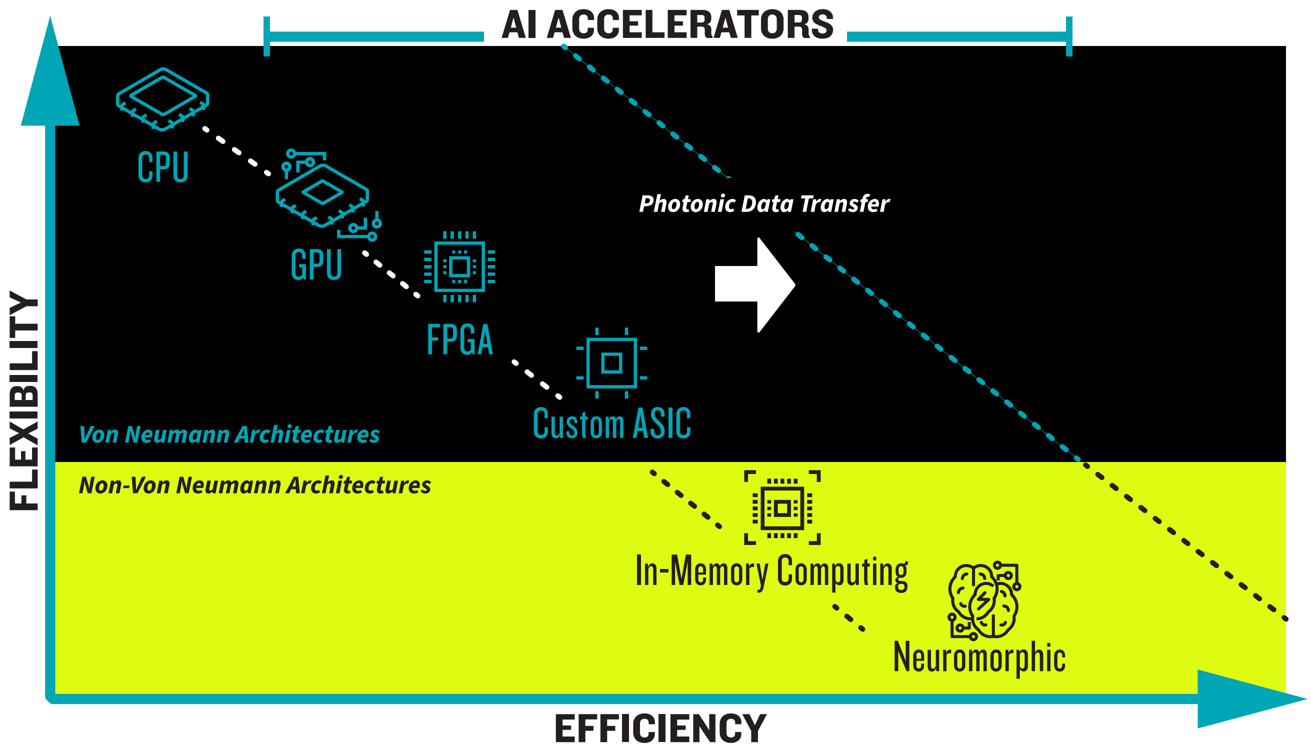


Figure 2: *From GPUs to neuromorphic chips, AI chips can be understood as existing on an architectural spectrum, with a tradeoff between flexibility in the deep learning models they can run and efficiency in performing operations. Advances in silicon photonics have the potential to drive improvements in efficiency of all types of chips.*

AI Chips Investment Trends

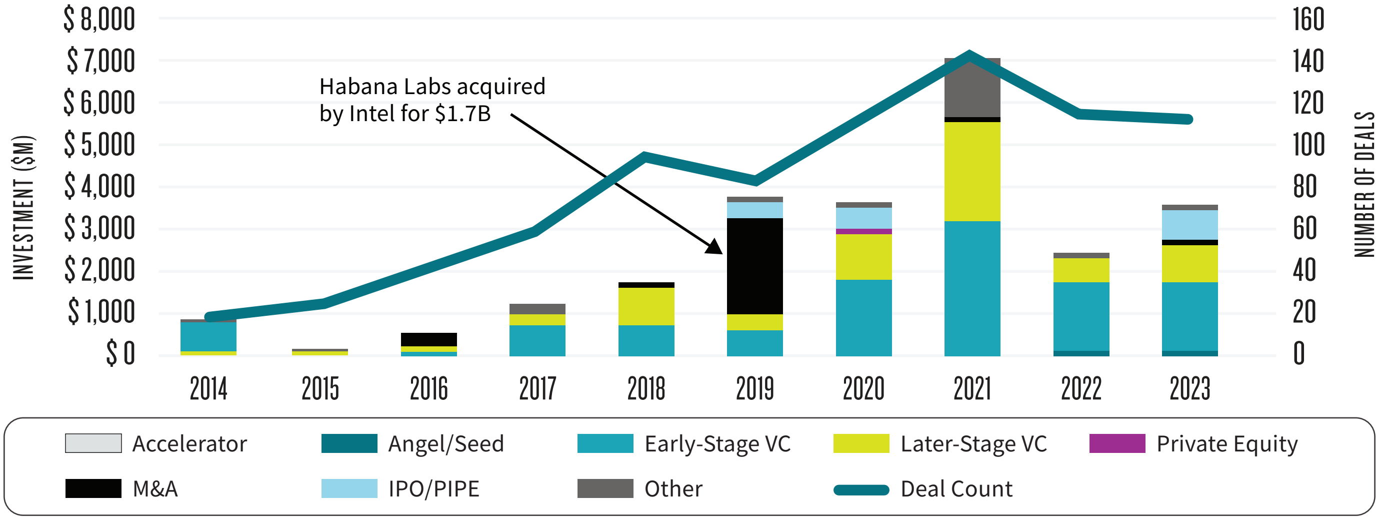


Figure 3**:** *Investment trends underscore complexities in the emerging AI chips market. Several large deals have driven much of the attention over the prior decade, in large part because of the heightened operational expenditure (OpEx) and capital expenditure (CapEx) associated with hardware development. In addition, NVIDIA and AMD have an oligopolistic market share in chip design, resulting in a "winner-take-all" mentality, and therefore, a reduction in deal flow to newer entrants in the wake of recent high-profile advancements in AI software. Note: This chart only includes companies specializing in beyond-GPU hardware, which biases the numbers downward. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

For its own part, the U.S. is increasingly taking the microelectronic geopolitical race seriously—particularly as it pertains to winning the AI race—as evidenced by the 2022 CHIPS and Science Act, recent National Defense Authorization Acts (NDAA), and a variety of Defense Advanced Research Projects Agency (DARPA) programs. For example, in September 2023 the Under Secretary of Defense, Kathleen Hicks, announced the establishment of eight innovation hubs through the CHIPS and Science Act worth a total of $238 million.

These hubs will focus on accelerating semiconductor development for AI, along with other DOD technology priorities. Regarding DARPA programs, the Electronics Resurgence Initiative (ERI), which started in 2017 and continued to spur innovation through 2023, seeks to reinvent domestic microelectronics manufacturing. Of note, ERI is working to advance AI accelerators to catalyze edge AI capabilities, which have clear warfare use cases.

Future: As AI takes over the public and defense consciousness, AI chips will become ever more essential to running sophisticated AI/ML applications, thereby offloading manual data analysis and decision making. AI chips are especially critical at the edge, where the warfighter will increasingly depend on AI and where low SWaP specifications are not optional. While current chips are unable to perform, for example, CV operations on small UASs in contested airspace, next-generation hardware could make this routine. Autonomous vehicles, augmented reality/virtual reality (AR/VR) headsets, and the internet of military things (IoMT) at the tactical edge would all be enabled by the right hardware.

In the more distant future, the ecosystem may see continued disruption with the maturation of even more efficient engines that leverage non-von Neumann architectures in which compute, control, and memory functions are deeply convolved. IMC and neuromorphic computing (consisting of spiking neural networks and analog computations) are examples of these types of systems, which take inspiration from how biological brains—themselves optimized for pattern matching of very noisy data and other low-precision but high-efficiency functions—learn and make decisions. One could even imagine a future in which LLMs could be run with low power at the edge, a feat unimaginable with today's hardware. Before the close of this century, the brains of our machines may achieve form and functionality increasingly akin to the brains in our heads—opening the door to new and untapped defense potential.

Emerging Innovators

Non-Exhaustive

Emerging VC-backed companies have looked to disrupt the AI chip market by leveraging customized architectures. For example, companies like SiMa.ai and Groq have developed custom (von Neumann) ASICs optimized for SWaP-constrained edge environments and data center compute of LLMs, respectively. EnCharge AI aims to leverage a non-von Neumann architecture—IMC—that promises to train models with less power input than GPUs, while Extropic is, uniquely, exploring a new, thermodynamic-based computing approach. Both could be highly disruptive to AI compute speed and efficiency. Still other startups, such as Celestial AI, are focusing on photonic data transfer solutions to address the communications bottleneck impeding AI runtime efficiency. Because almost all advanced chip fabrication takes place in East Asia, the associated security risk has made it challenging for USG to work with most emerging chip companies. Underscoring the strategic importance and vulnerability of this tech area, many startups are compromised by significant funding from Chinese investors. Indeed, it is conceivable this is a conscious strategy meant to "poison the well" of American chip innovators and undermine the ability of USG to leverage their technologies.

Celestial AI

HQ: Santa Clara, CA

TOTAL RAISED: $339M

SERIES: Later Stage

USG TRACTION: N/A

Celestial AI is developing a photonic fabric technology for data center compute and memory connectivity. Celestial combines the advantages of photonics, mixed-signal ASICs, and advanced packaging to move data more efficiently both within and between chips via photonic links. Celestial's photonic fabric enables memory disaggregation, overcoming the memory capacity bottleneck and ensuring all compute and memory can be maximally utilized. Ultimately, this results in 25 times higher bandwidth and 10 times lower latency and power consumption, which will have a disruptive impact both at the edge and in data centers.

EnCharge AI

HQ: Santa Clara, CA

TOTAL RAISED: $44.3M

SERIES: Early Stage

USG TRACTION: Developed from Princeton University research conducted in part with DARPA funding

EnCharge AI is commercializing robust and scalable next-generation analog IMC that provides orders-of-magnitude higher compute and cost efficiency compared to today's solutions. Their peer-reviewed technology was developed at Princeton University with support from DARPA and has been validated on chips fabricated at TSMC using 16 nm technology. The reductions in energy and cost requirements for EnCharge AI's full-stack solutions will enable AI to be accessible at scale in SWaP-constrained applications. EnCharge AI is led by veteran technologists with backgrounds in semiconductor design and AI systems.

Extropic

HQ: Austin, TX

TOTAL RAISED: $14.1M

SERIES: Seed

USG TRACTION: N/A

Extropic is pioneering a novel, full-stack approach to generative AI hardware and software grounded in thermodynamic physics. The company's leadership team, which previously spearheaded the development of physics-based AI software and hardware for quantum computing at Google and Alphabet's X, is now advancing this new paradigm of thermodynamic computing for generative AI. This approach has the potential to deliver orders-of-magnitude improvement in both speed and energy efficiency for deep learning and probabilistic inference. The team ultimately aims to develop a new physical substrate for generative AI in terms of speed, energy efficiency, and spatial density.

Groq

HQ: Mountain View, CA

TOTAL RAISED: $362.55M

SERIES: Later Stage

USG TRACTION: DOE (Argonne National Lab)

Groq is a generative AI solutions company and the creator of the LPU Inference Engine, the fastest language processing accelerator on the market. It is architected from the ground up to achieve ultra-low-latency, energy-efficient, and repeatable inference performance at scale. Customers rely on the Groq LPU Inference Engine as an end-to-end solution for running LLMs and other generative AI applications at 10 times better performance. Jonathan Ross, inventor of the Google Tensor Processing Unit (TPU), founded Groq to preserve human agency while building an AI economy.

SiMa.ai

HQ: San Jose, CA

TOTAL RAISED: $270M

SERIES: Early Stage

USG TRACTION: N/A

SiMa.ai's software-centric, machine learning system-on-a-chip (MLSoC) accelerates the proliferation of very low-power, high-performance ML-embedded edge applications. The MLSoC integrates complete ML pipeline and application processing on a single chip. SiMa's push-button user experience simplifies the deployment and scaling of AI/ML and CV models for forward operating base (FOB) edge use cases, such as drones, portable equipment, and expendable surveillance and munitions devices. SiMa government customers enhance new and legacy systems with 15 times frames per second real-time processing and less than 15 W while meeting SWaP, extended temperature, reliability, and packaging requirements.

ESTABLISHED PLAYERS

Today, the AI chips market is dominated by GPU manufacturers—in particular NVIDIA, AMD, and Intel. Other notable Big Tech announcements include Microsoft's Maia accelerator. Additionally, the corporate venture funds are actively funding novel offerings—leading to a market dominated by Big Tech players that will eventually hold substantial equity or even full acquisitions.

2. Alternative Position, Navigation, and Timing

> **GPS is the backbone of the modern global economy and at the heart of the military's ability to command and control the battlefield. With increasing risks to GPS, developing alt-PNT innovation will be essential to provide resilient and continuous high-quality navigation resources to users in any domain.**
>
> **– Gilman Louie**
> CEO, America's Frontier Fund

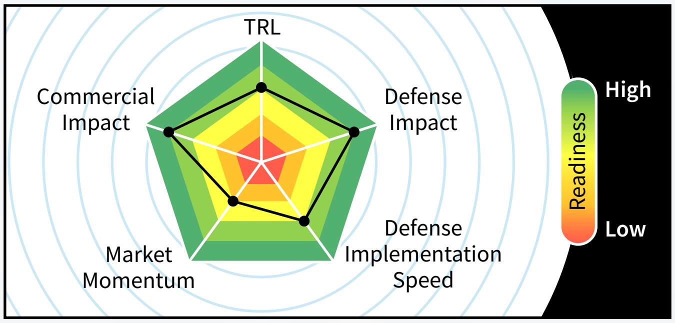
Executive Summary

Definition: Alternative position, navigation, and timing (alt-PNT) refers to the suite of technologies used to supplement, enhance, or even replace the Global Positioning System (GPS) for geolocation and timing when necessary.

Technology: Some of the main alt-PNT options include inertial, visual, low Earth orbit (LEO) satellite, terrestrial radio frequency (RF), and environmental/geophysics-based PNT. While several alt-PNT solutions have been available and deployed since the 1990s, there is currently a new wave of innovation, much of which is enabled by advances in atomic clocks and deployment of LEO satellites.

Strategic Insight: Threats to—and even direct attacks on—GPS are mounting. U.S. adversaries have known capabilities to disable GPS, which could cripple military operations and snarl commercial activity. Even so, the Government Accountability Office (GAO) has disclosed that DOD continues to heavily rely on GPS, which presents an alarming vulnerability to national security.

Future: Ideally, future navigation systems will be embedded with multiple alt-PNT modalities that can be used separately or in tandem, depending on need and context, and perhaps leveraging multimodal (AI) fusion. Lower SWaP and cost (SWaP-C), ultra-precise optical clocks, and other sensor innovations will be essential to making such systems accessible and interoperable in GPS-denied environments.



Navigation in GPS-Denied or Contested Environments

PNT technologies are an essential part of daily operations for the U.S. military and myriad foundational commercial and civilian applications. The majority of PNT use cases rely on GPS, which is part of a set of satellite constellations known as Global Navigation Satellite Systems (GNSS). GPS and GNSS are intrinsically vulnerable to interferences, whether through jamming, spoofing, cyberattacks, or even accidental obstruction. More alarmingly, near-peer adversaries will undoubtedly endeavor to degrade and globally disrupt GPS in the event of a "great power" conflict. A 2019 study sponsored by the National Institute of Standards and Technology (NIST) estimated that a GPS outage would cost the U.S. about $1 billion per day; a multiday outage could jeopardize communications networks, supply chains, digital financial transactions, and much of the transportation sector. Such attacks are already being used by U.S. adversaries and will only become more effective over time. For example, drug traffickers and others are spoofing the GPS receivers

USE CASES

- Autonomous Vehicles
- Underwater/Underground Vehicles
- Spacecraft
- Commercial Vehicles
- GPS-Denied/Contested Environments

<< Back to Table of Contents

on drones used by the U.S. Border Patrol at the southern border to interfere with their geofencing ability. Thus, alternatives to GPS/GNSS-based PNT technologies (referred to variously as alt-PNT, APNT, assured PNT, or complementary PNT) are critical for a secure and resilient military and economy.

Technology: Alt-PNT is not a single technology but, rather, a set of solutions that can act both as a replacement to GPS in the event of an outage and as a complement to improve accuracy. Broadly, these methods can be classified into two major categories: relative and absolute. Relative PNT uses onboard sensors to track position without the requirement of an external signal. This approach, which includes inertial navigation systems, is immune to jamming and spoofing but can suffer from error accumulation over time, particularly using current state-of-the-art (SOTA) sensors. Absolute PNT, meanwhile, leverages external sources of information, typically making it more accurate but subject to interferences. Absolute PNT technologies include terrain-based or celestial visual positioning systems (VPSs); LEO satellite-based PNT; geophysical sensing, such as of Earth's magnetic and gravity fields; and navigation based on various dedicated and/or opportunistic RF signals, among others.

Critically, many PNT options—GPS or otherwise—rely on ultra-precise timekeeping to navigate accurately. Therefore, one common technical thread underlying them is atomic clocks, which measure time by monitoring the resonant frequency of atoms. While this technology has been used for decades, a new generation of low SWaP-C atomic clocks is rapidly maturing. These advances will soon reach the point where they can allow for lightweight and cost-effective precision PNT systems to be widely embedded in platforms without the large tradeoff of earlier technology generations.

Strategic Insight: The vulnerability of GPS was underscored in late 2021, when Russia successfully tested its anti-satellite technology and threatened to "blind NATO and the U.S." by shooting down all GPS satellites. In the Indo-Pacific region—the epicenter of emerging geopolitical challenges—military strategists are forecasting that, in the event of a conflict with China, one of the first acts undertaken by the People's Liberation Army (PLA) will be to disable the U.S.'s and its allies' access to GPS/GNSS—again highlighting the essential nature of assured precision navigation.

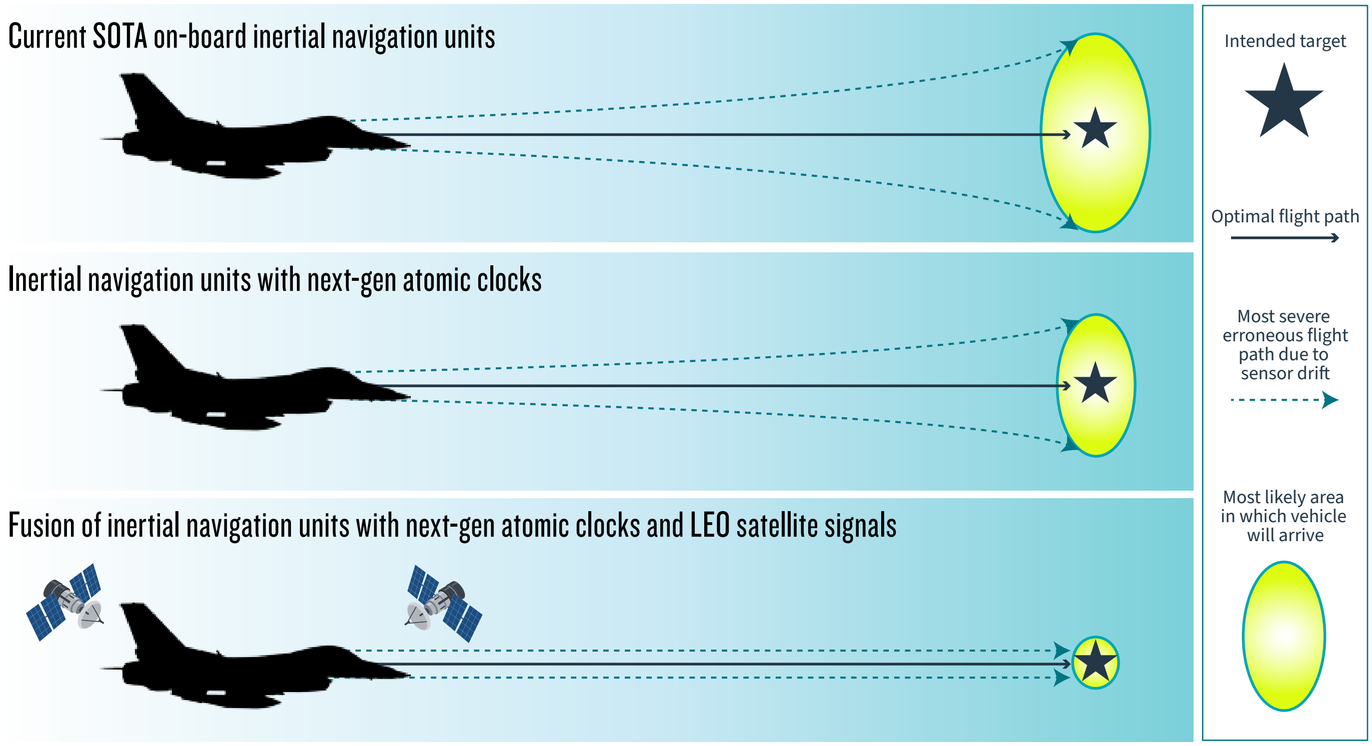


Figure 4: *Better timing elements can positively impact missions in both relative and absolute PNT systems under GPS-denied conditions. For example, next-gen atomic clocks in onboard inertial navigation units combined with signals from LEO satellites can help guide flight paths much more precisely, ensuring accurate PNT even in contested environments.*

 |

Alt-PNT Investment Trends

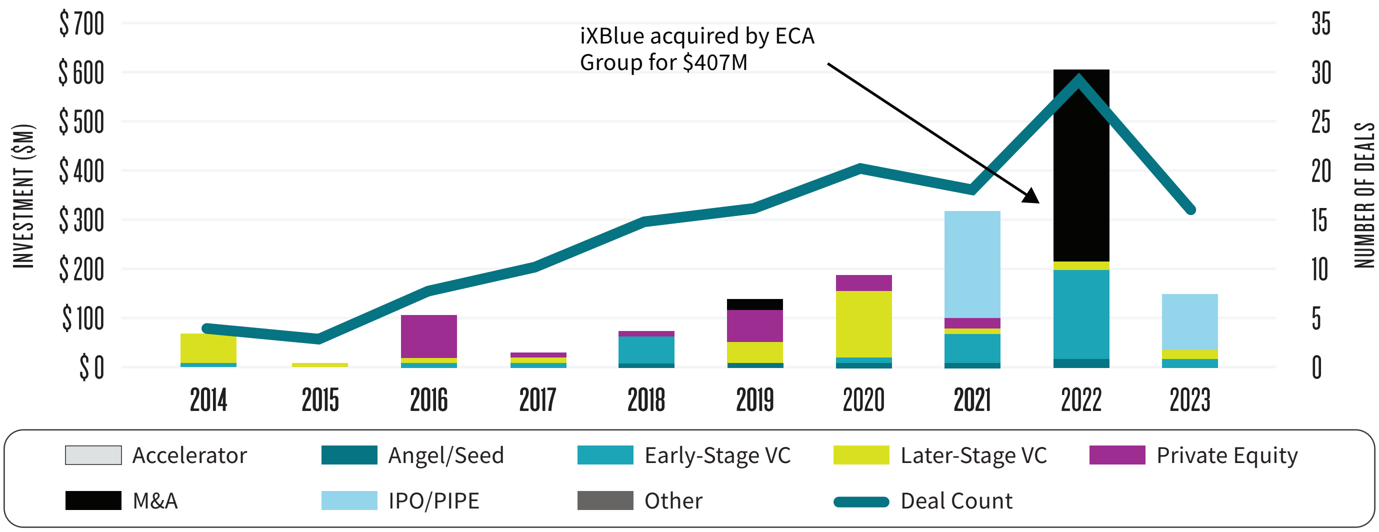


Figure 5: *Because alt-PNT as a concept is not new, the market for this technology is characterized by a mix of earlier- and later-stage deal flow. Companies innovating in, for example, LEO satellites, visual positioning, and quantum sensors are breaking in with earlier venture funding rounds, while more mature inertial and celestial navigation solutions are characterized by consolidation (private equity and M&A activity). Note: This analysis is solely focused on global positioning and does not include companies developing indoor local positioning systems—for example, for navigation of robots in warehouses. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

The GAO has raised significant concerns that DOD is not sufficiently prioritizing this space. In light of this, the NDAA for FY22 saw a $218 million increase from FY21 to mature, test, and produce resilient PNT solutions, with an emphasis on opportunistic RF approaches. Subsequently, the NDAA for FY23 highlighted continuing investments in developing alt-PNT to reduce reliance on a single modality.

To decrease the time and cost needed to field new PNT capabilities, several efforts are underway across DOD to implement modular open systems approaches (MOSAs). Even so, while there are now several existing programs and systems with embedded alt-PNT (e.g., the U.S. Air Force's [USAF] B-2, which combines celestial and inertial navigation), they still suffer from limitations in SWaP-C and precision. A combination of small and low-cost navigation components would dramatically improve military systems' reliability and accuracy.

Future: When it comes to alt-PNT, there is no one-size-fits-all solution. In an ideal future, all navigation systems will be designed with many built-in precision PNT modalities that can be swapped or fused depending on need and context. For example, an Army UAS uses GPS in friendly airspace but can, in a contested environment, implement inertial sensors supplemented with LEO satellites, leveraging the benefits of tiny but highly precise atomic clocks. Even more advanced timing units known as optical clocks could further revolutionize navigation should they be sufficiently miniaturized. For instance, U.S. missiles already include preinstalled relative positioning systems that are resistant to interference. However, these missiles are limited by the distances they can currently travel before their positional accuracy degrades dangerously. Continued innovation in precision timing, such as with low-SWaP quantum clocks, will enhance the accuracy of these missiles and other military weapons, thus minimizing off-target damage and loss of life.

<< Back to Table of Contents

Emerging Innovators

Non-Exhaustive

Navigation technologies today primarily center around GPS/GNSS, particularly in the private sector. Because of the additional cost, alt-PNT is not widely perceived as dual-use. Unfortunately, private industry may not feel compelled to adopt alt-PNT capabilities until after a catastrophic failure to GPS. As a result, commercial sector innovators today largely cater to USG and DOD. Because of its similarity to GPS, high accuracy, and low cost, LEO-satellite-based PNT—such as that being explored by Xona Space Systems and TrustPoint—may have the best early commercial traction. VPSs, often enhanced with inertial navigation, are also gaining significant traction due to improvements in hardware and software for CV, as with PSIONIC. Ultimately, next-generation atomic clocks from companies like Vector Atomic and Infleqtion can boost the accuracy and latency of both relative and absolute PNT solutions (including GPS), setting the stage for wide applicability.

Infleqtion

HQ: Boulder, CO (R&D); Austin, TX (Executive)

TOTAL RAISED: $182.21M

SERIES: Early Stage

USG TRACTION: DARPA, NRL, U.S. Army Futures Command, AFRL, DOE, NASA

Infleqtion is the developer of an optical atomic clock, Tiqker, which is designed to ameliorate the increasing complexity of receiving accurate time standards from satellite networks and provide precise and resilient timing, even during GNSS/GPS interruptions. Tiqker addresses the demand for higher-performance time protocols needed for telecommunications, data centers, financial transaction tracking, metrology, logistics, and defense. In addition, Infleqtion is developing alt-PNT solutions based on quantum magnetometry, quantum gravimetry, quantum inertial measurement, and Rydberg atoms for opportunistic RF sensing and geolocation, as well as quantum computing software and hardware, making them a leader in a wide variety of quantum technologies.

PSIONIC

HQ: Hampton, VA

TOTAL RAISED: $18.8M

SERIES: Later Stage

USG TRACTION: NASA, U.S. Army, ONR

PSIONIC develops advanced inertial navigation systems designed to provide relative motion and position for commercial and defense applications. Their SurePath product is a multifunction device using NASA-born Doppler lidar that enables precision navigation in GPS-denied environments. It works on the ground and in the air, can operate in contested environments, and neither relies on any input RF signals nor emits an RF signal. It is currently being tested by defense and commercial customers.

TrustPoint

HQ: Dulles, VA

TOTAL RAISED: $4.0M

SERIES: Seed

USG TRACTION: U.S. Navy, USAF, USSF

TrustPoint is a venture-backed, dual-use company focused on developing a next-generation GNSS through the use of LEO satellites and proprietary signal processing. TrustPoint aims to deliver improved navigation performance, jam resistance, security, and reliability, leveraging their innovative and differentiated C-band service approach. Their technology supports USG PNT resiliency and vital infrastructure management, as well as enables next-generation commercial applications like drone delivery, self-driving cars, urban air mobility, and augmented reality. TrustPoint is led by a team with more than 150 combined years of USG and commercial experience.

Vector Atomic

HQ: Pleasanton, CA

TOTAL RAISED: $110M

SERIES: N/A (all from USG contracts)

USG TRACTION: AFRL, ARL, ARO, DARPA, DIU, MDA, NASA, NAVAIR, NGA, ONR, OUSD, USSF, SSP

Since 2018, Vector Atomic has been developing quantum technology for mission-critical applications, including navigation and communications. The company is building high-performance clocks and synchronization hardware for picosecond-level timing networks, which will enable centimeter-scale autonomous vehicle navigation, ultrahigh-bandwidth data networks, and precise mapping of Earth. Synchronization has been demonstrated over city scales (30 km) and can ultimately be extended globally through ground-to-satellite relays. Vector Atomic also develops quantum inertial sensors to further complement their alt-PNT portfolio. Multiple at-sea trials of their maritime gravimeter have been carried out. Recently, they delivered a pathfinder atomic gyroscope for space that will launch in 2024.

Xona

HQ: San Jose, CA

TOTAL RAISED: $26M

SERIES: Early Stage

USG TRACTION: AFRL, ONR, USSF, NGA, NIST, U.S. Army

Xona Space Systems is the creator of the first independent precision LEO PNT service designed to provide a secure and robust alternative to GNSS. Using LEO satellites with its patented system architecture, Xona's Pulsar provides a PNT service that is over 100 times stronger and 10 times more accurate than GNSS, and is designed to integrate directly into existing GNSS equipment with a firmware update. Pulsar also has added security with encryption and authentication. This technology supports many sectors/industries, from trucking and agriculture to maritime and aerial mobility.

ESTABLISHED PLAYERS

The alt-PNT space is dominated by companies with a business model of business-to-government (B2G) rather than business-to-business (B2B) or business-to-consumer (B2C), which is especially true when it comes to large, established companies. This is largely because commercial industry currently sees little need for alternatives to GPS, which is sufficiently reliable and accurate for most industrial purposes. Thus, historically, the traditional alt-PNT players have been the major defense primes and systems integrators, such as Northrup Grumman and Collins Aerospace (now owned by Raytheon). These entities serve USG clients who are much more sensitive to issues of assurance and resiliency than their commercial counterparts.

<< Back to Table of Contents

3. Autonomous Swarms

> **True swarming—cooperative autonomous behavior at the battlefield's edge—confronts the enemy with an ever-shifting amorphous mass that is everywhere and nowhere at the same time, constantly adapting to their every move.**
>
> **– Paul Scharre**
> Executive Vice President and Director of Studies, CNAS

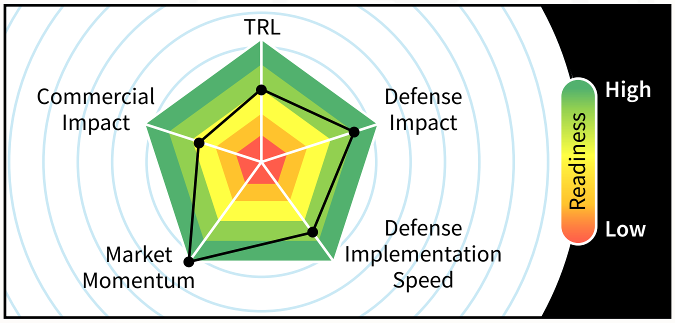
Executive Summary

Definition: Autonomous swarms are groups of autonomous robots that operate as a cohesive unit to perform a mission, inspired by self-organizing, nonhierarchical biological systems.

Technology: Units in a swarm use AI "pilots," communication with humans, other units in the swarm, and non-swarming systems to make decisions, optimize roles, and execute tasks; redundancy and fault tolerance ensure mission success even if multiple agents fail.

Strategic Insight: Replicator, DOD's sUAS (small drone) procurement program announced in fall 2023, is a forcing function to accelerate development timelines for swarming AI pilots, scalable and affordable hardware platforms, and a secure supply chain.

Future: Swarming hardware and software that is modular and platform-agnostic will enable a smooth transition to new use cases, including counter-swarming against enemies.



Force Multiplication Through Teaming

Autonomous swarms are groups of autonomous robots that operate as a cohesive unit to perform a mission. Consisting of many individual, independent autonomous platforms—each piloted by an onboard AI-powered autonomous agent as opposed to a remote human pilot—swarms coordinate and cooperate to achieve a common objective, leveraging varying degrees of communication with human operators and each other. Applications for swarms in defense settings include collecting intelligence, monitoring infrastructure, maintaining perimeter security, and engaging targets or delivering effects on the battlefield. Swarming behavior is inspired by nonhierarchical, self-organizing systems in the natural world, including social insects, schools of fish, and flocks of birds. Autonomous swarms are often used and envisioned with aerial robots, but ground, surface, and subsurface swarms are also used and in development.

Technology: Fully autonomous, decentralized swarms are designed to operate without a designated "pack leader," meaning that each unit within a swarm makes decisions independently based on interactions with its surroundings and with other members of the swarm. Onboard AI models help swarms adapt to changing conditions, optimize task allocation and behavior over time, and make collective decisions, which can involve voting systems, consensus protocols, or other mechanisms to reach agreement. Redundancy and fault tolerance are often built into swarms to ensure mission success even if one or a few agents fail. This is essential in single-use swarms or those with disposable members, such as swarms designed to counter

USE CASES

ISR | Weapons | Counter-Swarm | Logistics | Communications

<< Back to Table of Contents

enemy swarms. Mission needs, mission risk, and the degree of trust in autonomous algorithms will all influence a swarm's level of autonomy, though most swarms will rely on a human operator in the loop to some degree for the foreseeable future.

Recent advances in decentralized and adaptable AI controls include the creation of more robust and scalable algorithm testing and training, development of low SWaP materials and systems (including sensors, processors, and power supplies), and novel cybersecurity and electronic warfare (EW) tactics. These technologies will further solidify autonomous swarms as key battlefield assets and teammates of the future warfighter.

Even with these advances, modular open software architectures must be adopted to enable secure and trusted teaming across platform roles, domains, operating systems, and vendors. Optimizing task-agnostic sensor suites will allow future swarms to conduct a greater breadth of missions, particularly on platforms with modular payloads. Addressing these issues will accelerate the speed of swarm development, support the creation of more diverse platforms with broader capability sets, and increase overall mission effectiveness of robotic swarms. Adopting clear policies and specifications for hardware and software systems will also help vendors address these issues efficiently.

Strategic Insight: Autonomous swarms enable comparatively smaller teams to project greater power, collect more information, and better protect key assets. Replicator, DOD's program to rapidly field "attritable" autonomous systems, announced in September 2023, is viewed by industry as a forcing function to rapidly develop and procure mission-ready swarming systems to counter robust competition from China. Replicator follows other DOD programs aiming to develop swarms, such as DARPA's Autonomous Multi-Domain Adaptive Swarms-of-Swarms (AMASS) and OFFensive Swarm-Enabled Tactics (OFFSET) initiatives. In a potential future engagement, effective force multiplication through technologies such as drone swarms will be necessary to deter enemies and ensure battlefield dominance.

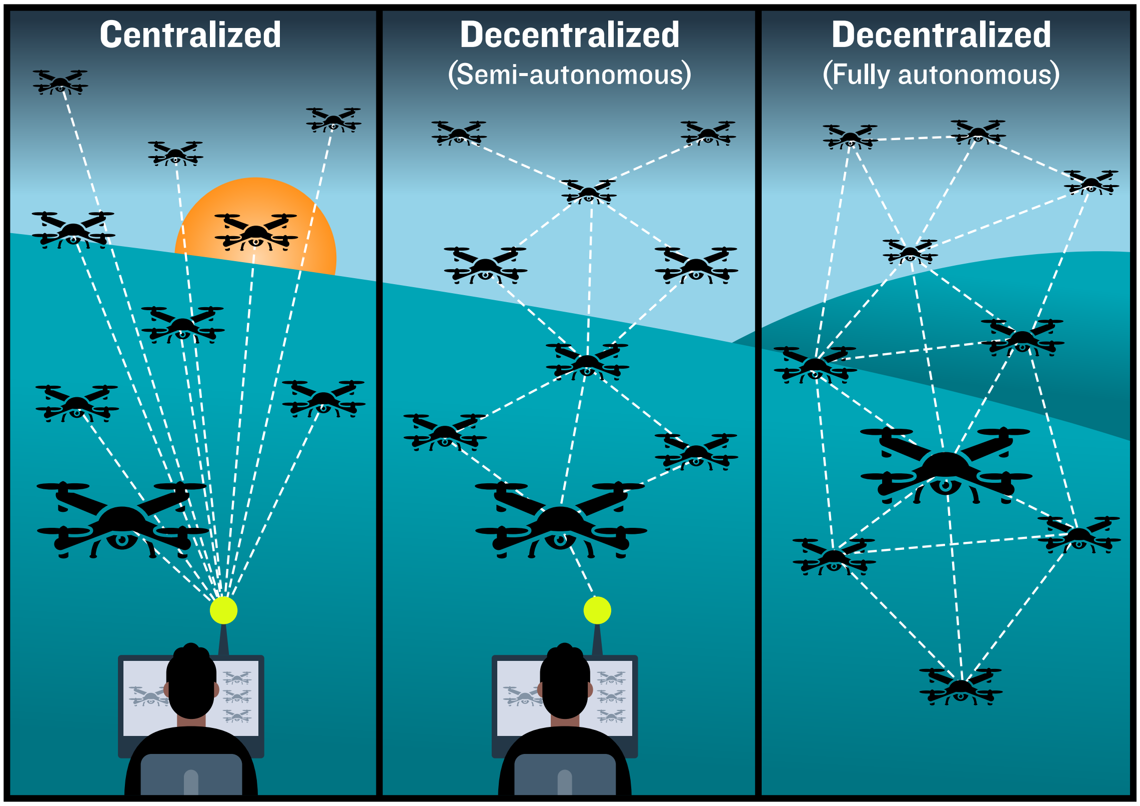


Figure 6: *Methods of drone swarm command and control (C2). Future systems will increasingly use semi-autonomous and autonomous decentralized architectures, with the optimal balance between the two based on specific mission needs. Source: GAO 23-106930.*

Autonomous Swarms Investment Trends

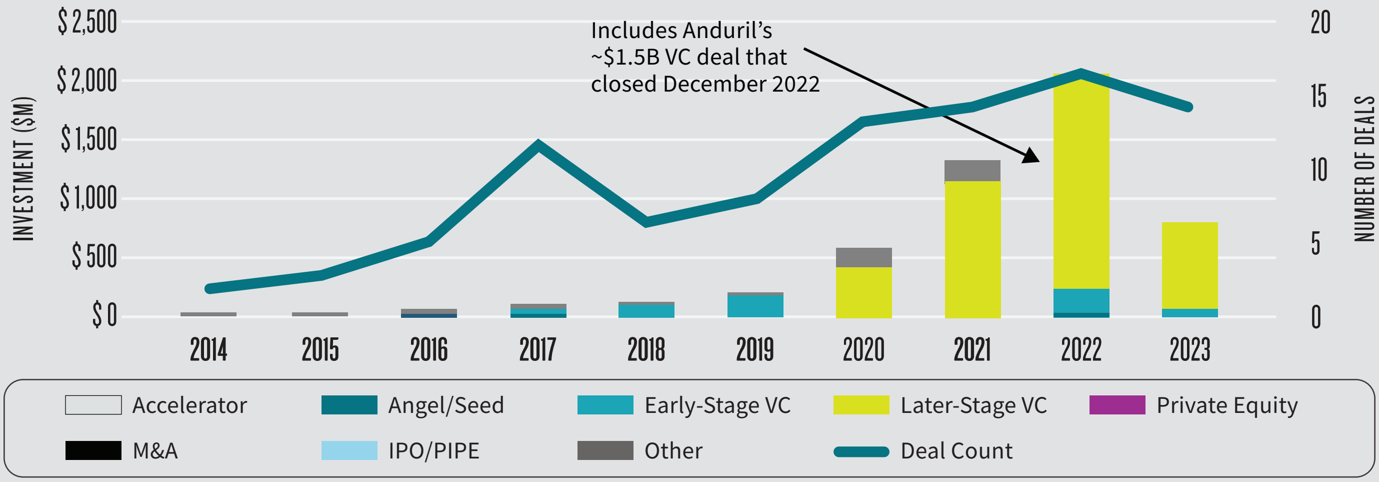


Figure 7: *Disclosed funding for swarming continues to rise as the capital-intensive technology develops further; most funding is concentrated in a few massive VC-backed defense startups, including Anduril, Shield AI, and Skydio. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

The ongoing conflict in Ukraine has demonstrated one key challenge with existing drone operations that autonomous swarms could address: vulnerability to jamming and hacking. Fully autonomous and decentralized swarms are less reliant on RF links to operate and accomplish missions, and therefore are less susceptible to EW attacks. Policymakers and warfighters must strike an optimal balance between autonomy and human control in the adoption of this technology, and it is likely that this balance will move toward autonomy as systems mature and trust in them builds.

Israel became the first country to use true drone swarms, deploying them in its 2021 conflict with Gaza, and is arguably the global leader in this technology because of their implementation of Elbit Systems' Legion-X, a modular, heterogeneous, multi-domain C2 swarm system. Legion-X was subsequently used by Azerbaijan in the 2023 Nagorno-Karabakh conflict against Armenia and by Israel in its recent 2023–2024 campaign in Gaza. Further, Iranian-backed Houthi militants in Yemen have taken lessons from the Ukraine war and launched Iranian-made Shahed drones in a swarming formation to overwhelm U.S. Navy positions in the Red Sea shipping lanes.

Future: Future applications for autonomous swarms range widely, though widespread use will likely first involve nonlethal applications, such as intelligence, surveillance, and reconnaissance (ISR), communications and EW links, and logistics support. Developing platform-agnostic C2 software and designing swarms to carry modular payloads will ease the transition to new use cases. As enemies develop their own swarms, counter-swarm systems will be necessary to maintain battlefield dominance. "Beating fire with fire"—using friendly swarms against enemy swarms—is currently an attractive solution for military leaders.

Commercial applications for swarms will include search and rescue missions, natural disaster response, infrastructure monitoring, security and public safety, and logistics. Industry leaders believe the companies that "win" the defense space will be best positioned to capture the future commercial market as well. Commercial and defense adoption, however, requires tangible federal guidance. Experts generally agree that widespread cultural adoption will require greater governance over testing, innovations in electronic jamming resistance, and greater algorithm trust in both the short and long term as swarm development advances.

Emerging Innovators

Non-Exhaustive

Defense-focused startups are the future of the autonomous swarming space. Massive, venture-backed companies like Anduril, Shield AI, and Skydio are well positioned to continue as market leaders, with each offering novel swarming solutions. Darkhive and Firestorm are both early-stage original equipment manufacturers (OEMs) of small UAVs optimized to operate in massive swarms.

Saronic has prototyped two models of small swarming autonomous surface vehicles (ASVs) with a third on the way. Vatn Systems creates small underwater autonomous vehicles designed to carry modular payloads for a variety of missions. Meanwhile, Swarmbotics AI specializes in the development of swarming ground robots.

DARKHIVE

Darkhive

HQ: San Antonio, TX

TOTAL RAISED: $5M

SERIES: Seed

USG TRACTION:
AFWERX, AFRL, OUSDRE, DIU NSIC

Darkhive develops low-cost autonomous tactical drones for defense and public safety applications. Their unique combination of affordable hardware, ease of use, open interface design, and secure software continuous delivery has enabled them to rapidly gain traction in the autonomous drone swarming space with program offices like AFWERX Autonomy Prime, with whom they were recently awarded a $100 million Phase III Small Business Innovation Research (SBIR) IDIQ contract.

FIRESTORM

Firestorm

HQ: San Diego, CA

TOTAL RAISED: $13M

SERIES: Early Stage

USG TRACTION:
AFWERX, AFSOC, INDOPACOM, EUCOM, Air National Guard

Firestorm disrupts the traditional defense technology model by pursuing systems that can scale up and be affordable enough to deploy in large numbers. Its drones are assembled in sections like a LEGO set and can be 3D printed in nine hours, making them very cost-effective. Prioritizing speed and agility in their manufacturing process allows Firestorm to produce drones anywhere in the world using the same technology used for rapid payload integration.

Saronic

HQ: Austin, TX

TOTAL RAISED: $72.5M

SERIES: Early Stage

USG TRACTION: Collaborating with several undisclosed USG stakeholders, including participating in naval exercises

Saronic is a defense technology company building unmanned surface vessels designed for autonomy from the keel up. The company's vessels combine best-in-class software, hardware, and AI into attritable, scalable, configurable platforms that will enhance the range, capability, and survivability of the U.S. Navy and allied fleets.

Swarmbotics AI

HQ: Scottsdale, AZ

TOTAL RAISED: Undisclosed

SERIES: Early Stage

USG TRACTION: N/A

Swarmbotics AI is a low-cost swarm robotics company for industry and defense. The founders see a world of ubiquitous low-cost robots transforming almost all aspects of society with an urgent need in the defense industry. Swarmbotics focuses on a low-cost Bill of Materials (BOM), an autonomous stack optimized for off-the-shelf components, and a global planner that enables swarm capabilities for groups of robots to accomplish sophisticated tasks.

Vatn Systems

HQ: Portsmouth, RI

TOTAL RAISED: $3.06M

SERIES: Seed

USG TRACTION: N/A

Vatn Systems Inc. is currently developing the S1 Autonomous Underwater Vehicle. The S1's core strengths lie in its low cost and cooperative swarm capabilities. Vatn's R&D efforts focus on advanced navigation software effective in the GPS-denied and communications-compromised underwater environment, all while reducing hardware costs. The S1 pairs covert infiltration with economical design and straightforward deployment.

ESTABLISHED PLAYERS

The autonomous drone swarming market is almost exclusively a B2G market, as most commercial drone swarms for light shows and consumers are not autonomous; they typically fly preprogrammed routes and are not designed for reactive and collaborative missions. While autonomous swarm C2 technology is still very much in development across all players, large and more entrenched startups—notably Anduril, Skydio, and Shield AI—are believed to lead the market as technology (software) developers and join defense primes, including Raytheon and Northrop Grumman, as leading systems integrators.

4. Generative AI Software Development

> **Today, good software engineers are the most highly sought-after talent in the labor market and a critical resource that DOD never has enough of. Generative AI-based code development can help bridge that gap by bringing a proxy for the best of Silicon Valley talent to U.S. military operations.**
>
> **– Jacqueline Tame**
> Operating Partner, Playground Global
> and Executive Director, Silicon Valley Defense Group

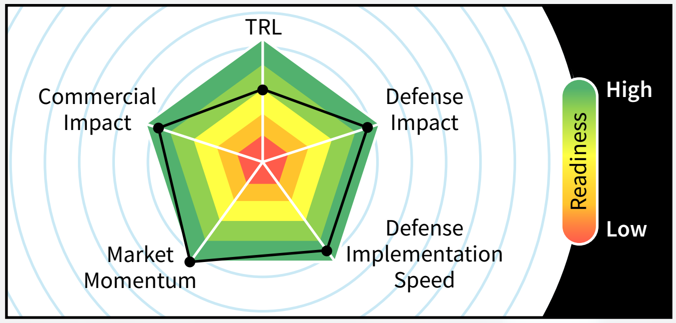
Executive Summary

Definition: Generative AI software development refers to any tool that uses generative AI to improve coding efficiencies, including code generation, code completion, code documentation, legacy code conversion, and software testing and debugging.

Technology: Generative AI-enabled software development solutions typically use LLMs to generate code and other content central to software development.

Strategic Insight: The defense sector's use of AI-enabled software development tools is still limited due to a lack of trust and reliability in the underlying technology, though DOD and other federal agencies are aggressively exploring ways to integrate generative technologies, especially in light of the 2023 presidential AI executive order.

Future: As generative coding tools progress, the technology will be able to handle more of the actual coding process, allowing humans to focus on the design and logic of the software rather than its programming syntax.

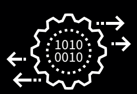


The Future of Building Software

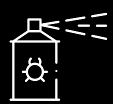
Generative coding harnesses advancements in generative AI to enhance coding efficiencies, including code generation, code completion, code documentation, legacy code conversion, and software testing and debugging. The level of autonomy these tools possess can differ significantly, ranging from producing a description about the function of a code snippet to, theoretically, creating an entire program from a natural language prompt. Harnessing AI-enabled software development tools will significantly streamline the development and deployment of DOD's software-centric warfare capabilities.

Technology: Generative AI-enabled software development solutions typically use LLMs to generate code and other content central to software development. LLMs are probabilistic models that take in large amounts of data and produce the most likely outputs. Tools specific to software development must be trained on massive

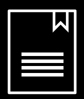
USE CASES



Code Generation

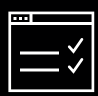


Bug-Free Code



Automatic Documentation

Code Refactoring



Code Testing

<< Back to Table of Contents

codebases and other code-related content to gain an "understanding" of how code works, enabling the tools to assist across the software development process.

Tech giants like Microsoft, Meta, and Google have played a significant role in shaping today's best LLMs, which form the core of generative software tools and often act as the base upon which startups build their AI products. These tools are evolving rapidly with tech giants' backing, promising continued advancement in code-related AI assistance.

Strategic Insight: Since January 2021, more than half of DOD's major IT business initiatives have faced significant cost or schedule changes due to technical complexities or new program requirements. Facing prolonged software development cycles due to contracting and acquisition barriers and low retention of technical talent, DOD is pivoting toward accelerating AI solutions to mitigate delays and enhance development efficiency. Despite concerns about the accuracy and reliability of AI-generated content, DOD agencies are aggressively exploring ways to integrate generative AI to avoid or streamline hurdles within their software development processes. DOD agencies' focus remains on adapting commercial innovations for federal use cases as opposed to contributing to the research itself, indicating the degree to which the commercial sector has advanced generative coding technology.

With the integration of these AI tools comes an increased need to test software more rigorously and consistently, as reliability and functionality of generated content must still be validated, especially considering potential defense and national security use cases. Regulatory frameworks and security protocols around AI are evolving, with recent directives, like the October 2023 executive order, addressing the safe and trustworthy deployment of AI. In addition, in August 2023, the Chief Digital and Artificial Intelligence Office (CDAO) launched Task Force Lima, a DOD-wide initiative to explore how to implement generative AI capabilities safely and responsibly.

As DOD launches new programs, software will increasingly define military capabilities and the programs' successes. Generative software development can be most impactful by enabling the force to respond to emerging threats in hours or days rather than months or years, accelerating decision making in critical scenarios. For example, the Pentagon's new program, Replicator, will require a large

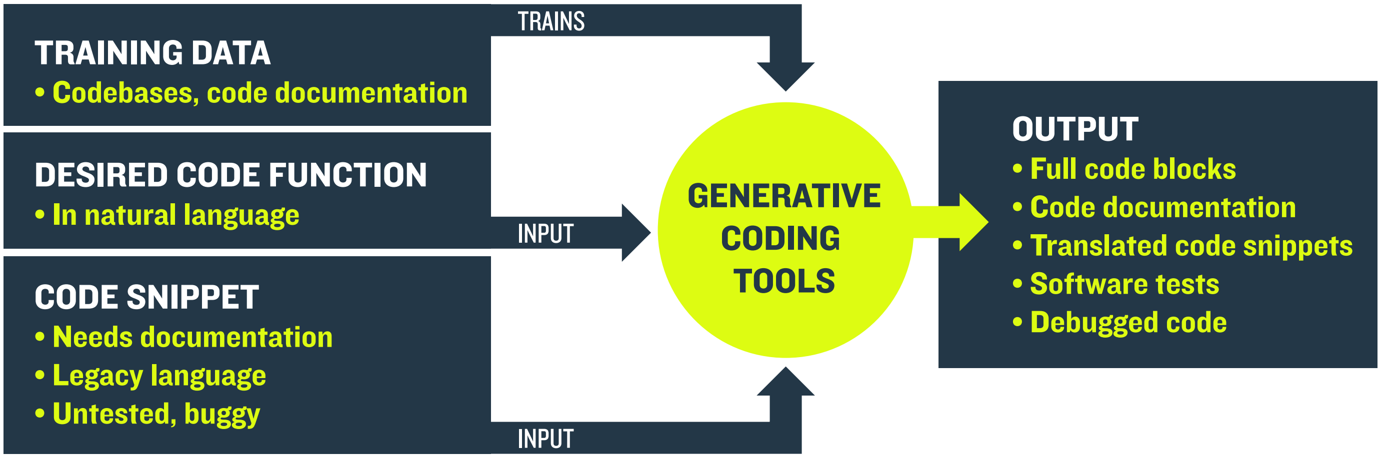


Figure 8: *The figure depicts the process of training and software development using generative coding tools.*

Generative AI Software Development Investment Trends

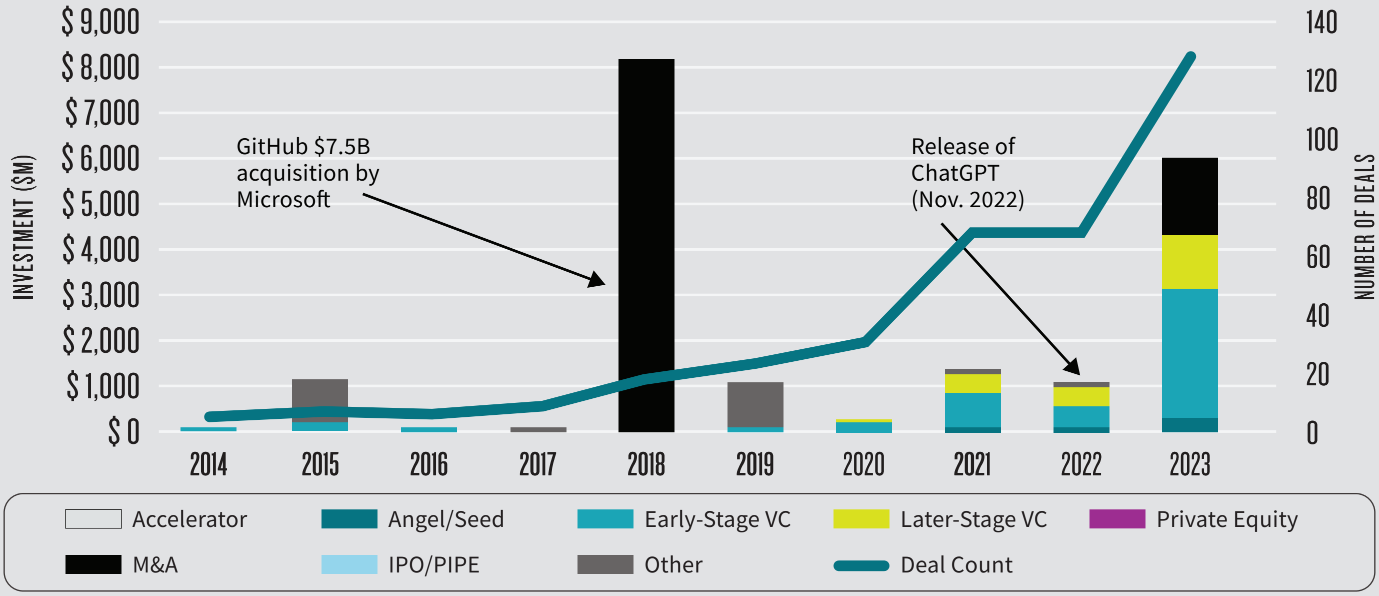


***Figure 9**: Investment in generative software development tools exploded in 2023 with the popularization of LLMs and other generative AI capabilities. Note: Given the anomalous GitHub M&A deal in 2018, along with the fact that GitHub was not acquired for its generative software capabilities, this deal was excluded when calculating the CAGR between 2018 and 2023 for use in the market momentum segment of this technology area's radar chart. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

team of developers to build and maintain complex and scattered autonomous systems in real time. Generative AI tools can increase efficiency in processes like identifying and fixing bugs, updating code, and testing programs at computer speed, resulting in shorter implementation timelines for the software central to these autonomous systems. While AI tools may reduce developer headcount, integration will necessitate strategies for retaining and upskilling talent for oversight and AI collaboration.

The adoption of AI-powered software development tools can reduce the most burdensome parts of the software development process to shorten the timeline between identifying a problem and deploying the solution. This can be the difference between success and defeat on the battlefield.

Future: The future of software has already shifted dramatically with the advent of generative AI, and it will continue to evolve alongside generative technology advances. As model performance improves and companies develop new tools, the technology will increasingly automate much of the coding process. This will allow humans to focus on big-picture issues like software design and logic rather than programmatic syntax and other minutiae involved in software coding. Moreover, generative AI will make the software development process more accessible for everyone. In the future, even nontechnical users will have the ability to create programs that directly address their operational problems using natural, rather than coded, language—thereby lowering the need for specialized developer talent. It's unlikely that these tools will replace humans; instead, they will likely free them up to focus on more complex problems that are outside AI's scope of abilities.

Fully AI-generated code is projected to dominate software development mid- to long-term. In the short term, more mature generative coding tools, such as debugging tools, code completion, and coding assistant chatbots, can take some of the mental load off humans and allow for more time to execute software-specific missions.

Emerging Innovators

Non-Exhaustive

When it comes to generative AI coding, there are a handful of companies pushing toward a new world of development. Business models ranging from direct funding by FAANG (Meta [formerly Facebook], Amazon, Apple, Netflix, and Google) to competition, via open-source channels, will enable both long-term and more nascent companies, such as Hugging Face and Replit, to share a role in defining the future of what is possible. Meanwhile, companies like Sourcegraph, Mabl, and Mutable handle more niche, but nonetheless important, aspects of software development like testing and documentation. Currently, most smaller players in this space are still using larger companies' models due to the entrenchment of technologies from dominating players like Meta and OpenAI. Meanwhile, evolving federal requirements and regulation challenges have combined to stymie federal adoption of commercial generative AI software tools. Going forward, two central questions will be: How can smaller players in this space move and innovate without depending on larger companies' models? And can they do so in a way that caters to both commercial and federal needs?

Hugging Face

HQ: New York City, NY

TOTAL RAISED: $399.9M

SERIES: Later Stage

USG TRACTION: N/A

Hugging Face provides the foundation for building AI/ML applications, including open-source model repositories, datasets, and fully developed ML applications. In April 2023, they also released their chatbot, Hugging Chat, which can assist in various code-related tasks. The public sector can leverage Hugging Face's large repertoire of open-source models to cater to their use cases, as well as use Hugging Chat to speed up the coding process. Implementing a company like Hugging Face would give DOD access to build and test new ML models quickly without having to train proprietary internal models.

Mabl

HQ: Boston, MA

TOTAL RAISED: $76.1M

SERIES: Later Stage

USG TRACTION: N/A

Mabl is a leading unified test automation platform—built on cloud, AI, and low-code innovations—that delivers a modern approach, ensuring the highest-quality software across the entire user journey. The company's SaaS platform allows teams to scale functional and nonfunctional testing across web apps, mobile apps, APIs, performance, and accessibility for best-in-class digital experiences for federal clients. With Mabl, the DOD could output stable releases at a faster pace than is currently possible.

mutable.ai

Mutable.ai

HQ: Dover, DE

TOTAL RAISED: $4M

SERIES: Early Stage

USG TRACTION: N/A

Mutable.ai's Auto Wiki product converts code into Wikipedia-style articles in which citations link to code with clickable references to each line of code being discussed. Auto Wiki makes it easier to understand and document complex technologies, especially for large DOD codebases. This enables anyone to understand the code. In addition, the need to keep documentation up-to-date is also removed, as it is updated automatically. Mutable.ai can be deployed privately and off the cloud.

replit

Replit

HQ: San Francisco, CA

TOTAL RAISED: $207.85M

SERIES: Later Stage

USG TRACTION: N/A

Replit is a cloud-native software development platform. Developers can spin up any development environment and most popular frameworks in seconds. With collaboration and AI built at the foundations, developers can code, use AI, and deploy all in one place, moving from idea to software more quickly. Developers in the federal space can use Replit to speed up their coding process; collaborate with others; and build, test, and deploy from their browser. Using a tool like Replit would allow DOD to generate and deploy code at a significantly faster rate than currently possible.

Sourcegraph

Sourcegraph

HQ: San Francisco, CA

TOTAL RAISED: $223M

SERIES: Later Stage

USG TRACTION: In partnership with Leidos to introduce secure, generative AI-enabled software development tools to USG customers

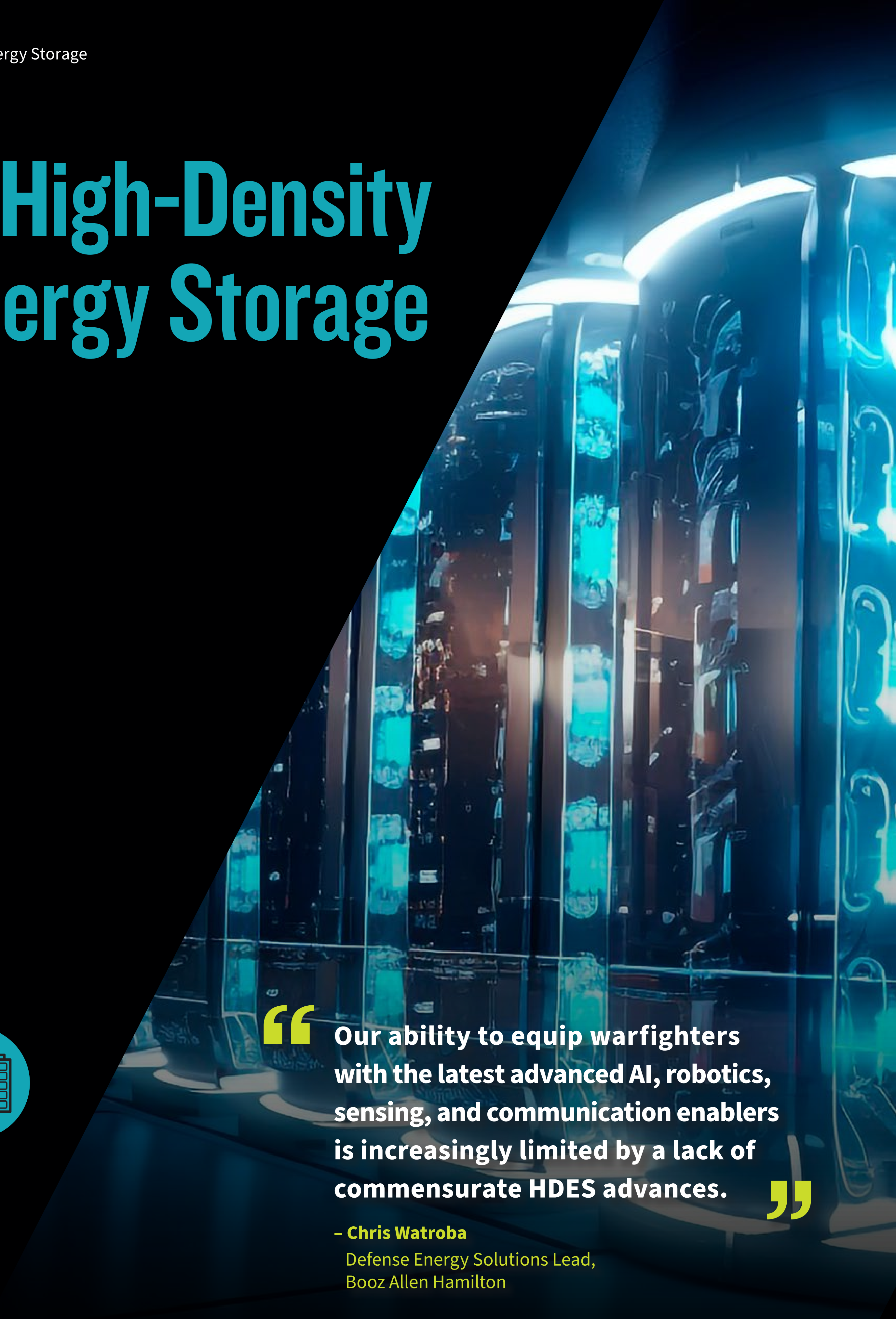
Sourcegraph is a code intelligence platform: "software that builds software." Their code graph powers Cody, the AI coding assistant for writing, fixing, and maintaining code, and Code Search, which helps developers explore their entire codebase and make large-scale migrations and security fixes. When integrated in federal agencies' codebases, Cody helps engineers code faster with AI-assisted autocomplete and leverages AI-powered chat for their code to help answer questions about the codebase, understand legacy code, or take on tricky problems.

ESTABLISHED PLAYERS

Large tech companies, such as Google, Microsoft, AWS, and Meta, alongside smaller generative AI-focused companies, such as OpenAI, Anthropic, and Cohere, are leading the charge in terms of overarching generative models and comprehensive chatbots.

<< Back to Table of Contents

5. High-Density Energy Storage



Our ability to equip warfighters with the latest advanced AI, robotics, sensing, and communication enablers is increasingly limited by a lack of commensurate HDES advances.

– Chris Watroba
Defense Energy Solutions Lead,
Booz Allen Hamilton

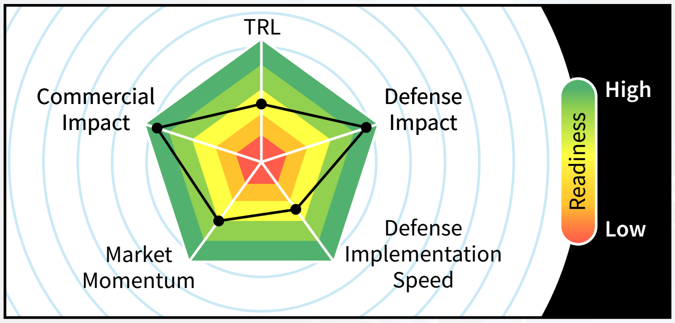
Executive Summary

Definition: High-density energy storage (HDES) aims to optimize the energy-to-weight and energy-to-volume ratios of energy systems. HDES systems store a large amount of energy in a relatively small and lightweight form (e.g., batteries), enabling more efficient and long-lasting power for applications ranging from portable electronics to electric vehicles.

Technology: Recent progress in silicon anode (SiA) chemistry suggests that, over the next one to three years, SiAs will offer much better energy density and efficiency compared to graphite-based lithium-ion technology. Solid-state batteries (SSBs) also have potential to improve current thresholds, although over a longer time horizon.

Strategic Insight: HDES is integral to various missions, from supply chain logistics to base and communication operations, and to supporting the warfighter in the field. Currently, DOD's use of traditional batteries creates bottlenecks and operational inefficiency.

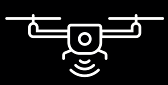
Future: Near-future electric systems will be characterized by drop-in solutions, such as SiA lithium-ion batteries and SSBs. In the longer term, hydrogen batteries have the most compelling potential, but estimates for their widespread adoption and full-scale use span from 10 to 20 years.



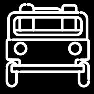
Powering Future Military Equipment

HDES encapsulates a range of technologies currently under development with the goal to significantly improve the ratios of energy-to-weight and energy-to-volume of existing SOTA energy storage systems. In a battlefield environment increasingly defined by electronics, it is critical to provide warfighters with ways to efficiently store adequate energy so they can power essential electrical systems. Electrified military equipment enables smaller form factors, significantly extended operational duration, and diminished heat and noise signatures compared to its fossil fuel-powered predecessors. A wide range of military equipment—including communications devices, all-terrain vehicles (ATVs), UASs, and medical equipment—will be augmented by innovations in HDES in the next decade, as will emergent technology still in development, such as robotic dogs and the Integrated Visual Augmentation System (IVAS).

USE CASES

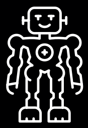


Powering Drones at the Edge

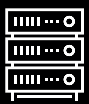


EV Automobile Power

Radio/Communication Systems



Robotics



Edge Computing And AI

Technology: Batteries store and supply energy by converting chemical energy into electrical energy—thus powering many of the electronic gadgets we interact with in everyday life. Traditional lithium-ion batteries create this chemical reaction by transferring electrons between the positive cathode and negative anode, resulting in an electrical current. Today, battery anodes are generally composed of graphite—a reliable yet inefficient way to store lithium-ion energy. However, recent progress in SiA chemistry suggests that SiAs over the next one to three years will offer much better energy density and efficiency—better than graphite-based lithium-ion technology. The current challenge is that SiAs drastically expand and contract during charge cycles, an issue that innovative, fluctuation-resistant nanomanufacturing processes are attempting to address. As SiAs begin to reliably demonstrate uniform size during charging, SiA batteries will see a pronounced improvement in operational duration.

Following SiA innovation, the industry is likely to undergo a complete shift from lithium-ion to SSBs, which are expected to reach a maturity point in the next three to five years. SSBs use solid rather than gel-like electrolytes to conduct charge between anodes and cathodes. SSBs store more energy and are considered to be safer than lithium-ion batteries due to their reduced risk of leakage or flammability, among other factors. Still, SSBs have their challenges, including issues regarding their cost, manufacturing processes, and materials acquisition. Other HDES battery chemistries, such as liquid organic hydrogen carriers (LOHCs) and metal air, are notable in their high theoretical energy densities, but their commercialization will take many years.

Strategic Insight: The Defense Logistics Agency (DLA) spends more than $200 million on batteries annually, but this only scratches the surface of the money DOD will spend on emerging electric technology and associated power systems in the future. For example, USAF is already spending hundreds of millions on new electric vertical takeoff and landing (eVTOL) systems, which will theoretically take over some missions traditionally assigned to legacy helicopters. Energy is the foundation upon which a digital battlefield depends.

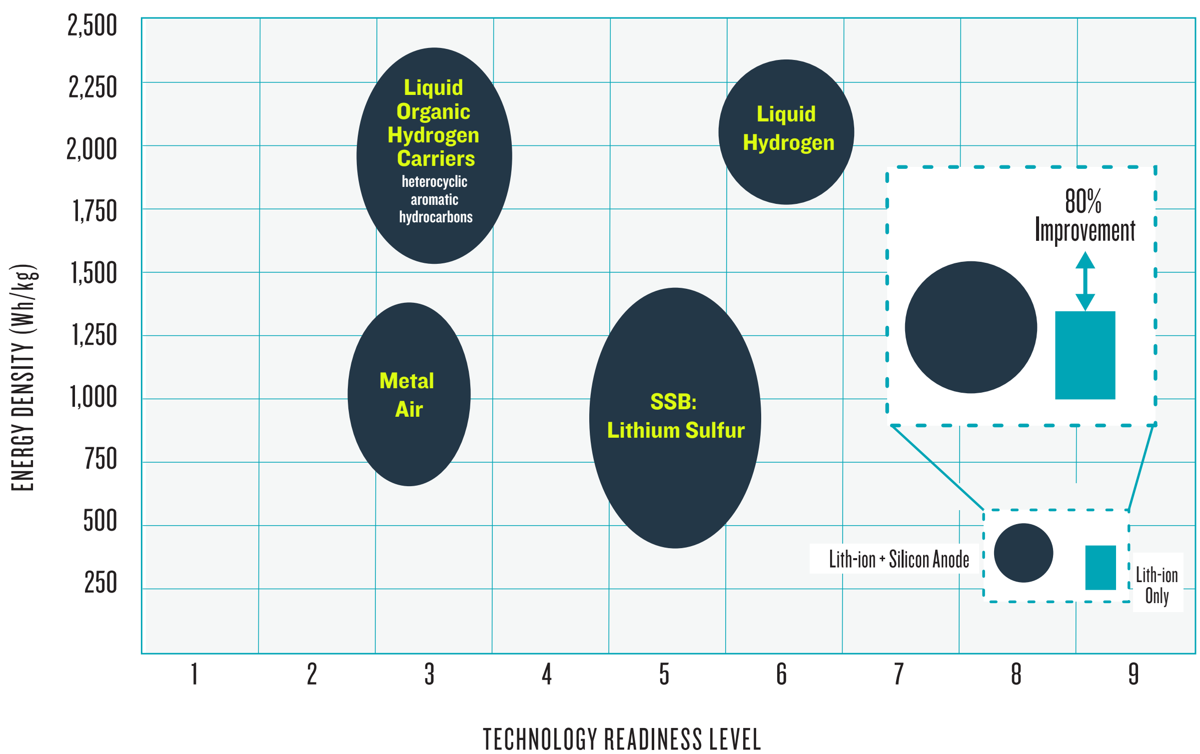


Figure 10: *The graph illustrates the relationship between TRL and energy density (Wh/kg), or the amount of power that can be stored, for various battery technologies and hydrogen fuel cells. The higher the energy density, the longer it can be used. Values are representative of the most advanced versions of each technology, and lower TRL solutions are likely to experience decreases in energy density during commercialization.*

High-Density Energy Storage Investment Trends

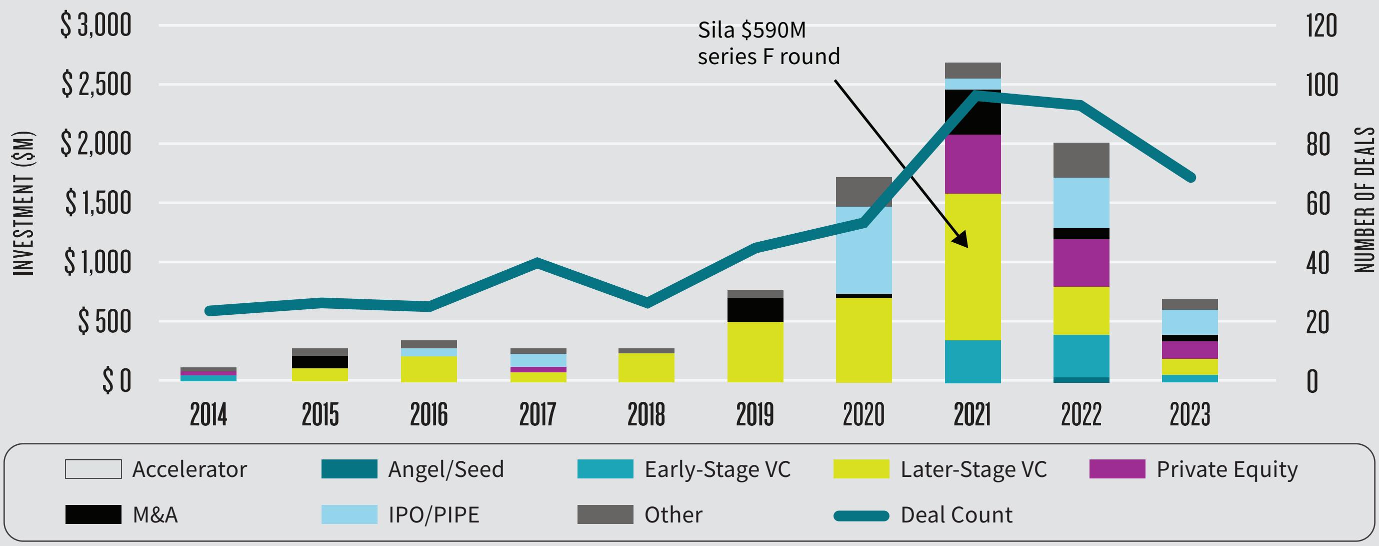


Figure 11: *Investment in HDES has seen a consistent rise in funding and number of deals between 2014 to 2021, with the majority being later-stage VC funding or from private equity. In 2021, two later-stage venture deals (Northvolt and Sila) constituted most of the year's funding. This signals market maturation of lithium-ion batteries. The next generation of HDES focuses on SiAs and SSBs. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

The future IoMT, which will accelerate the time in which sensor data reaches key decision makers, is completely enabled by reliable, long-lasting energy sources. Even incremental improvements in performance can have resounding effects when applied across services, domains, and use cases. Take, for example, the current soldier, who may be carrying more than 50 pounds of gear for a 72-hour mission—including radios, visual augmentation goggles, wearable sensors, Android Team Awareness Kit (ATAK) tablets, and other electronics. Every minute that HDES can extend the lives of these systems contributes to uninterrupted capabilities and advantages for U.S. warfighters.

Future: The ideal near-future state for DOD is widespread creation of immediate drop-in solutions, such as SiAs and SSBs, engineered to seamlessly fill gaps within equipment. Drones will fly longer, systems will be miniaturized, and energy will become less of an operational bottleneck. With an eye toward efficiency and design, some experts suggest that future batteries should be built as structural components within equipment—for example, batteries engineered as the body of a drone or electric vehicle. In addition to energy density, characteristics like ruggedization and flexibility will be essential for future DOD adoption.

Beyond the near future, hydrogen will likely mature as a fuel source due to its energy density and potential for low carbon production. Full-scale adoption requires advances across the value chain, from production to end use, as well as a decade or more for infrastructure build-out. Initial use cases are likely to focus on large trucks and other applications with demand for electrification that batteries cannot meet.

Energy is the backbone of both a tactical/kinetic and a digital/software-defined military. It is a complex capability currently underprioritized when discussing capabilities and advantages in the context of the Great Power Competition. Future conflict is likely to occur in large, vast areas of responsibility. By ensuring our military electronics are as energy efficient as possible, we can equip our warfighters with the tactical tools they need to successfully execute their missions—no matter the battlefield scale.

<< Back to Table of Contents

Emerging Innovators

Non-Exhaustive

Current HDES storage technologies focus on medical, military, and electrification use cases. Lithium-ion batteries from Anthro Energy and Advano use SiA technology for higher energy density. Nanotech Energy has differentiated itself with lithium-ion batteries focused on graphene-based or partial graphite replacement for electric vehicle applications. Prometheus Hydrogen is unique in its development of clean hydrogen-fueled batteries for military use cases.

Advano

HQ: New Orleans, LA

TOTAL RAISED: $46M

SERIES: Later Stage

USG TRACTION: N/A

Advano uses SiA technology to improve lithium-ion batteries, making them more cost-effective and offering better energy storage. Their A-SiFx technology leads to a 40% improvement in energy density and up to a 210% cost reduction. The company's innovative process involves using metallurgical silicon and upcycled silicon from silicon waste to produce eco-friendly battery technology.

Anthro

HQ: San Jose, CA

TOTAL RAISED: $28M

SERIES: Early Stage

USG TRACTION: OSD, U.S. Army

Anthro Energy is revolutionizing the field of high-density energy storage with its cutting-edge batteries for wearable, medical, and IoT devices. The company's AdhesION Polymer Electrolyte enables the batteries to be safe, flexible, and high performing, even in harsh environments. This technology is ideal for auxiliary military equipment like drones and robotics, where space and weight are critical factors. Using SiAs and SSBs, Anthro Energy can deliver more power and longer life to these applications while reducing the risk of fire or explosion.

 |

NANOTECH

Nanotech Energy

HQ: Sunny Isles Beach, FL

TOTAL RAISED: $256.61M

SERIES: Later Stage

USG TRACTION: N/A

Nanotech Energy has successfully used graphene to enable the next generation of lithium-ion batteries. Using the conductivity and surface area of graphene (it can stretch up to 20% of its length) to improve the electrochemical properties of the lithium-ion battery anode and cathode simultaneously, this super battery delivers ultra-high power density, energy density, and cycling life. In addition, their nonflammable cells limit the potential of a flame or explosion, providing a safer battery solution.

PROMETHEUS Hydrogen

Prometheus Hydrogen

HQ: Saint Charles, IL

TOTAL RAISED: Undisclosed

SERIES: Undisclosed

USG TRACTION: U.S. Navy, USG Pilot

Prometheus Hydrogen provides DOD with innovative hydrogen power and storage solutions. When integrated with a fuel cell, this company's products can increase gravimetric and volumetric energy density by several times that of traditional lithium-ion batteries. These products are safe, mobile, and affordable, potentially increasing operational system performance while reducing the logistics burden for tactical units. They are also transportable by various means, resilient to damage, easy to operate and maintain, and scalable to different needs.

ESTABLISHED PLAYERS

The defense primes and large tech companies building in the HDES space, such as Lockheed Martin, Boeing, Northrop Grumman, Honeywell, Microsoft, and IBM, are going to play a large role in HDES' future development while being well positioned to invest in HDES startups via corporate VC funds.

6. Hypersonics

> **We see significant investments made in tests and evaluation infrastructure and our universities [for hypersonics]. It's a much more optimistic picture today than a few years ago.**
>
> **– Mark J. Lewis, Ph.D.**
> CEO, Purdue Applied Research Institute

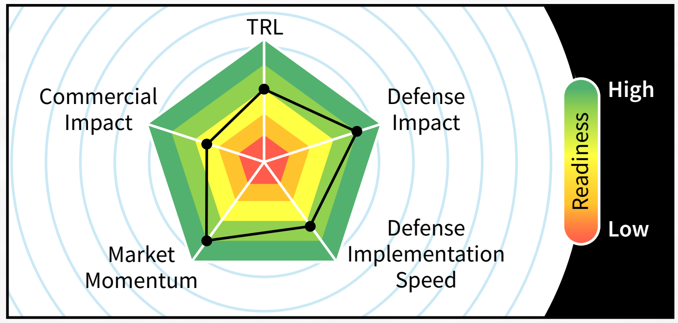
Executive Summary

Definition: Hypersonic propulsion refers to an object traveling faster than Mach 5 (five times the speed of sound). Generally, "hypersonics" today refers to technologies that allow for the testing and production of weapons that achieve these speeds.

Technology: The U.S. military is currently pursuing two types of hypersonic weapons: cruise missiles equipped with an air-breathing jet engine, or "scramjet," and glide vehicles that are launched into the air, then glide to their targets at high speeds. Advances in digital technology, such as modeling and simulation (M&S), are enabling cheaper hypersonic R&D and shortening the path to innovation and scaling.

Strategic Insight: With great distances between the U.S. and its adversaries, and with China attempting to create an "impenetrable bubble" in the Indo-Pacific, long-range hypersonics that can strike at speed will be a key component of the U.S. (and enemy) arsenal.

Future: Hypersonics will essentially shrink the globe. If hypersonics are harnessed properly in the more distant future, the U.S. will be able to deter threats and transport resources around the world in a matter of minutes.



Peace Through Deterrence

Hypersonic propulsion refers to an object traveling faster than Mach 5 (five times the speed of sound). To put this into perspective, hypersonic speed equates to a four-minute commute from Washington, DC, to New York City. In today's world, the term "hypersonics" is typically associated with aircraft and, more commonly, with missiles. While there are commercial applications, such as passenger transport and space launches, hypersonics are primarily used for, and associated with, military or defense applications.

Technology: Objects traveling at hypersonic speeds require advanced propulsion systems that must be carefully developed through numerous design iterations and test events. Consequently, there are two technology classes associated with hypersonics: propulsion and M&S.

Hypersonic propulsion systems come in several forms but can be categorized as either liquid or solid fueled. These types of engines can be applied to manned or unmanned vehicles, such as the North American X-15

USE CASES

- Long-Range Strike
- Commercial Transportation
- Supply Chain/Logistics
- Counterstrikes

<< Back to Table of Contents

or hypersonic glide vehicles (HGVs). An HGV uses a rocket engine to reach high altitudes, then leverages gravity and aerodynamics to reach hypersonic speeds as it descends toward its target.

Hypersonic engines can also be applied to ballistic missiles, allowing them to travel unpredictably—from an adversarial perspective—at high speeds, something previously unachievable. Hypersonic cruise missiles (HCMs) typically travel at low altitudes, achieve initial hypersonic speeds via rocket engine, and maintain them using a supersonic combustion ramjet (scramjet). Ramjets are innovative, as they use the vehicle's speed to compress and extract surrounding air for combustion. This eliminates the need for onboard oxidizers to fuel the engine, reducing overall weight and increasing stealth and thermal efficiency.

The best way to ensure a hypersonic vehicle design is ready for production and flight is through proper test and evaluation (T&E). When hypersonic speeds are reached, friction and air resistance cause the temperature surrounding the vehicle to become so great that airflow, thermal loads, and combustion processes must be considered. However, manually re-creating this flight process in a physical T&E environment is currently difficult, slow, and expensive. In fact, it can cost up to $100 million for a single flight.

Therefore, M&S technology has emerged as a cost-effective alternative to traditional T&E techniques. M&S of hypersonic flight is achieved by integrating various physical models and computer programs to simulate the aerodynamic phenomena experienced during flight.

Strategic Insight: Hypersonic propulsion technology is not a new concept; in fact, it has been studied for over 60 years. However, innovation in digital M&S capabilities is making the technology more feasible and attainable on the battlefield—especially when a future battlefield may span across oceans, making increased speed to attack an essential capability. Not only is the U.S. thousands of miles from adversaries, but foreign military strategies, like China's anti-access/area denial (A2/AD) bubble, prevent local allied bases from engaging. This reinforces the need for domestic weapon systems capable of deterrence from range.

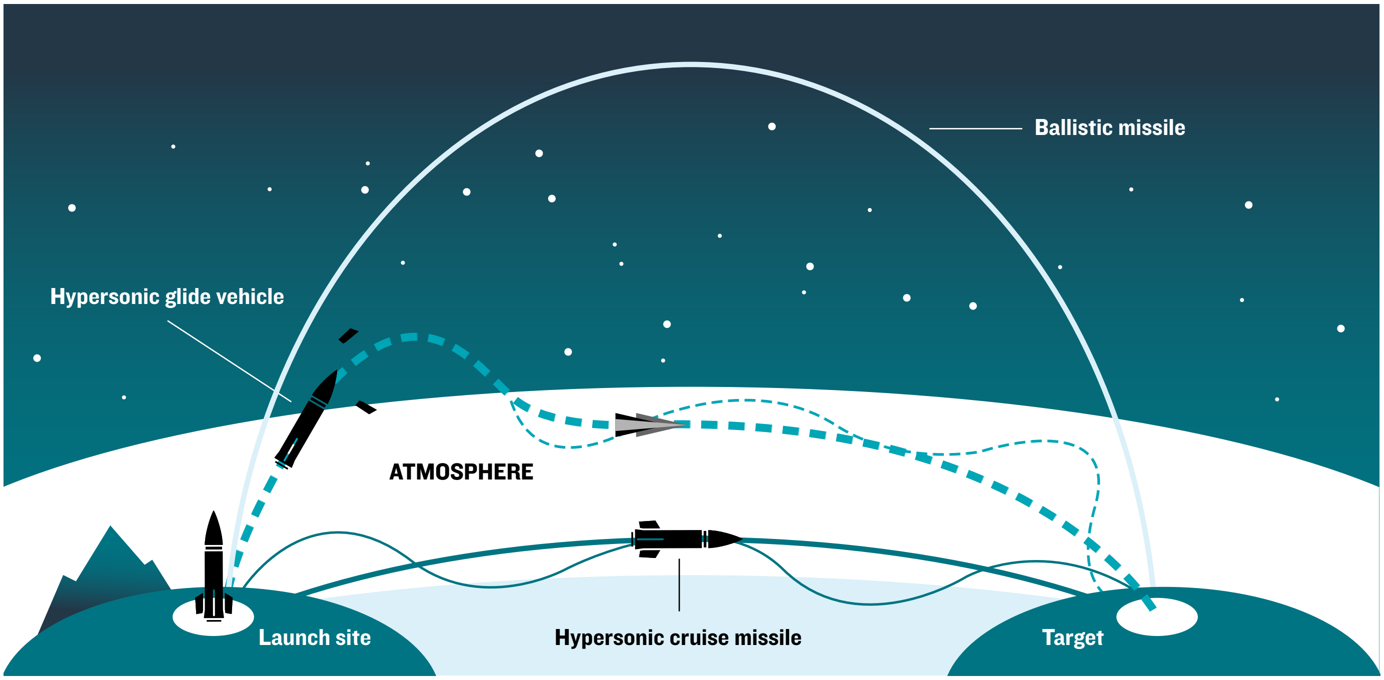


Figure 12: *The figure shows the difference between the two main flight patterns of hypersonic weapons—HGVs initially travel on a parabolic trajectory and glide down toward a target, while hypersonic cruise missiles remain at low altitudes during flight. Source: GAO-21-378.*

Hypersonics Investment Trends

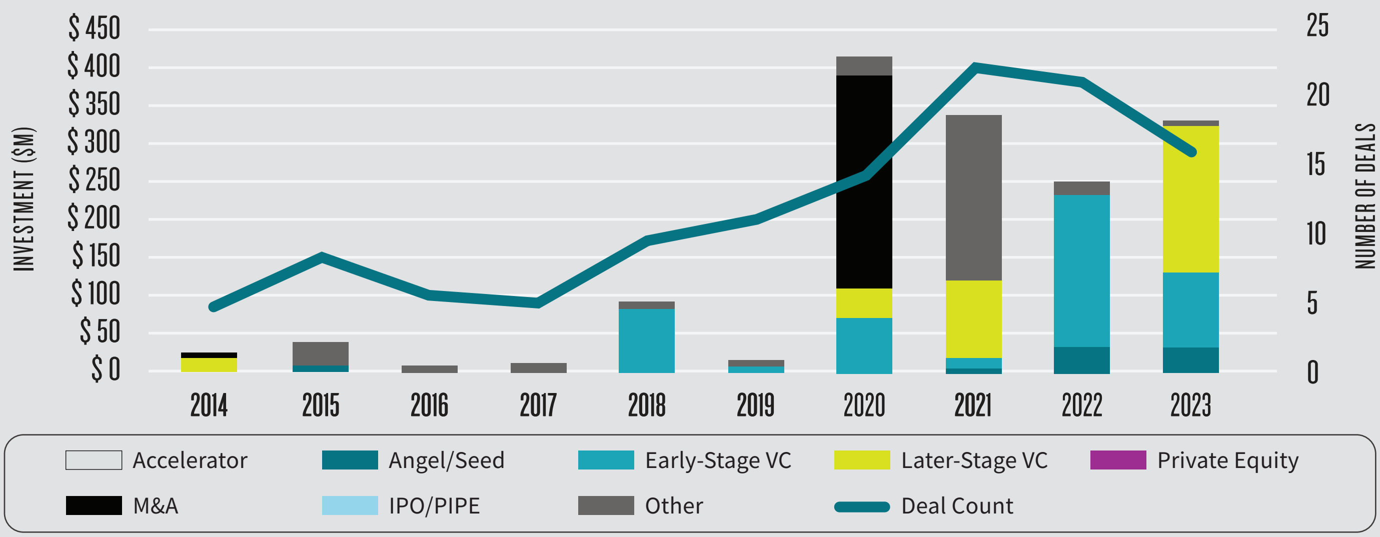


Figure 13: *National and international hypersonic investment interest has gone through cycles, fluctuating significantly for decades. Recent interest in hypersonics has exploded as overseas threats have emerged and attention has turned from counterterrorism to Great Power Competition in the Indo-Pacific, generating robust foreign adversary investment and highlighting a need to strike and deter from range. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

USG interest is evident and backed by significant funding. In 2023, the U.S. Navy made a $1.2 billion award to integrate hypersonic missiles within the Navy's Zumwalt destroyer. The USAF also awarded $985 million in 2022 for air-launched, scramjet-powered hypersonic weapons. Much of this interest may be driven by necessity—the U.S. is not the only country interested in the ability to strike from range. Foreign adversaries like China, Iran, North Korea, and Russia continue to invest heavily in the development of advanced hypersonic propulsion and missile systems. In addition to trying to win the offensive hypersonics arm race, DOD has begun bolstering its sensor-based tracking systems as well as its counter-hypersonic missile interceptors.

Future: Large defense contractors will likely always own production of hypersonic systems and integrations, but up-and-coming startups will continue to push the envelope with regard to digital simulation and other component solutions. These technologies enable a quicker pace of innovation and scaling, allowing the U.S. to build a larger fleet that's easier and cheaper to test while strengthening our ability to strike and deter from a distance.

In the distant future, hypersonics development will enable both domestic and military travel to become exponentially more efficient, allowing for faster response times and expedited access to military units abroad. From an arsenal perspective, hypersonic innovation will enable more attainable global production of sophisticated, long-range, less detectible missile systems—an exciting opportunity but also an exacerbating threat to national security. As the U.S. continues to grapple with potential adversaries halfway across the world, the hypersonics arms race is one we cannot afford to lose.

Emerging Innovators

Non-Exhaustive

In the defense world, hypersonic technologies primarily refer to vehicles and weapons traveling at hypersonic speeds. However, creating such technologies requires immense and iterative T&E processes. As defense and commercial entities look to validate their hypersonic designs, companies are emerging to create low-cost, reusable T&E environments. Moreover, to power these designs, companies such as Hermeus, Specter Aerospace, and Castelion have taken on the challenge of developing propulsion systems that can launch these designs into production. With the advent of these hypersonic propulsion systems, companies like Venus Aerospace and Velontra believe DOD can extend its range and conduct speed-dependent missions that will bolster national security.

Castelion

HQ: El Segundo, CA

TOTAL RAISED: $14.2M

SERIES: Seed

USG TRACTION: Multiple undisclosed USG contracts

Castelion was founded in late 2022 by former SpaceX leaders to bring a modern, agile hardware development and mass production strategy to long-range strike weapons. The company believes that America's pace of innovation in weapons development has fallen behind that of rising authoritarian states and seeks to put the U.S. back in a leadership position. Castelion is internally developing new, mass-manufactured hypersonic and tactical strike weapon systems, including designing and producing its own solid rocket motors, avionics, and thermal protection systems. The company is currently ground testing and will begin flight testing in 2024.

Hermeus

HQ: Atlanta, GA

TOTAL RAISED: $118M

SERIES: Early Stage

USG TRACTION: USAF, DIU

Hermeus is an aerospace and defense technology company founded to radically accelerate air travel by delivering hypersonic aircraft. The company aims to develop hypersonic aircraft quickly and cost-effectively by integrating hardware-rich, iterative development with modern computing and autonomy. This approach has been validated through design, build, and test of the company's first combined turbojet-ramjet engine and is now being scaled through its first flight vehicle program, Quarterhorse. In partnership with the U.S. Air Force, Hermeus is also developing Darkhorse—an uncrewed hypersonic aircraft designed to deliver unique asymmetric capabilities to the warfighter.

Specter Aerospace

HQ: Peabody, MA

TOTAL RAISED: $20M

SERIES: Later Stage

USG TRACTION: USAF, U.S. Navy, NASA

Founded in 2013, Specter Aerospace, formerly FGC Plasma Solutions, is a venture-backed startup with offices in the Boston, Massachusetts, and South Bend, Indiana, areas. Specter works to develop hypersonic systems for future defense and commercial applications, leveraging its developments in advanced propulsion, affordable structures, and digital engineering. Powered by extended operability ramjets and scramjets, the hypersonic weapons Specter Aerospace is developing will provide Joint Force partners with additional options for extended-range, time-critical, affordable strikes.

Velontra

HQ: Lebanon, OH

TOTAL RAISED: $2.3M

SERIES: Early Stage

USG TRACTION: USAF, USSF

Velontra is an aerospace technology company that will offer orbit access from any runway, using its HyperLaunch system. HyperLaunch uses an air-breathing, hypersonic aircraft first stage and liquid-rocket second stage to deliver payloads to orbit, significantly lowering costs while dramatically increasing launch reliability. Velontra seeks to change the modern defense acquisition paradigm by leveraging venture and DOD funding to offer a series of dual-use, revenue-producing products that develop requisite technologies in a timely, cost-effective manner. Air-breathing propulsion is at the core of the company's expertise, and its initial product offering, Bronco, is a small, low-cost, supersonic propulsion system.

Venus Aerospace

HQ: Houston, TX

TOTAL RAISED: $48.2M

SERIES: Early Stage

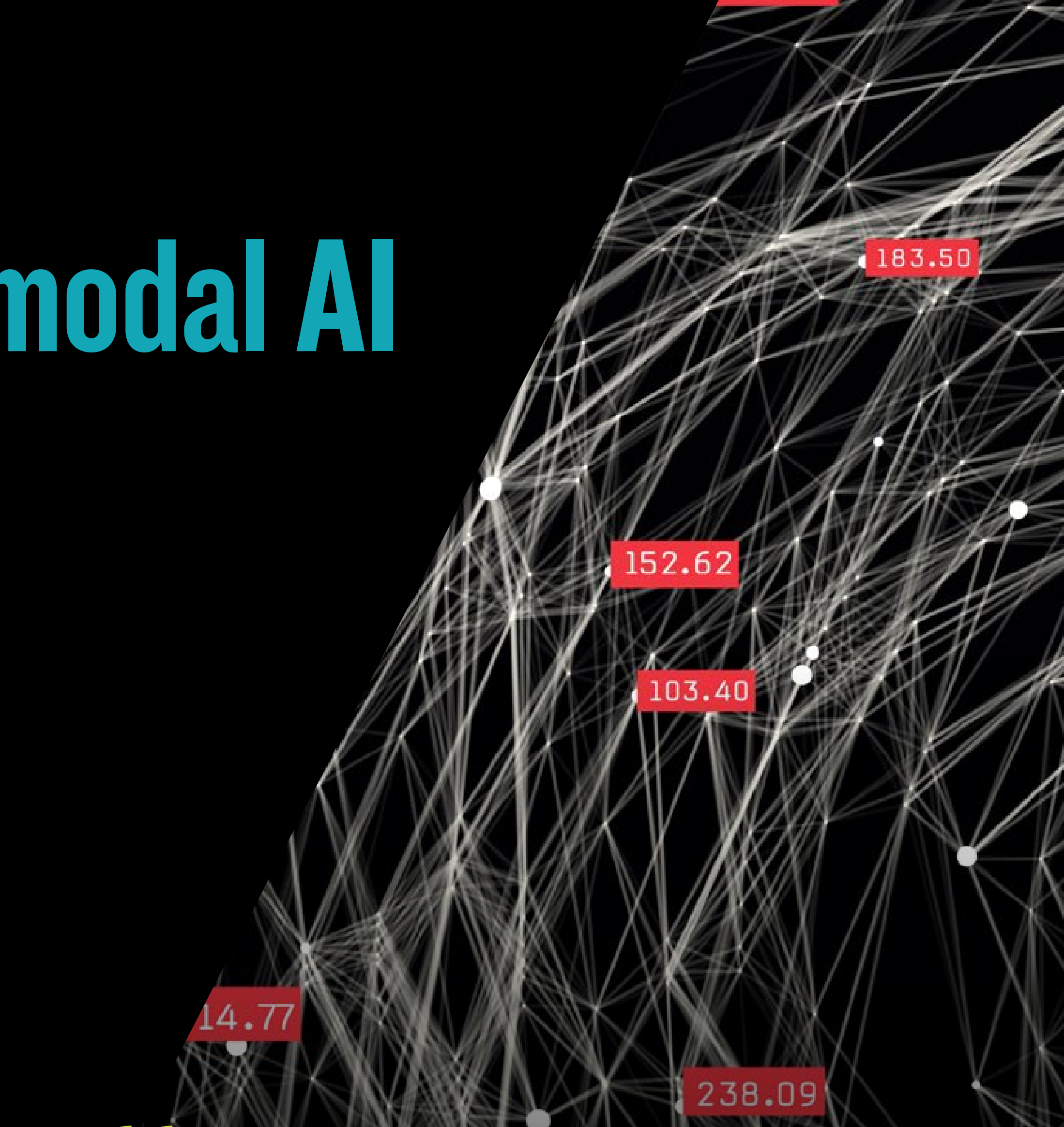
USG TRACTION: USAF, NASA

Venus Aerospace is a venture-backed, dual-use hypersonic aerospace company. With a focus on high-speed commercial transportation and multi-mission defense applications, Venus is developing novel rocket propulsion systems and a unique vehicle design for hypersonic travel. The Rotating Detonation Rocket Engine (RDRE) is at the core of Venus' approach to hypersonics, which enables flight profiles in lower heat environments and at altitudes greater than 140,000 feet, an altitude other air-breathing aviation platforms cannot access. This innovative rocket engine is compact and efficient, with increased performance. A hypersonic-capable DOD will extend range and speed-dependent operational missions, protecting our overall national security.

ESTABLISHED PLAYERS

Large defense primes and defense contractors, such as Lockheed Martin, Boeing, Northrop Grumman, and Raytheon, will continue to play an integral role in developing and integrating hypersonic weapons systems.

7. Multimodal AI



> **Anything related to human behavior, from operating a machine to expressing chronic pain, requires a multimodal AI approach. Like having only one piece of a complex puzzle, no one modality, like imagery, is sufficient to train the algorithm. Like many trends nowadays, what is old is new. Multimodal AI has been around for some time, but now, with access to data, compute, and diverse architectures, we are closer to infusing multimodality into all AI.**
>
> **– Catherine Ordun, Ph.D.**
> Vice President, Booz Allen Hamilton

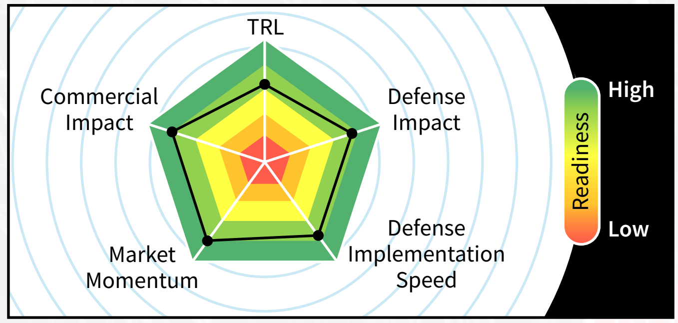
Executive Summary

Definition: Multimodal AI (MMAI) models can ingest and/or output more than one data type. Our report focuses on multimodal fusion of inputs.

Technology: Deep neural networks are being trained to understand different types of data in relation to each other. The notion of multimodality is not new—it has been an area of research and proven success in effective computing for decades. However, with the ability to acquire diverse data and combine algorithms, fusion is becoming a more commonplace method of training AI models across multiple signals. MMAI can be used in a variety of tasks, including recommendation systems, language understanding, image generation, and SOTA biometrics.

Strategic Insight: The ability to fuse different types of intelligence into an output that informs decision making is the key business of the Pentagon, and multimodal models that enable this will be in high demand. Nascent DARPA, Task Force Lima, and SBIR efforts point to the importance of multimodal algorithms for intel-aggregation, human behavior prediction, deepfake detection, and predictive maintenance.

Future: Multimodal algorithms are the foundation of high-performance and trusted AI—every model of consequence will incorporate all relevant data types to automate analysis. MMAI is a step toward future artificial general intelligence (AGI), which many believe will enable algorithms to learn, understand, and perform a wide range of tasks on their own.



Context-Aware AI

MMAI refers to AI models that can ingest and/or output more than one type of data. For this report, we focus on MMAI that can fuse different types of input, such as text, images, or much more mission-specific information, in relation to each other and produce a desired output—emulating how humans gather and interpret information. The goal of multimodal models is to create AI that distills information from multiple signals to make decisions based on different points of view. This is a departure from traditional AI development, where models often make decisions based on a limited breadth of relevant information. As DOD wrestles with implementing AI in high-stakes environments, MMAI is poised to enhance trust in models and analysis.

Technology: MMAI is not a new concept—in fact, MMAI derives from legacy AI concepts of multi-sensor interfaces, where information is gathered from imagery, audio, and other unstructured, static, or dynamic inputs. Netflix, Amazon, and Spotify all use MMAI that trains on multiple data types and learns data patterns using different fusion

USE CASES

- Intelligence Fusion
- Human Behavior Prediction
- Deepfake Detection
- Predictive Maintenance
- Healthcare Diagnosis

algorithms, resulting in customized recommendations. As AI continues to progress, multimodal algorithms will remain the foundation of sound model development—no single data type holds the explanatory power needed for proper analysis of hard-to-solve problems.

However, this realization means MMAI is now reaching an inflection point where it is being developed and is in demand by every industry for nearly every use case—GPT-4's launch and incorporation of imagery inputs is just one example. In 2022, ABI Research predicted that the total number of devices that include MMAI capabilities would grow from 3.9 million in 2017 to a staggering 514 million by end of 2023. The recent maturation comes as a result of the increased compute power now available to train the deep neural networks that power MMAI. The requirement for greater computing power stems from the incredible training and operating complexity of multivariate models, which require more sophisticated architectures compared to single-modality AI models.

For some use cases, multimodal sources entail the obvious examples—text, images, video, and audio. However, DOD's interest will extend beyond these data types into the niche modalities essential to its missions. For intelligence-based insights, this could include the expanse of data needed across space and time to predict human behavior. For other use cases, such as detecting deepfakes, models may incorporate "sub-modalities" to uncover manipulation imperceptible to the human eye—this could include saccades (iris movement and fixation); gestures; intonation patterns; and spectral signatures, such as artifacts and stippling.

Strategic Insight: MMAI promises to alleviate the manual burden of analysis by automating pattern recognition and insights across huge, diverse datasets. For most use cases, humans will remain in the loop and make key decisions but spend significantly less time making sense of raw data. This is true for AI in general, but MMAI's purpose is to learn information from diverse datasets to make the model more contextually aware and potentially more trustworthy due to liberation from dependence on one single data type.

MULTIMODAL DEEPFAKE DETECTION

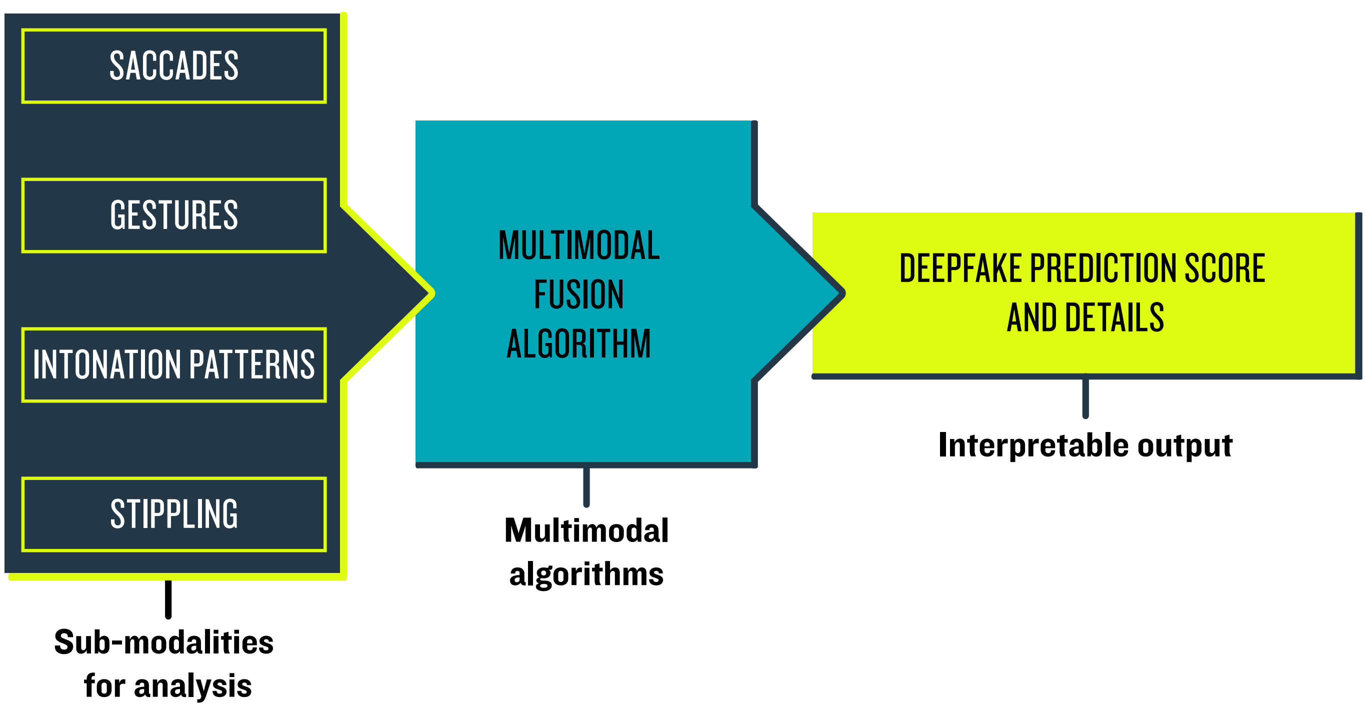


Figure 14: *The graphic above illustrates a simplified, hypothetical MMAI architecture for a model attempting to identify deepfake videos. Sub-modalities such as those listed above must be considered in relation to each other to uncover signs of synthetic manipulation.*

 |

Multimodal AI Investment Trends

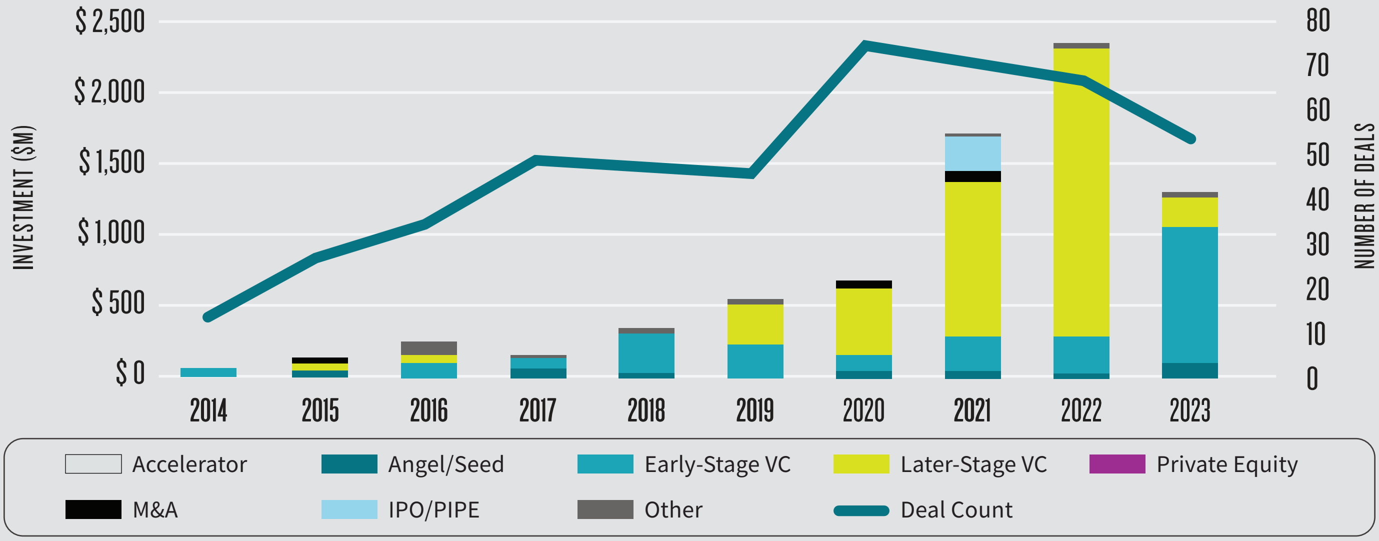


Figure 15: *Multimodal AI is seeing increased investment as it becomes more viable and the demand for predictive, trusted AI increases. Note: late-stage VC has dominated investment flows, reflecting an initial desire by investors to double down on investments with bigger players. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

Several defense use cases are currently primed for adoption of MMAI analysis. At the forefront is the use of all-source intelligence to predict human behavior, benefiting both the intelligence community (IC) and DOD. MMAI aims to aid the IC's SOTA biometrics (e.g., gait, facial recognition, heat signature, acoustics) and DOD's object detection by merging imagery and geospatial data. Ultimately, MMAI holds the promise to build a complete body of information that will enhance an AI's ability to power more accurate predictions, make more precise recommendations, and generate more aligned outputs. Humans are complex, and no single modality AI can provide predictive power in isolation. Rather, all-source intelligence must be assessed holistically, taking into account data such as emotional state, infrared readings, voice tone, social media posts, and cyber indicators. Recent government solicitations regarding the information environment, often worth more than $100 million, allude to the importance of emerging tech in understanding and making sense of these diverse indicators that are now available for analysis.

Further, as the U.S. attempts to close the kill web from sensors to shooters in lethal and nonlethal contexts, understanding the variety of data generated in a Joint All-Domain Command and Control (JADC2) scenario is inherently a multimodal undertaking. Future models will be able to assist in this task through programs such as the U.S. Army's Project Convergence or the USAF's Advanced Battle Management System. Models analyzing disparate pieces of information, such as terrain, intelligence sources, and logistics, make sense of data patterns and deliver initial mission-planning recommendations, potentially consolidating a monthlong process into minutes.

Future: MMAI is a step toward AGI, which enables algorithms to learn, understand, and perform almost any task on their own, exceeding human performance. Today, AI models collect specific data and achieve specific tasks—a predictive maintenance algorithm intakes equipment telemetry and outputs when it requires preemptive care. In the future, humans will begin to interact with AI agents that collect all available data and provide timely insights across use cases. For example, the same AI interface, albeit further out, may notify an operator of a deepfake circulating the internet; contextualize it within an adversary's information warfare campaign; surface a variety of sensor- and satellite-based geospatial intelligence (GEOINT) to dispel the falsified images; and make suggestions on counter-information campaigns to recontrol the narrative and disseminate legitimate information.

Emerging Innovators

Non-Exhaustive

MMAI can be used across a wide range of use cases and industries, and current and future iterations hold the potential for diverse applications for DOD. Primordial Labs is an early-stage startup looking to enable multimodal C2 of unmanned systems prompted via natural language. Pryon is an enterprise platform that fuses different data sources from an organization into a knowledge repository that can be queried. Reality Defender detects deepfake-altered media by assessing different data and metadata points, and Twelve Labs offers multimodal video analytics that enable natural language search of videos.

Primordial Labs

HQ: New Haven, CT

TOTAL RAISED: $4M

SERIES: Seed

USG TRACTION: SOCOM, U.S. Army

Primordial Labs' Anura platform enables drone operators to command and control uncrewed systems by voice through a natural language human-machine interface. Platform-agnostic and already integrated on several different OEM drones, the Anura platform ingests natural language commands and uses AI/ML processes to infer the operator's intent, ground that intent in the real-time operational context, and drive real-world actions, such as flying complex ISR missions. Anura's hierarchical autonomy architecture allows for a highly tailorable mix of ML and traditional robotic controls to meet specific mission needs across domains and use cases.

Pryon

HQ: Raleigh, NC

TOTAL RAISED: $139.2M

SERIES: Early Stage

USG TRACTION: Undisclosed

Founded by the minds behind Alexa, Siri, and Watson, Pryon's full-stack AI platform securely transforms multimodal assets, including audio, images, text, and video, stored in myriad sources, including Amazon S3, SharePoint, and other applications, into a knowledge fabric. By using natural language prompts, warfighters can unlock fully attributed, verifiable answers or reports that have been extracted or generated from complex, unstructured content, including PDFs, PowerPoints, and Word files. Use cases include acquisitions, business operations, and intelligence. Pryon is a National Security Innovation Network (NSIN) company and is being scaled at leading brands, such as Dell, NVIDIA, and the World Economic Forum.

 |

Reality Defender

HQ: New York, NY

TOTAL RAISED: $22.42M

SERIES: Early Stage

USG TRACTION: DOD, DHS

Reality Defender's deepfake detection platform uses multiple concurrent detection models and methods to identify AI-generated content within audio, video, images, and text. By applying simultaneous detection methods for every scan, the platform detects AI-generated content across modalities, giving agencies and institutions a first line of defense against advanced AI-powered fraud attacks and disinformation campaigns. Regular upgrades empower detection models to provide proactive protection against current threats and potential future risks well before they surface.

Twelve Labs

HQ: San Francisco, CA

TOTAL RAISED: $22.09M

SERIES: Seed

USG TRACTION: N/A

Twelve Labs is a multimodal search company that extracts multiple features from video, such as time, objects, text, conversation, people, and actions, to synthesize the vast amount of information into vectors. Vectors enable fast, semantic, and scalable search. The Twelve Labs API allows for SOTA, highly accurate video search infrastructure to be integrated in fewer than 20 lines of code, enabling context-specific search and insights, and effectively replacing ineffective keyword tagging.

ESTABLISHED PLAYERS

The large tech companies building and innovating in the multimodal space, like Google, Microsoft (OpenAI), and Meta, are going to play a large role in MMAI's future development and are well positioned to invest in MMAI startups.

8. Non-Kinetic Counter-UAS

"While the ability to take down a drone with a single pulse is critical today, it only hints at the paradigm shift that is happening."

– Joe Lonsdale
Managing Partner at 8VC
and Co-Founder of Epirus

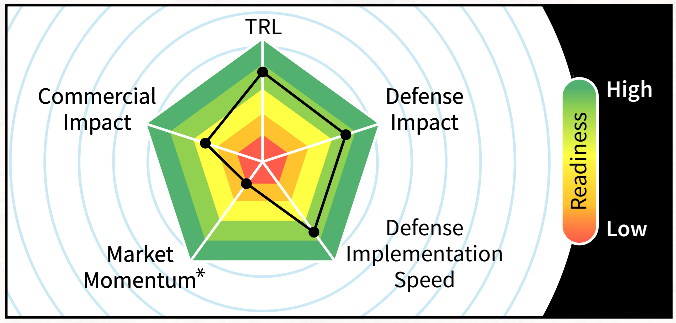
Executive Summary

Definition: Non-kinetic counter-UAS is a subset of counter-UAS (c-UAS) focused on disabling small- and medium-sized drone threats using effectors such as RF jamming, cyber takeover, or directed energy.

Technology: RF jamming and cyber takeover disrupt operator and UAS communication, making them essential to combat COTS systems. For more advanced threats, directed energy will be the preferred effector. C2 may be the most pressing technical challenge—for c-UAS to be effective against a variety of threats, multiple effectors need to be layered and largely automated.

Strategic Insight: For the U.S., the pacing threat for c-UAS technology is China's development of autonomous drones and swarm technology. The U.S. Joint Counter-small Unmanned Aircraft Systems Office (JCO) spent over $700 million on c-UAS research and procurement in 2023. Recent statements suggest that non-kinetic effectors may be preferred for neutralizing those emerging swarm threats.

Future: As drones become more popular in society and the battlefield, future c-UAS will be characterized by AI-driven C2 systems that fuse sensor data, rapidly identify novel threats, and automate an optimal response with human oversight.



***Note:** Due to an anomalously low year of funding in 2023, the CAGR of this market from 2018 to 2023 is skewed very low. However, the investment trend of the years prior suggests a much more optimistic outlook to this industry—see Figure 17.*

Defending Against Evolving UAS Threats

Non-kinetic counter-UAS is a subset of c-UAS focused on disabling small- and medium-sized drone threats using effectors such as RF jamming, cyber takeover, or directed energy. Effector systems, whether kinetic or non-kinetic, are generally used in combination with drone detection and identification technologies, such as RF, radar, optical, and/or acoustic sensors. As militaries field large quantities of small, low-cost drones that increasingly have autonomous capabilities, air defenses will require a level of evolution from kinetic to non-kinetic defenses that are backed by AI-defined C2 software.

USE CASES

- Swarm Defense
- Base Protection
- Mobile Air Defense
- Directed Energy Hypersonic Defense
- Crowd Protection

Technology: Within the non-kinetic c-UAS space, RF jamming, spoofing, and cyber takeover are key methods for mitigating drones operated by RF communications links, such as remotely piloted drones. RF-based c-UAS will continue to be vital in both commercial and defense settings to combat COTS drones, such as those made by Chinese manufacturer DJI. However, advances in autonomous drone technology will progressively decrease RF-based c-UAS efficacy on the battlefield and necessitate hard-kill solutions capable of neutralizing dozens or hundreds of autonomous drones at a time.

This is where directed energy comes into play. Directed energy weapons take two forms: high-energy lasers (HELs), which use concentrated light to inflict physical damage on a target, and high-power microwaves (HPMs), which emit electromagnetic energy that overwhelms a target's electronics.

Of the two, HPMs have a broader area of effect, making them ideal for missions that require swarm-defeating capabilities. While traditional HELs and HPMs are technically mature, several issues have impeded their adoption by DOD, including cooling and SWaP challenges. However, the more enduring challenge—and opportunity for innovation—may lie in the C2 of layered c-UAS solutions. To keep pace with rapid advancements in autonomous drones, future c-UAS solutions will need to be largely automated to speed up sense-shoot decision making (while still having a "human on-the-loop").

Strategic Insight: While conflicts in Ukraine and Israel provide ample evidence for the need to defeat attritable low-cost drones, the forcing function for DOD adopting non-kinetic c-UAS effectors—especially HPM—is the PRC. The PRC views autonomous drones and swarm technology as an asymmetric capability and has mobilized its military, university system, and venture capital ecosystem to prioritize their development. U.S. warfighters will need to be able to rapidly defeat such capabilities at scale.

The Army's JCO leads DOD small c-UAS strategy and directs R&D spending across the services. Meanwhile, procurement strategy and acquisition authority remain at the service level. Directed energy is especially of interest

Notional Depiction of High Power Microwave and High Energy Laser Defending an Installation

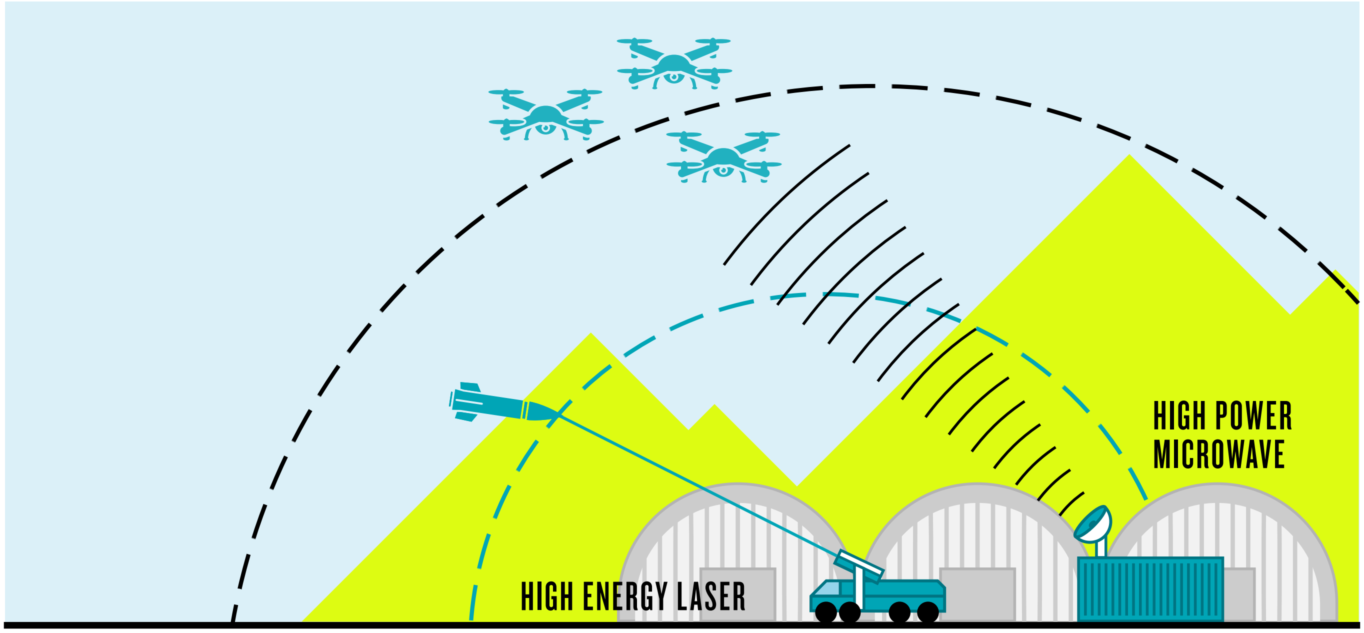


Figure 16: *Depiction of HPM and HEL directed energy systems in action. HPM systems may be preferred for autonomous swarming threats, an innovation priority for China. The SWaP of directed energy systems are improving. Range, while generally classified, is also increasing. Source: GAO-23-105868.*

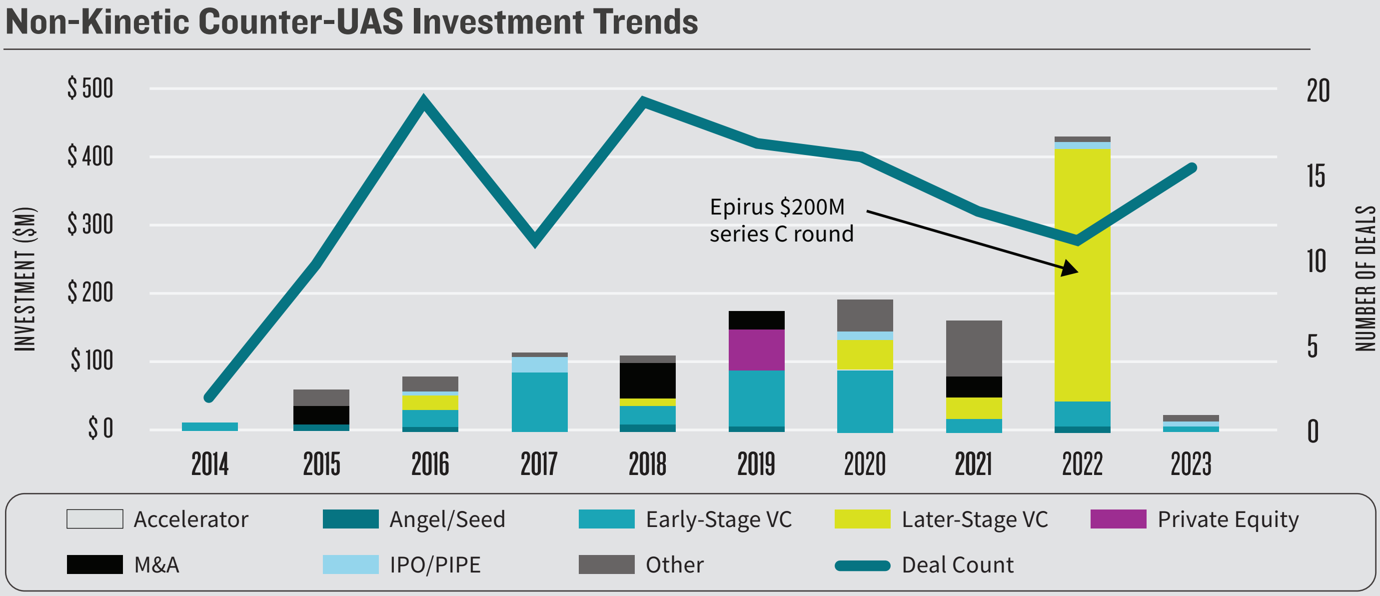


Figure 17: *Investment in non-kinetic c-UAS has evolved from early-stage VC to later funding stages. In 2022, three later-stage venture deals dominated the year's funding. This signals that non-kinetic c-UAS technologies and the market may be more mature compared to other ecosystems, and several companies have emerged as winners. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

within the c-UAS realm—GAO estimates that DOD at large is spending approximately $1 billion annually on researching, testing, evaluating, and procuring directed energy systems. JCO Chief of Acquisition and Resources Col. Michael Parent recently noted that a June 2024 demonstration will focus heavily on non-kinetic solutions because of the difficulties kinetic weapons have with drone swarms up to 50 in number.

Future: China and other adversaries will continue to rapidly innovate in swarming and lethal unmanned capabilities; in the future, high-risk autonomous drone conflict may occur often and abruptly. Therefore, c-UAS systems must be adaptable, intuitive, and driven by AI that can determine optimal responses based on the fusion of data from all pertinent sources. Forward operators will not have the time or luxury to review all available information and deliberately craft a response to incoming drone threats. Rather, future systems will be highly trusted through extensive T&E, and c-UAS responses will be automated with precautionary human oversight.

In addition to this decision support component, future systems will be smarter and incorporate AI that can recognize novel approaching threats rather than a library of existing ones. On a more tactical side, systems will continue to decrease in size and require less power, making them more mobile and operationally feasible. Dispersed warfighters operating in logistics- and communications-denied environments will come to rely on portable directed energy systems backed by AI decision support. And lastly, advancements in effector range and precision will be essential for complex unmanned battlefields of the future—a future which may not be far off.

Emerging Innovators

Non-Exhaustive

c-UAS startups are maturing and finding their way into defense and civil missions. Epirus, a California-based HPM startup, is improving SWaP metrics through innovative cooling techniques, incorporating AI-defined precision targeting and integrating with advanced C2 software like Anduril's Lattice platform. Other companies, such as High Point Aerotechnologies, are building modular AI C2 software that automates the c-UAS kill chain through threat evaluation and effector queuing. Hidden Level automates sensing for non-kinetic solutions, while D-Fend Solutions provides cyber and RF effects.

D-Fend Solutions

HQ: McLean, VA (alternate)

TOTAL RAISED: $34.5M

SERIES: Early Stage

USG TRACTION: DOD, DHS, DOJ, FAA

D-Fend Solutions provides RF cyber-based counter-drone takeover technology, enabling control, safety, and continuity during rogue drone incidents across complex environments, including military and homeland security. EnforceAir, D-Fend's core offering, detects, locates, and identifies rogue drones in protected airspace, neutralizing threats by taking control of and landing the drones safely in a predefined zone. The EnforceAir non-jamming, non-kinetic technology provides end-to-end detection and mitigation for situational awareness, operational continuity, and safe controlled outcomes.

Epirus

HQ: Torrance, CA

TOTAL RAISED: $312M

SERIES: Later Stage

USG TRACTION: U.S. Army, U.S. Navy, USAF, DARPA

Epirus is a high-growth technology company developing software-defined, solid-state, long-pulse HPM systems with devastating counter electronic effects on modern drone threats. The Epirus Leonidas HPM family of products, powered by AI and advances in gallium nitride, is human-safe, cost-effective, and production-ready. Distinguishing itself from laser and kinetic counter-drone solutions, Leonidas excels against drone swarms while also bending the cost curve back in DOD's favor, taking drone-defeat costs from millions of dollars per drone to pennies on the dollar.

Hidden Level

HQ: Syracuse, NY

TOTAL RAISED: $41M

SERIES: Early Stage

USG TRACTION: USAF, U.S. Army

Hidden Level is a next-generation sensor company, specializing in the design and manufacture of RF/electromagnetic spectrum sensing solutions with applicability to airspace awareness, c-UAS, and signals intelligence use-cases. Hidden Level designs and manufactures a variety of sensors, including multi-band passive radar in a low SWaP form factor that can be used in both fixed and mobile instances. The company serves both commercial and defense markets through stand-alone hardware or as a flexible, networked Data as a Service (DAAS) solution which highlights different pertinent data to different user groups.
**Invested in by Booz Allen Ventures*

High Point Aerotechnologies

HQ: Dallas, TX

TOTAL RAISED: Merger

SERIES: Private Equity

USG TRACTION: U.S. Army, AFRL, SOCOM

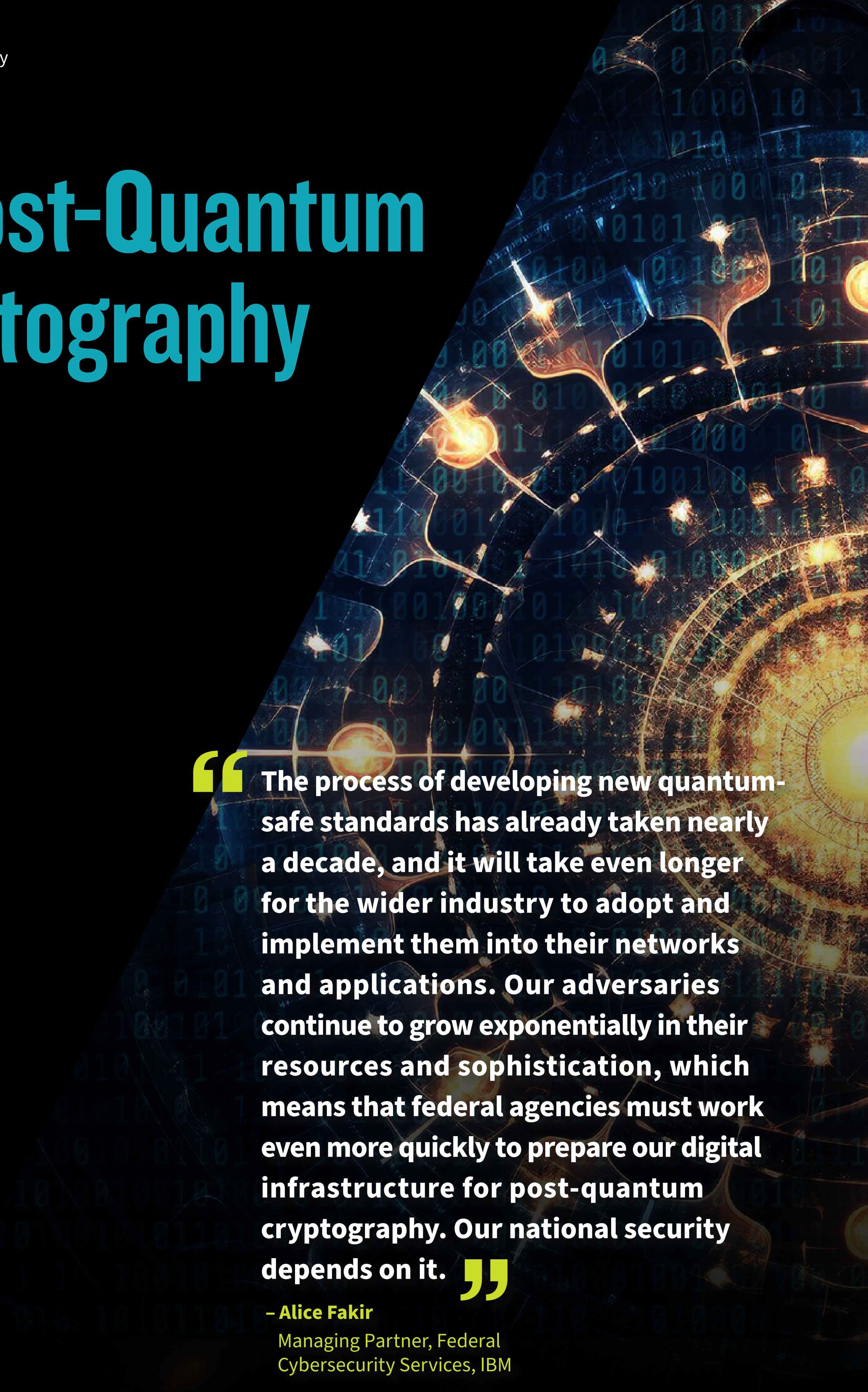
High Point Aerotechnologies develops c-UAS solutions across air, land, and maritime domains. Its innovative solutions and DefenseOS open architecture software environment enable operations at machine speed to detect, identify, track, and defeat UAS and other conventional and autonomous threats. Formed through the merger of Black Sage Technologies and Liteye Systems, High Point offers an array of integrated, interoperable solutions to provide fixed, mobile, and distributed c-UAS capabilities for civilian, military, and critical infrastructure clients.

ESTABLISHED PLAYERS

Non-kinetic c-UAS is an industry that only succeeds because of collaboration among the Joint Force, defense primes, and startups. In the race for innovation, startups will continue this collaboration due to the defense nature of the industry. Defense prime contractors like Northrup Grumman, General Dynamics, Lockheed Martin, and Anduril will continue to play an integral role in c-UAS development and integration. Anduril's recent launch of Roadrunner-M, its vertical take-off and landing (VTOL) autonomous air vehicle, is one example of a promising next-generation (albeit kinetic) solution.

<< Back to Table of Contents

9. Post-Quantum Cryptography



The process of developing new quantum-safe standards has already taken nearly a decade, and it will take even longer for the wider industry to adopt and implement them into their networks and applications. Our adversaries continue to grow exponentially in their resources and sophistication, which means that federal agencies must work even more quickly to prepare our digital infrastructure for post-quantum cryptography. Our national security depends on it.

– Alice Fakir
Managing Partner, Federal Cybersecurity Services, IBM

 |

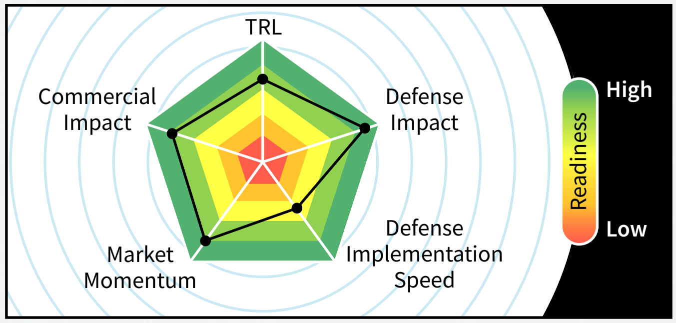
Executive Summary

Definition: Post-quantum cryptography (PQC) refers to mathematical algorithms—believed to be secure against attacks by current and future quantum computers—used to encrypt the private communications of individuals, organizations, and governments.

Technology: PQC is based on complex mathematical models for which no known quantum shortcut exists. NIST is in the process of standardizing these models for government and industry use while also advocating a framework of crypto-agility, or the ability to easily swap out encryption algorithms should the working one be compromised.

Strategic Insight: Secure data and communications are the bedrock of national security and economic prosperity. Time is of the essence, as the U.S.'s adversaries are already collecting our data in the hopes of decrypting it in the future with a quantum computer. Moreover, as transitioning to PQC is expected to take at least a decade and given the pace of quantum computing advances, organizations must act now.

Future: In the future, crypto-agility will be key to adapting to emerging vulnerabilities, and hybrid encryption protocols may also improve resiliency. Ultimately, only time will tell if existing PQC algorithms are secure against quantum computers, but continuous innovation of models will likely be necessary.



Cybersecurity in a Quantum World

Individuals, companies, and governments rely on public-key encryption (PKE) to protect private communications and sensitive data from eavesdropping and cyberattacks—similar to how a lock on a house's front door prevents intruders from entering without a key. PKE relies on the difficulty current computers have solving certain mathematical problems, such as factoring very large numbers or calculating elliptic curve discrete logarithms. However, quantum computers process information in a fundamentally different way than current classical computers, and it is believed they will soon be able to quickly crack many of today's PKE methods. In the future, when such a cryptographically relevant quantum computer (CRQC) comes online, any organization relying on current PKE will be vulnerable to hacks, making even the worst data breaches of recent years pale in comparison. Fortunately, new PKE algorithms, collectively known as PQC, are

USE CASES

- Critical Infrastructure
- National Security Intelligence
- Military Communications
- Financial Transactions
- Personal Health/Biometric Data

emerging that have the potential to defend against the looming quantum threat.

Technology: Quantum computing (QC) represents a profound technological revolution that, once sufficiently advanced, will be able to solve the math problems underlying current PKE relatively quickly and efficiently—a predicted future event humorously referred to as Y2Q ("years to quantum"). In the meantime, PQC algorithms are designed to secure information on today's classical computing hardware as well as on quantum computers. It is critical to understand that PQC relies only on complex math and does not require a quantum computer or any quantum phenomenon to implement, making it distinct from quantum encryption methods such as quantum key distribution (QKD).

In anticipation of Y2Q, NIST has been working to standardize PQC protocols, a process which began in 2016 and reached a major milestone in 2023 with the release of PQC draft standards. Unfortunately, due to the ever-changing quantum threat landscape, there is always a risk that a future quantum innovation might introduce a vulnerability to NIST's current PQC portfolio. Therefore, a key engineering framework to de-risk the uncertainty of PQC will be crypto-agility, in which flexibility is embedded into an organization's PKE infrastructure, allowing IT administrations to easily switch between algorithms in case one becomes compromised. Even without this crypto-agile framework, transitioning to new encryption protocols could take years—or even a decade—to complete. Organizations must take significant technical, financial, and logistical steps before they can fully adopt these new cryptographic techniques, including inventorying all their secure data and applications.

Strategic Insight: Though Y2Q is likely still several years away, PQC is quickly becoming a high priority given the accelerating pace of QC advances. It is widely accepted that foreign adversaries are vacuuming up encrypted American data—whether individual health data held

Possible Timeline to a Cryptographically Relevant Quantum Computer

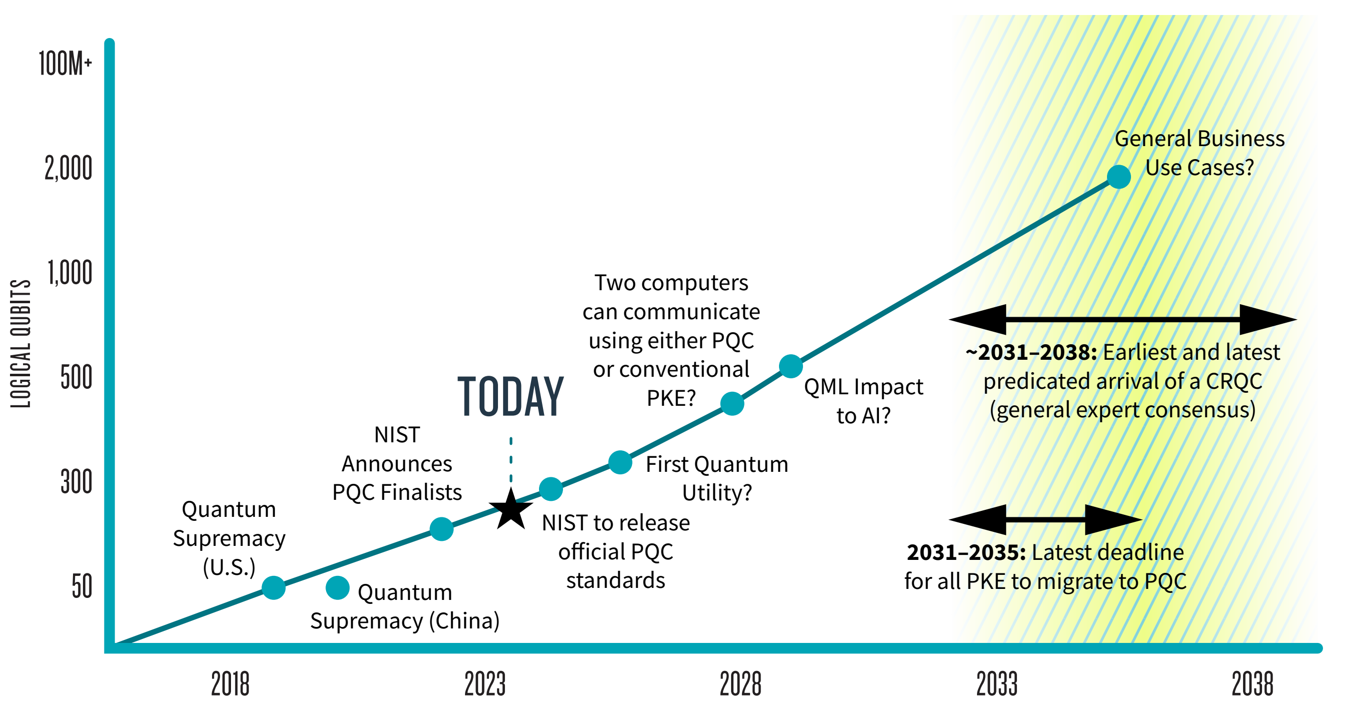


Figure 18: *The rapid progress in QC over the past several years (as measured by logical qubits, a convolution of physical qubits and error-correcting code) underscores the pressing need to secure data against future quantum cyberattacks.*

PQC Investment Trends

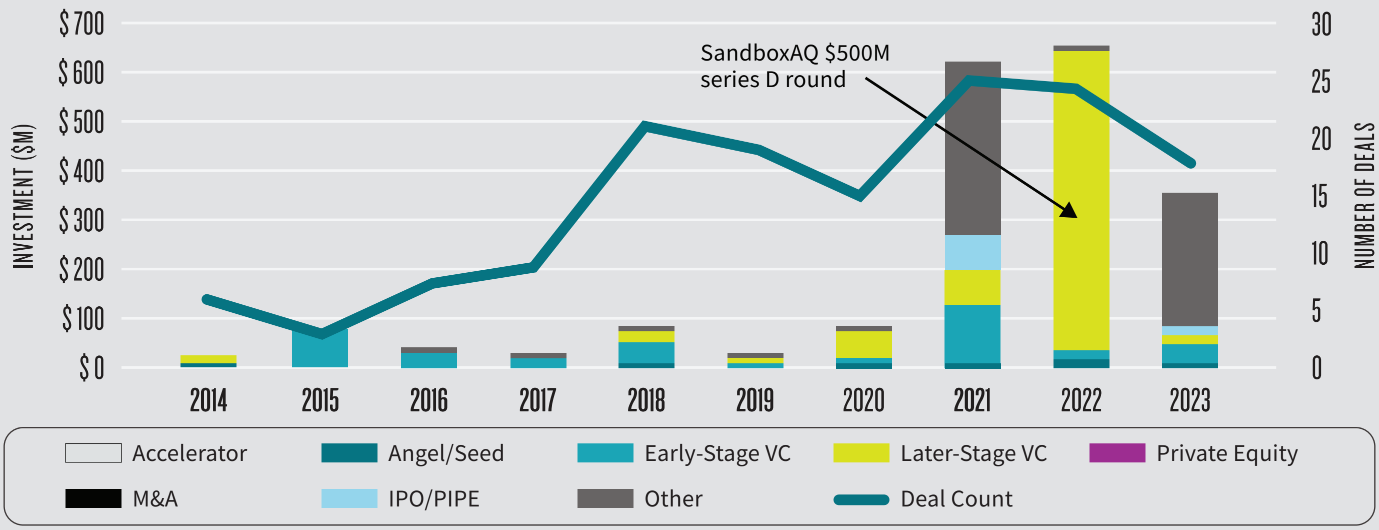


Figure 19: *Investment into PQC underwent a significant boom in 2021, underscored further by the enormous investment in Google spinout SandboxAQ in 2022. Today, the industry is poised for significant expansion: VCs and startups are likely waiting for NIST standards to be released, as USG, international governments, and most of commercial industry is mandated (or at least strongly incentivized) to adopt NIST's protocols. However, government-mandated solutions have the potential to stifle innovation where only particular solutions are allowed. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

by private insurance companies or military secrets—in anticipation of being able to decrypt it with a CRQC in the near future. This strategy, known as harvest now, decrypt later (HNDL), puts highly sensitive data (e.g., nuclear weapons information) in extreme danger of exposure, compromising our national security perhaps more than any other information-based threat.

To prepare for Y2Q and address the risks of HNDL, the National Security Memorandum 10 (NSM-10) requires an inventory of all federal IT systems as of May 2022, particularly those that are vulnerable to a CRQC. Later that year, President Biden signed the Quantum Computing Cybersecurity Preparedness Act, which orders an examination of all agencies' cryptography. The act exempts all national security systems, though transitioning these to PQC is already underway. While migration to PQC cannot take place in earnest until NIST standards are released later in 2024, USG and industry can and must begin to inventory their data, public key infrastructure, and applications today so they can be ready to transition as soon as possible. This is especially true of the U.S.'s most sensitive national security data, such as classified information held by the IC and DOD.

Future: In the best-case scenario, PQC standards will be quickly adopted by both USG and commercial industry, and NIST's algorithms will prove, over time, to be resistant to QC attacks—thus preventing any further risk from HNDL. However, no mathematical algorithm is provably quantum-secure, and the risk will always remain that a clever new approach can hack PQC protocols. Thus, it will be vital to establish a framework of crypto-agility during the current migration that will empower organizations and individuals to rapidly respond to any future threat. Improvements to hybrid cryptography methods—in which information is encrypted with multiple PQC algorithms so that a vulnerability in one will not compromise the integrity of the data—may also be used in the future to enhance data security. Ultimately, our ability to securely transmit data is essential to maintaining an information-based civilization, and ensuring the U.S. is prepared for the rapidly approaching post-quantum world is mission critical.

<< Back to Table of Contents

Emerging Innovators

Non-Exhaustive

The PQC VC landscape is becoming energized as the NIST protocols near finalization and uncertainty regarding requirements diminishes. As the cryptographic algorithms themselves will be highly standardized by NIST, the private sector is focused on innovating along parallel avenues. Several companies, such as SandboxAQ and Quantum Xchange, are concentrating on enabling crypto-agility while otherwise taking an algorithm-agnostic approach. American Binary has focused its attention on lattice-based PQC solutions for cloud infrastructure, networking, and in-field communications. Fully hardware-based solutions, such as Anametric's, represent a separate category altogether—one that offers post-quantum cryptographic acceleration (analogous to how AI chips accelerate AI algorithms) in low-SWaP form factors, ideal for edge systems.

AMERICAN BINARY

American Binary

HQ: Kirkland, WA

TOTAL RAISED: $3.25M

SERIES: Pre-Seed

USG TRACTION: Subcontracted with defense primes

American Binary delivers quantum-resistant cloud infrastructure solutions to critical defense and infrastructure verticals, helping them comply with upcoming cybersecurity standards and protecting them from current and future cyber threats. American Binary's products use lattice-based cryptography constructions that provide networking performance and applications for data at rest. Each component of the products complies with the upcoming CNSA 2.0 standards, from Kyber 1024 (ML-KEM) key encapsulation to the finest implementation details, without any elliptic-curve or hybrid encryption. They are working with undisclosed defense agencies and Fortune 30 companies to develop novel post-quantum in-field communications solutions for broad interagency applications.

ANAMETRIC

Anametric

HQ: Austin, TX

TOTAL RAISED: $2.7M

SERIES: Seed

USG TRACTION: AFRL, U.S. Army

Anametric is a startup developing quantum photonic solutions for cybersecurity. Working with teams at Southern Methodist University in Dallas and under contract with the U.S. Air Force and Army, they are designing and building chips at AIM Photonics. Combining patent-pending quantum and classical technologies, Anametric's devices will offer a wide range of improved cybersecurity functions, including a quantum random number generator, PQC key pair generation, and both classical and PQC signatures. Additional features include a novel hybrid quantum physically unclonable function (PUF), supporting improved resistance against ML-based attacks. Overall, Anametric's products will provide flexible and crypto-agile support for the upcoming transition to PQC.

Quantum Xchange

HQ: Bethesda, MD

TOTAL RAISED: $29.6M

SERIES: Early Stage

USG TRACTION: N/A

Quantum Xchange specializes in cryptographic auditing/risk assessment, crypto-agility, and crypto-diversification. One of their products, CipherInsights, provides real-time automated cryptographic risk, discovery, and continuous monitoring in preparation for the government-mandated migration to PQC. Another product, Phio TX, allows organizations to dynamically stack, switch, mix, and deliver quantum-safe keys across any network media type. Together, these enable diversified security defenses at multiple layers to remove as many failure points as possible. Quantum Xchange is a member of the NIST NCCoE Migration to Post-Quantum Cryptography Project Consortium, with FIPS 140-2/140-3 (pending) validation of Phio TX.

Sandbox AQ

HQ: Palo Alto, CA

TOTAL RAISED: $500M

SERIES: Later Stage

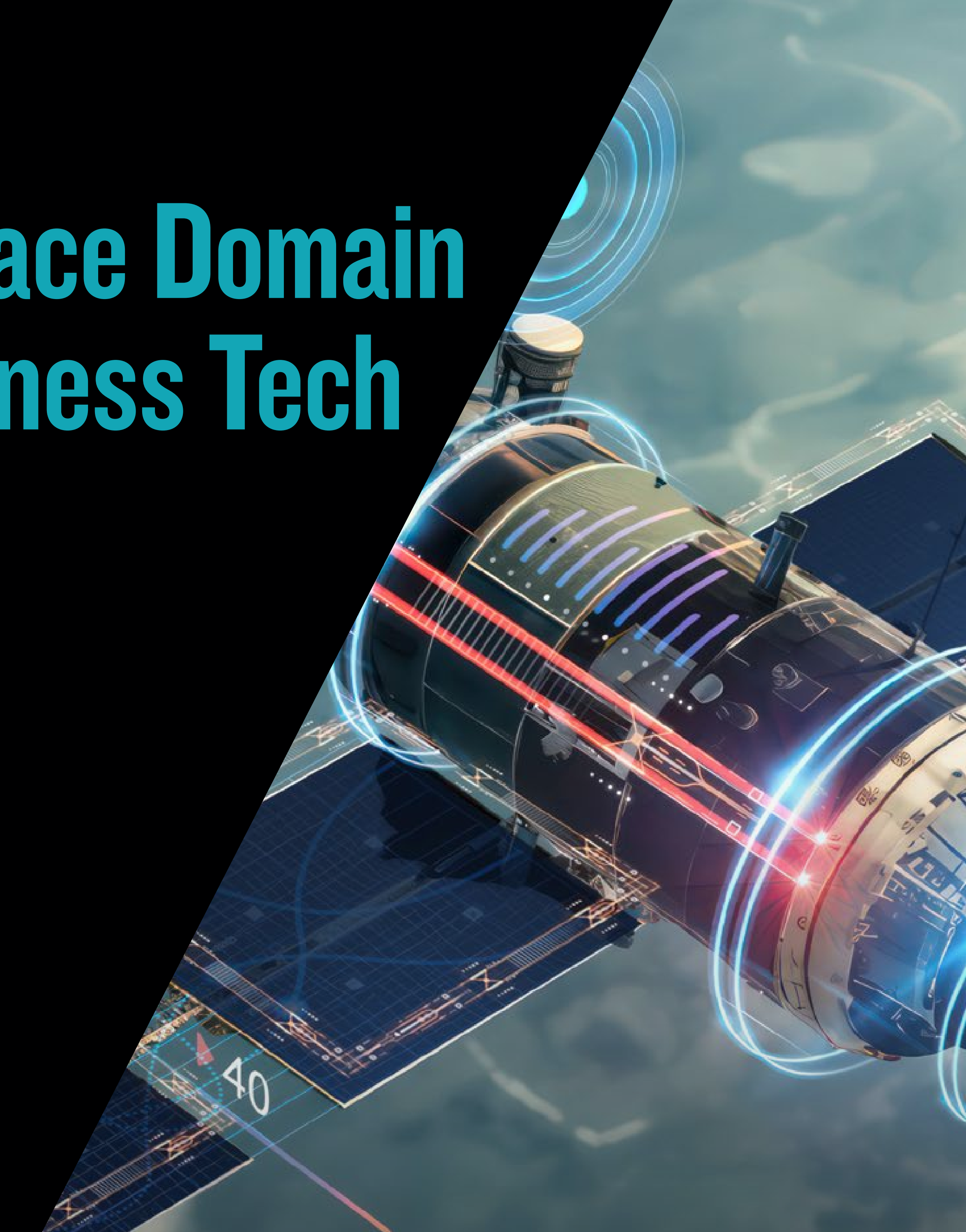
USG TRACTION: DISA, USAF, NCCoE member

The SandboxAQ Security Suite is an end-to-end crypto-agility platform that provides a full inventory of existing cryptography uses, including vulnerability and compliance analysis, as well as a path to centrally managed, robust, and agile cryptography. The result is protection from today's attacks as well as security against the future threat of a large-scale quantum computer. SandboxAQ was selected by NIST's National Cybersecurity Center of Excellence (NCCoE) for its Migration to Post-Quantum Cryptography Project, which partners with industry to help USG develop best practices to transition to PQC algorithms. The company also already works with a broad range of USG agencies and enterprise.

ESTABLISHED PLAYERS

As with many emerging tech areas, the Big Tech players are at the forefront of the PQC innovation space. Companies like AWS, Microsoft, and IBM are members of the NCCoE, a public-private partnership that is developing a framework to help industry with the PQC migration. These and other companies also have their own internal PQC strategies and development underway to protect their users and customers, as well as their internal systems, even before the NIST standards are released.

10. Space Domain Awareness Tech



> **The U.S. never wants to be in a fair fight. SDA will endow the U.S. military with an asymmetric advantage in the space domain and, therefore, has to be the top priority for the U.S. Space Force. And we need innovation from commercial partners to get it right.**
>
> **– Lt. Col. Dex Landreth**
> USSF, Secretary of Defense Executive Fellow

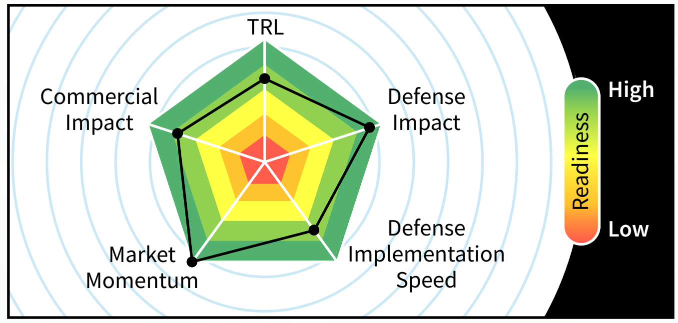
Executive Summary

Definition: Space domain awareness (SDA) enables an understanding of the space operating environment and perceived threats. It also allows commercial operators to safely fly their spacecraft, avoid debris, and maintain the orbital regimes they use.

Technology: The SDA mission is accomplished through a large technology stack, including a variety of sensor modalities, compute resources, AI/ML and analytics, visualization technologies, and the applications and services created on top of these. The sensor modalities can be both ground and space based.

Strategic Insight: Space is now a warfighting domain, a recent and dramatic shift over the past decade. Given that, the U.S. and allied partners need to accurately understand the threats to their assets and capabilities so they can prevent conflict and maintain environmental superiority.

Future: Expected innovations include the ability to accurately acquire, track, and distribute objects beyond geostationary Earth orbit (xGEO); proliferation of space-based commercial sensors; adoption of AR/VR for SDA missions; and space-based sensors operating in xGEO.



ISR for Space

DOD's space capabilities enable most platforms on Earth. Navigation, communication, intelligence, and threat warning systems are all space based, and without them, the U.S. military would be unable to effectively engage in conflict. Given this fact, space is now a warfighting domain. To inform and enable ground forces, assets in space must be protected via SDA missions and technologies. SDA is similar in scope to space situational awareness (SSA) and space traffic management (STM), though it is more sophisticated and defensive in nature. All three play a role in a spectrum of technical and mission complexity, with SDA focused on detecting, tracking, propagating orbits, and providing conjunction (i.e., collision) avoidance, as well as cataloging, characterizing, and understanding the orbital environment. This includes identifying objects, threats, and anomalous patterns-of-life and characterizing their capabilities, intentions, and ownership. In an offensive situation, SDA equates to comprehensive space battlespace awareness.

USE CASES

- Non-Earth Imaging
- Conjuction Avoidance
- Orbit Propagation
- Inspection
- Spectrum Resiliency

<< Back to Table of Contents

Technology: The SDA technology stack includes a variety of sensor modalities, compute resources, AI/ML and analytics, visualization technologies, and the applications and services built on top of these. The sensor modalities can be ground or space based, which, when combined, provide the most complete understanding of the space environment. Ground-based SSA and SDA sensors include radars, optical telescopes, and passive RF. Space-based sensors are typically optical, infrared, or RF and are sometimes deployed on maneuverable platforms to increase the fidelity of the collected data. Technology development is focused on creating a more complete picture of the sky and making sense of it more rapidly. Therefore, future sensor improvements to both ground- and space-based assets will allow for the tracking of smaller and increasingly maneuverable resident space objects (RSOs). In addition, this will mean the proliferation of sensor assets to reduce current gaps in coverage. According to U.S. Space Force's (USSF's) Gen. Chance Saltzman, Chief of Space Operations, there are challenges in data processing times and the ability to turn raw data into useful information. Improvements in automation and AI across the SDA architecture will streamline DOD's tracking and interpretation capabilities.

Strategic Insight: The current space environment has about 9,500 active satellites and is littered with over 100 million pieces of mostly untracked debris. This swelling number will require increasing amounts of conjunction avoidance maneuvers; the SpaceX Starlink constellation alone is on pace to hit 1 million such movements by 2028. Satellite maneuvers can make it difficult to provide accurate situational awareness; this will increase the likelihood of conjunctions unless there are advances in technology and regulation. In addition, because they consider U.S. space dependency an exploitable vulnerability, both Russia and China have made offensive counterspace a key component of their future warfighting focus. Having a complete picture of the operating environment, including the RF spectrum and

Objects in the Space Force Satellite Catalog: Calendar Years 2012—2022

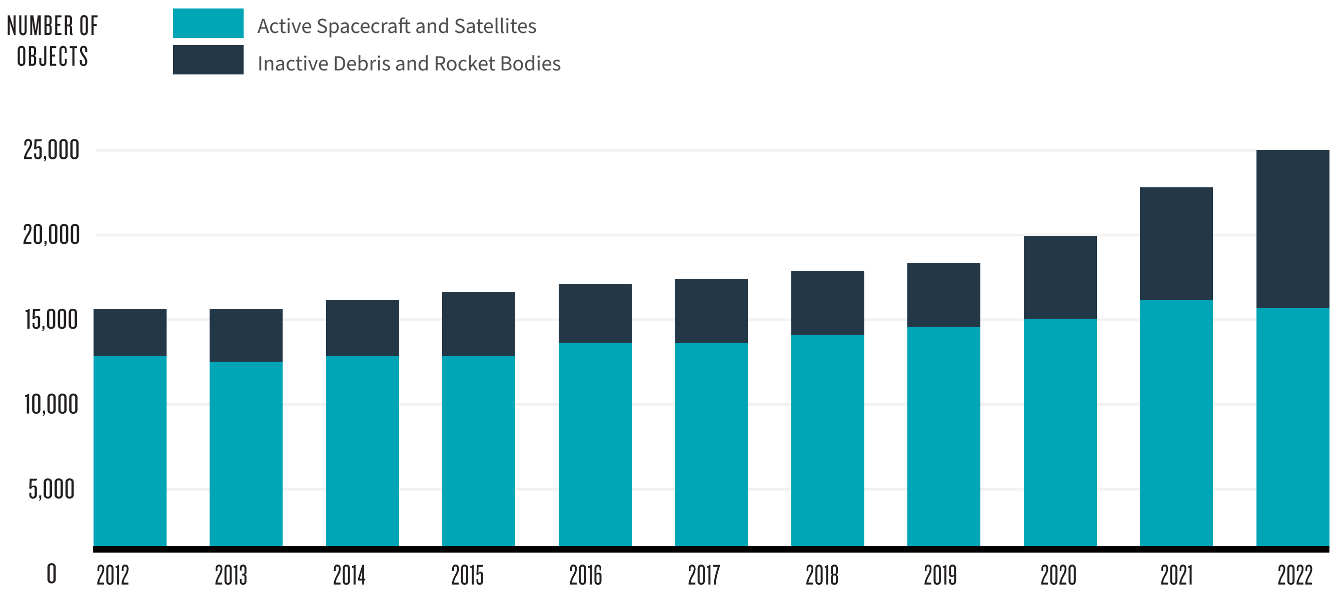


Figure 20: *Objects in the USSF Satellite Catalog, representing less than 0.1% of objects in space bigger than 1 mm. Even objects as small as 1 mm can damage active satellites. Image source: GAO-23-105565.*

SDA Investment Trends

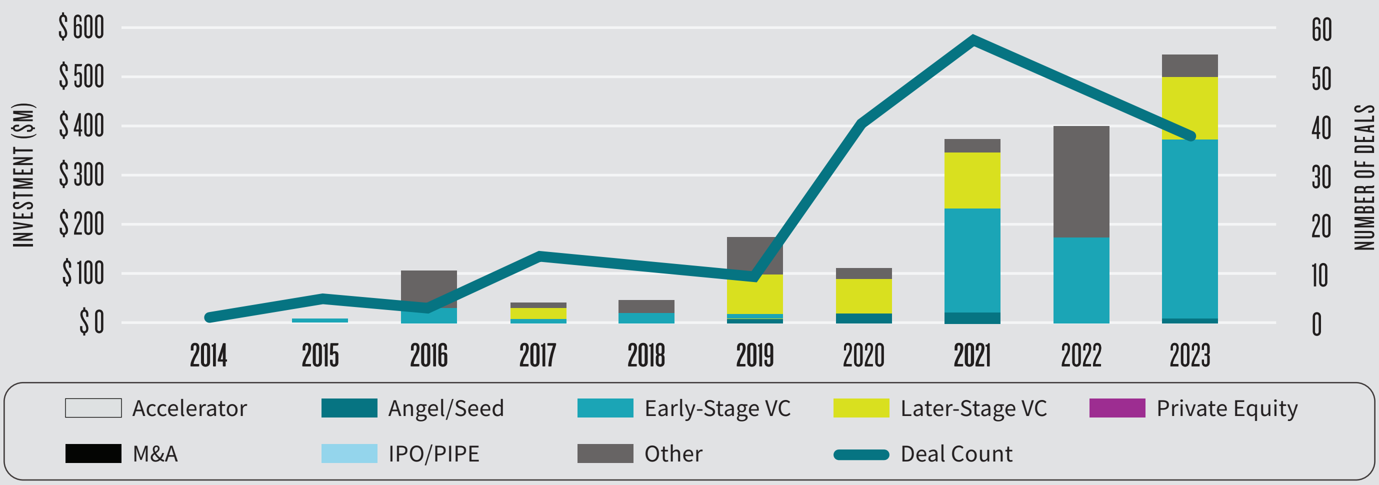


Figure 21: *Overall funding for SDA has seen a steady increase in recent years. The spike in 2021 is attributable to large deals inked by Astroscale and LeoLabs. The early-stage funding jump in 2021 stabilized in 2022, with companies such as Albedo, True Anomaly, Slingshot Aerospace, Quantum Space, and Atomos all raising healthy Series A rounds. The 2023 macro space market dip was bolstered by True Anomaly raising $100 million in Series B funding. Source: PitchBook Data, Inc.; *Data has not been reviewed by PitchBook analysts.*

cyber domain, will allow operators to act upon perceived threats and continue to provide critical services to the warfighter from space. Recognizing the urgency to secure space assets, in FY24 the USSF requested $612 million (a $120 million increase from FY22) for space tracking programs, ground-based radar, optical telescopes, space-based surveillance capabilities in geostationary Earth orbit (GEO) and beyond geostationary Earth orbit (xGEO), commercial data buys, and compute and analytics. Given the high priority of the mission, this cost is small compared to other USSF priorities. Commercial capabilities could be used to augment USG's budget and address technological pain points, as evidenced by efforts to create a commercial services budget line by 2025 and the recent unveiling of the SDA Tools, Applications, and Processing (TAP) Lab.

Future: Innovative SDA offerings will help eliminate the gaps in sensor coverage, reduce the lag times to derive insights, and advance our understanding of the xGEO operational environment. Ideally, space-faring nations will have an international arbiter capable of regulating and directing space traffic automatically in a cloud-based system. Also, due to increasing space congestion, platforms may be required to have autonomous conjunction avoidance capabilities. In the future, gaps in orbital coverage from ground assets will be filled by commercial capabilities. Given the loosening of regulatory restrictions on non-Earth imaging (NEI), many of these ground assets will autonomously tip and cue, a process of complementary sensors working with other commercial NEI platforms to inspect anomalous pattern-of-life detections with greater fidelity. Defense customers will use these partnerships to acquire unclassified insights and speed decisions, aiming to have complete SDA coverage by 2026. By then, USSF satellite operators should have the ability to fuse commercial and government SSA data seamlessly on upgraded computer systems. Finally, according to USSF, new sensors of all types, particularly space-based, will be required to develop and maintain SDA beyond GEO. Thus, to ensure U.S. safety and stability in space, prototype missions to xGEO and dedicated sensor developments will come online to study complex orbital mechanics and further our military's space-based SDA capabilities.

Emerging Innovators

Non-Exhaustive

Companies such as LeoLabs are building radars and optical telescopes to decrease current coverage gaps. Due to decreased regulations concerning NEI, several startups—such as HEO and Albedo—are building capabilities to capture images of other RSOs to sell commercially or to government customers. As space becomes more crowded, conjunction threats will become more prevalent, lending opportunities to unique capabilities such as Kayhan Space's space traffic coordination and safety solutions.

Meanwhile, others, such as True Anomaly, are building maneuverable platforms that can inspect other spacecraft at close distances. Commercial SDA outlook is uncertain, though, due to unanswered regulatory questions, defense prime contractor dominance, and the government's free public service. Startups that thrive will be those whose SDA business is secondary or uniquely valuable. Even so, the market will likely support only a few commercial startups long term.

Albedo

HQ: Denver, CO

TOTAL RAISED: $125M

SERIES: Early Stage

USG TRACTION: USAF

Albedo is building VLEO satellites to capture the highest resolution commercial imagery for government and commercial markets, with 10 cm/pixel visible co-collected and 2 m/pixel thermal infrared. Albedo enables on-demand, ultra-high-quality data to support DOD and IC strategic and tactical missions. Albedo's agile platform allows it to perform thermal NEI for monitoring space objects and safeguarding national assets in space.
**Invested in by Booz Allen Ventures*

HEO

HQ: Washington, DC (alternate)

TOTAL RAISED: $8M

SERIES: Early Stage

USG TRACTION: Classified Customer

HEO is a satellite-to-satellite imagery and intelligence provider that enables assessment of the status, operation, and anomalous behavior of targets in orbit so that decision makers can confidently act in space and on Earth. HEO modifies concept of operations (ConOps) of partner Earth observation satellites through proprietary software and launches its own NEI sensors as hosted payloads on a range of partner platforms. The goal of this hybrid approach is to achieve proliferation of NEI sensors on all orbits in the Earth-Moon system.

Kayhan Space

HQ: Boulder, CO

TOTAL RAISED: $11.2M

SERIES: Early Stage

USG TRACTION: NASA, USAF

Kayhan Space provides solutions in spaceflight safety, SSA, and SDA. The company's capabilities and integrated orbital dynamics library can be adapted to provide solutions for wide-ranging problems in space, further enabling spaceflight safety and complex operations. Kayhan's premier offering, the Pathfinder 3.0 Space Situational Awareness Suite, delivers autonomous collision avoidance, conjunction notification and assessment, and space traffic coordination solutions.

LeoLabs

HQ: Menlo Park, CA

TOTAL RAISED: $127M

SERIES: Early Stage

USG TRACTION: USSF, NOAA

LeoLabs, Inc. provides SSA services to private sector and U.S. federal government aerospace, defense, and environmental markets. The company's radar technology can detect and track small satellites and general debris in low-Earth orbit and propagate future orbits. LeoLabs' core technology includes a global phased-array radar network. This provides a sovereign data feed that serves an independently developed analytics platform. The LeoLabs SSA software platform provides timely analytics and accurate orbital and situational data. The company operates a 10-radar network that works around the clock—unaffected by sunlight, rain, or clouds.

True Anomaly

HQ: Centennial, CO

TOTAL RAISED: $125M

SERIES: Early Stage

USG TRACTION: USSF

True Anomaly is a technology company building innovative solutions at the intersection of spacecraft, software, and AI. It addresses space domain awareness and readiness challenges. This includes a combination of dynamic software applications as well as on-orbit rendezvous and proximity operations and NEI. The company's products and services also incorporate solutions for space operator training, capabilities testing, and rapid response missions.

ESTABLISHED PLAYERS

Today, the SDA market is dominated by major prime OEMs—Northrop Grumman, L3Harris, and Lockheed Martin. These companies have won major contracts, such as DARC, GSSAP, MOSSAIC, ATLAS, and Space Fence. Another notable Big Tech player is Amazon, which provides the compute for several SDA startups and has built ARGUS, an open architecture marketplace for SDA. Major prime venture funds are not very active in the space; however, Lockheed Martin Ventures has made a few startup investments. Look for defense primes to continue to win major programs of record.

<< Back to Table of Contents

Conclusion & Appendix

What's Next?

We believe the 10 technologies highlighted in this report have the potential to change the manner in which the U.S. protects its strategic interests and ensures national security for its citizens. The identification of ecosystems primed for investment is an important challenge ripe with complexities, yet it is only the beginning of the journey.

To fully harness the potential of the technologies listed in this report, we recommend:

- **Concentrating funding in these ecosystems (and others deemed essential by OUSD[R&E]).** Other key actions include picking winners who are willing and able to customize their dual-use product to defense needs and increasing award sizes to entice additional investments from investors and defense prime contractors.
- **Reimagining requirements and ConOps to harness the full potential of the technologies.** The U.S. will need to divest from legacy technology and programs that no longer provide strategic value to make room for new initiatives.
- **Creating white space for the unknown so that defense leaders across the board can experiment, iterate, and innovate as fast as humanly possible.** The technology which provides strategic advantage in one to three years will not be the same technology that wins wars in 10 to 15 years.
- **Building a foundation of radical accountability and responsibility in the midst of technology adoption**. Technology is a tool that has the promise to save lives, preserve peace, and promote economic prosperity—but only when used in the light, with an unbroken focus and emphasis on ethics, well-being, and the mitigation of unintended consequences.

We owe a huge amount of gratitude to all the people who helped put this report together, many of them included under List of Authors on page 79. If you wish to discuss something in the report, please reach out—we aggregated information as best we could from our own analysis, open-source and subscription-based tools, and the opinions of thought leaders, private industry, academia, government, and the VC community. We stand behind our analyses with conviction but humbly acknowledge that if we think we got everything right, we are doing something wrong.

Our team compiled this report because we believe emerging technology plays a key role in protecting our country, our warfighters, and our citizens within. **The U.S.'s greatest asset is its people—and with their ingenuity, creativity, and the help of the best technology in the world, we ensure a better and safer future for all.**

Want to learn more? Check out the Tech Scouting website.

Reach out to us at techscouting@bah.com.

Further Reading

Additional Studies on Defense Innovation

Atlantic Council: Commission on Defense Innovation Adoption

Center for New American Security (CNAS): DIU 3.0: Scaling Defense Innovation for Strategic Impact

Department of Defense Under Secretary of Defense for Research and Engineering (USD[R&E]): Critical Technology Areas

Defense Information Systems Agency (DISA): FY2022–2024 Strategic Plan

DefenseScoop: DISA's Updated Tech Watchlist Gets Specific on AI Capabilities

RAND Corporation: Strengthening the Defense Innovation Ecosystem

Special Competitive Studies Project: Funding for the Future: The Case for Federal R&D Spending

The Wall Street Journal: Investors Are Betting on Defense Startups. The Pentagon Isn't.

Stanford Emerging Technology Review

List of Authors

- Brian MacCarthy
- Kerry Chin
- Natasha Efrat-Sivan
- Elyse Jayson
- Kristina Brown
- Brandon Dube
- Paul Goebel
- Meghan Hauser
- Ryan Nelson
- Taylor Rhoten
- Connor Swain
- Griffin Arkilic
- Livia Dworaczyk
- Nicholas Free
- Natalie Kiernan
- Jake Mervis
- Lindsay Patterson
- Lukas Sznewajs
- Cara Valencia
- Andrew Walston

 |

Emerging Innovators

AI Accelerator Chips

celestial AI, SiMa.ai, EnCharge AI, EXTROPIC, groq

Alternative PNT

PSIONIC, TRUSTPOINT, Infleqtion, xona space systems

Autonomous Swarms

VATN Systems, SARONIC, DARKHIVE, Swarmbotics AI, FIRESTORM

Gen-AI Software Development

replit, Sourcegraph, Hugging Face, mabl, mutable.ai

High-Density Energy Storage

anthro, ADVANO, NANOTECH, PROMETHEUS Hydrogen

Hypersonics

VELONTRA, HERMEUS, CASTELION, SPECTER AEROSPACE, VENUS AEROSPACE

Multimodal AI

Primordial Labs, Reality Defender, PRYON, Twelve Labs

Non-Kinetic Counter-UAS

EPIRUS, D-FEND SOLUTIONS, Hidden Level, HIGH POINT AEROTECHNOLOGIES

Post-Quantum Cryptography

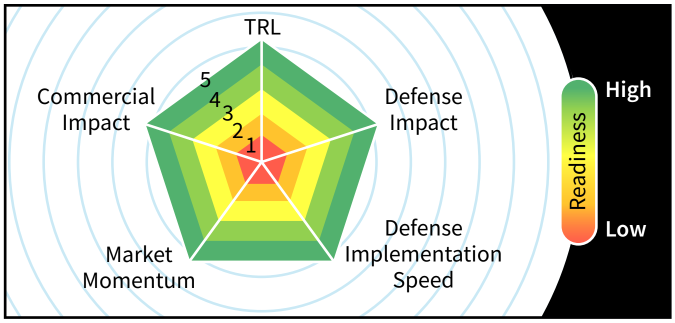
SANDBOXAQ, ANAMETRIC, AMERICAN BINARY, QUANTUMXCHANGE

Space Domain Awareness Tech

LEOLABS, ALBEDO, True Anomaly, kayhan. space, HEO

Radar Chart

Radar chart surveys were distributed to Booz Allen leaders and responses were averaged to provide a snapshot look at the technologies in this report. Responses provide a baseline view of current thinking, although rankings are situationally driven and subject to change.



TRL: How would you rank the technical maturity of this technology?

1 = Very immature, roughly TRL 1

2 = Immature, roughly TRL 2–3

3 = Intermediate maturity, roughly TRL 4–5

4 = Somewhat mature, roughly TRL 6–7

5 = Very mature, roughly TRL 8–9

Technology readiness levels (TRLs) are a method for estimating the maturity of technologies. The TRL scale was originally developed by NASA in the 1970s and is used widely across USG today.

Defense Impact: How would you rank the impact of this technology to the defense sector?

1 = Will not significantly impact national security

2 = Will not significantly impact most aspects of national security but will have moderate impact across a few key aspects

3 = Will have moderate impact across many aspects of national security or will have significant impact across a few key aspects

4 = Will have significant impact across many aspects of national security or will fundamentally transform/impact a few key aspects

5 = Will fundamentally transform/revolutionize or impact virtually every aspect of national security

Defense Implementation Speed: How quickly do you think the U.S. DOD and defense-related groups can widely implement this technology? For example, barriers to implementation would include not just tech maturity but also interoperability with existing U.S. DOD systems, ATO processes, data training barriers, etc.

1 = 10+ years

2 = 8–10 years

3 = 5–7 years

4 = 2–5 years

5 = <2 years

Commercial Impact: How would you rank the impact of this technology on commercial industry?

1 = Will not significantly impact commercial industry

2 = Will not significantly impact most industries but will have moderate impact across a few key industries

3 = Will have moderate impact across many industries or will have significant impact across a few key industries

4 = Will have significant impact across many industries or will fundamentally transform/impact a few key industries

5 = Will fundamentally transform/revolutionize or impact virtually every major commercial industry

Market Momentum (not in survey): Based on the five-year investment CAGR for the PitchBook list between 2018 and 2023

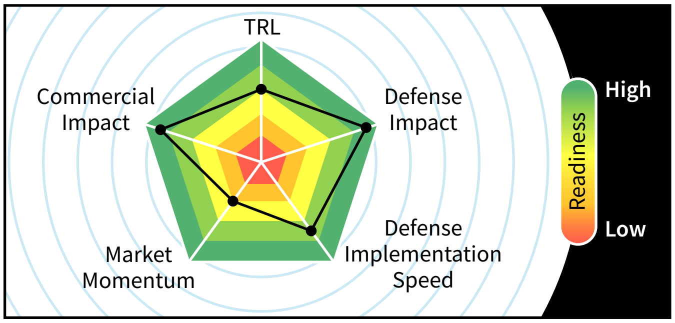
1 = <10%

2 = 10%–20%

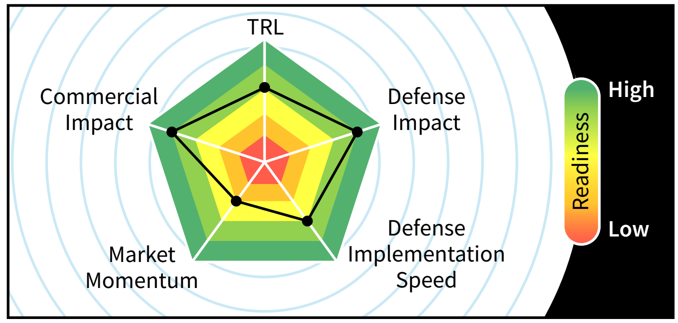
3 = 20%–30%

4 = 30%–50%

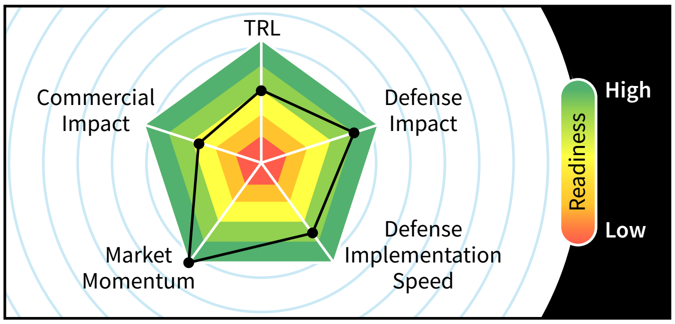
5 = >50%



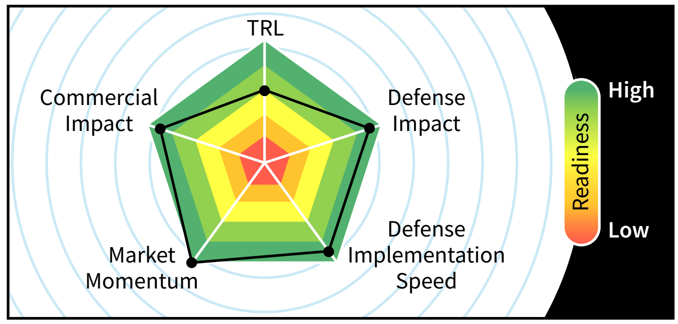
AI Accelerator Chips



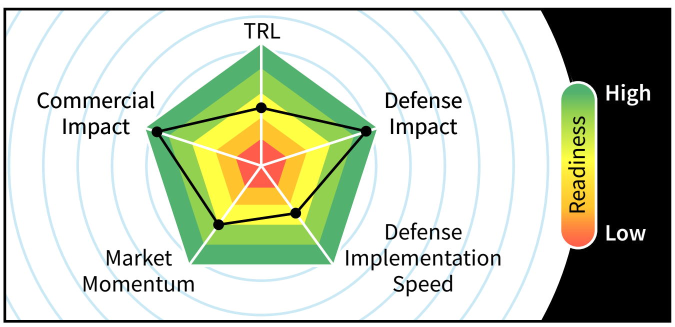
Alternative Position, Navigation, and Timing



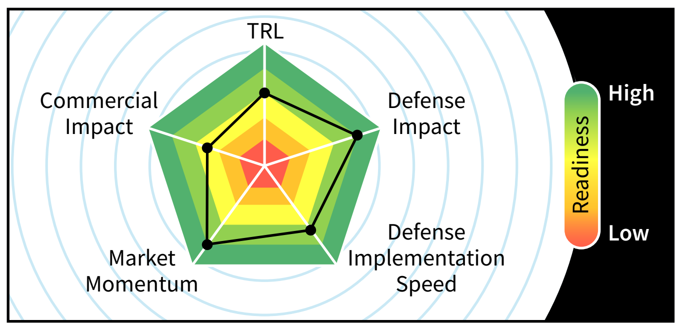
Autonomous Swarms



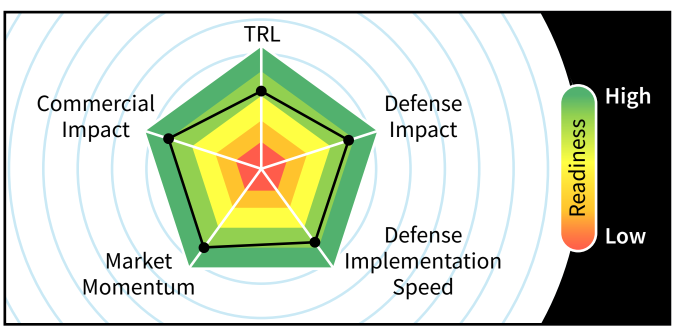
Generative AI Software Development



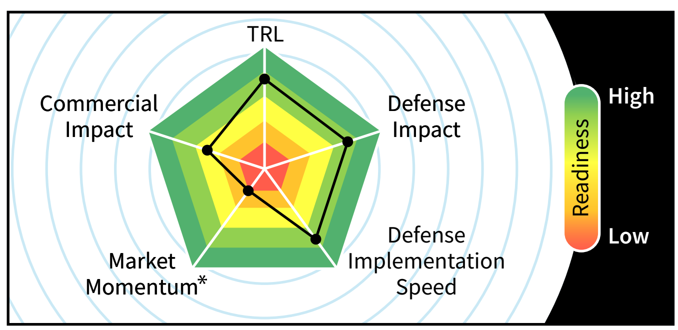
High-Density Energy Storage



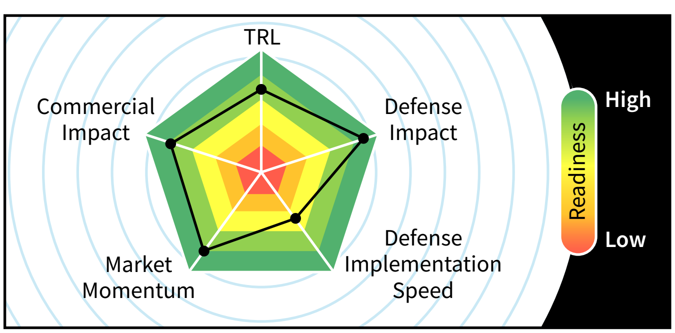
Hypersonics



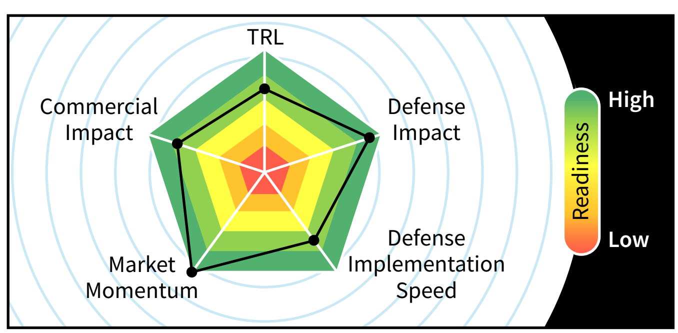
Multimodal AI



Non-Kinetic Counter-UAS



Post-Quantum Cryptography



Space Domain Awareness Tech

<< Back to Table of Contents

Glossary

Glossary of General Defense-Relevant Terms

Generative AI used to derive definitions

AFWERX: An innovation arm of the USAF fostering collaboration with the civilian sector.

Air Force Research Lab (AFRL): The USAF's R&D organization.

Artificial Intelligence/Machine Learning (AI/ML): ML is a subset of AI that uses algorithms to analyze large amounts of data, learn from insights, and make informed decisions.

Attritable Systems: A design trait that trades reliability and maintenance for low-cost, reusable, and eventually expendable weapons.

Augmented Reality/Virtual Reality (AR/VR): Technologies that enhance or create a virtual experience.

Chinese Communist Party (CCP): The founding and sole ruling party of the People's Republic of China.

Computer Vision (CV): A subset of AI/ML that enables computers to interpret and make decisions based on visual data.

Critical Infrastructure: Systems and assets vital for a country's functioning, such as electrical grids, oil and gas pipelines, rail systems, and communication systems.

Defense Advanced Research Projects Agency (DARPA): An R&D agency of DOD responsible for the development of emerging technologies for use by the military, established in 1958 in response to the Soviet Union's launching of Sputnik.

Defense Logistics Agency (DLA): An agency within DOD that provides the U.S. armed forces, other federal agencies, and partner nation armed forces with a full spectrum of logistics, acquisition, and technical services.

Department of Energy (DOE): A U.S. department advancing energy and nuclear security.

Edge Computing: A distributed computing paradigm that brings computation and data storage closer to the sources of data and/or operations.

Fiscal Year (FY): A 12-month accounting period for budgeting and financial reporting.

Force Multiplication: The use of systems and tools to increase the level of force or control that personnel exert on the battlefield.

Indo-Pacific: A region consisting of the Indian Ocean and the western and central Pacific Ocean.

Information Technology (IT): A set of related fields that encompass computer systems, software, programming languages, and data and information processing and storage.

Intelligence Community (IC): A group of distinct USG intelligence agencies and subordinate organizations that work both separately and collectively to conduct intelligence activities that support the foreign policy and national security interests of the country.

Intelligence, Surveillance, and Reconnaissance (ISR): The coordinated acquisition, processing, and dissemination of accurate, relevant, and timely information and intelligence to support a commander's decision-making process.

National Aeronautics and Space Administration (NASA): An independent agency of the U.S. federal government responsible for the civil space program, aeronautics research, and space research.

National Institute of Standards and Technology (NIST): An agency of the U.S. Department of Commerce whose mission is to promote American innovation and industrial competitiveness. It is also charged with providing many standards and metrics in support of DOD and all of USG.

Natural Language Processing (NLP): A subset of AI/ML that gives computers the ability to interpret and manipulate human language.

Naval Research Lab (NRL): The corporate research laboratory for the U.S. Navy.

North Atlantic Treaty Organization (NATO): An intergovernmental military alliance established in the aftermath of World War II between 31 member states—29 European and two North American; NATO is a collective security system in which its independent member states agree to defend each other against attacks by third parties.

Office of Naval Research (ONR): An organization within the U.S. Department of the Navy that coordinates, executes, and promotes the science and technology programs of the U.S. Navy and Marine Corps.

Office of the Secretary of Defense (OSD): The principal civilian leadership in the U.S. Department of Defense.

People's Liberation Army (PLA): The armed wing of the CCP and the principal military force of the People's Republic of China.

People's Republic of China (PRC): The official name of the country of China, as established by Mao Zedong in 1949.

Prime Original Equipment Manufacturers (OEMs)/Defense Prime: A major company in the defense industry that manages and oversees significant defense projects, serving as the primary contractor for government defense agencies and coordinating various aspects of project execution.

Radio Frequency (RF): A range of the electromagnetic spectrum from around 20 kHz to around 300 GHz used for a variety of communications, including wireless military communications.

Research and Development (R&D): The process of creating new technologies or improving existing ones.

Size, Weight, and Power (and Cost) (SWaP[-C]): Parameters used to evaluate the efficiency of military systems.

Small Business Innovation Research (SBIR): A program administered by the Small Business Administration (SBA) in which U.S. service branches award grants to encourage domestic small businesses to engage in federal R&D with the potential for commercialization as well as eventual procurement by the U.S. military.

State-of-the-Art (SOTA): The highest level of development, as of a device, technique, or scientific field. Usually refers to fielded rather than experimental systems.

Technology Readiness Level (TRL): A measure to assess the maturity of a technology during the R&D process.

U.S. Air Force (USAF): The aerial warfare service branch of the U.S. armed forces.

U.S. Department of Defense (DOD): A department of the U.S. federal government charged with coordinating and supervising all agencies and functions of USG directly related to national security and the U.S. armed forces.

U.S. Government (USG): The federal government of the U.S.

U.S. Government Accountability Office (GAO): An agency providing auditing, evaluation, and investigative services for Congress.

U.S. Missile Defense Agency (MDA): A U.S. agency developing missile defense systems.

U.S. Space Force (USSF): A military branch responsible for organizing, training, and equipping space forces.

Unmanned Aerial Systems (UASs)/Unmanned Aerial Vehicles (UAVs): Aircraft without a human pilot onboard, controlled remotely or autonomously.

Glossary of General Business/ Venture-Relevant Terms

Generative AI used to derive definitions

Accelerator/Incubator: A deal in which a company joins a temporary program that variably provides funding, office space, technological development, and/or mentorship, often in exchange for equity in the company.

Angel Investment: A deal in which a high-net-worth individual provides capital to a company in its early stage in exchange for a minority stake. The investment must come directly from the individual's own funds and not from any other source.

Business-to-Business (B2B): A business model characterized by commercial transactions between businesses.

Business-to-Consumer (B2C): A business model characterized by commercial transactions between businesses and consumers.

Business-to-Government (B2G): A business model characterized by commercial transactions between businesses and government entities.

Capital Expenditure (CapEx): The money an organization or corporate entity spends to acquire, maintain, or improve its fixed assets, such as buildings, vehicles, equipment, or land.

Early-Stage VC: A startup that has completed at least a Series A, B, 1, 2, or 3 (but no higher) venture capital financing round.

Grant: When a company receives financing that will not give the provider an economic interest or right in the assets or future cash flows of the company. Does not necessarily include all grants from USG.

Initial Public Offering (IPO): An investment open for the public or retail investors after a company has complied with the registration requirements of new securities laid down by the U.S. Securities and Exchange Commission.

Later-Stage VC: A startup that has completed a Series C, Stage 4, or higher venture capital financing round and has not undergone an M&A, IPO, or private equity financing.

Mergers and Acquisitions (M&A): When a corporation acquires at least a controlling percentage of a company's capital stock in another corporation. This deal type is often called a strategic investment.

Operating Expenditure (OpEx): The money a company or organization spends on an ongoing, day-to-day basis to run its business, such as electricity costs or employee wages.

Private Equity Investment: When a corporation receives equity financing from outside institutional investors, including private equity firms, asset managers, and select limited partners. The following deal types (as defined by PitchBook), are considered within this umbrella: growth/expansion and buyout/leveraged buyout.

Private Investment in Public Equity (PIPE): The action of buying shares of publicly traded stock at a price below the current market value per share.

Seed Investment: When any investor type provides the initial financing for a new enterprise that is in the earliest stages of development. PitchBook will only designate an equity raise as seed financing when it's explicitly referenced as a seed deal in sources or when undisclosed investors invest in a company under a set of predetermined circumstances.

Glossary of Technology Topic-Specific Terms

Generative AI used to derive definitions

Absolute PNT: A PNT system that uses external signals to navigate, such as satellite signals, RF signals, magnetic or gravity fields, or visual input.

AI Accelerator Chips (AI Chips): Specialized microelectronic hardware devices that speed up the processing of AI/ML software models.

All-Source Intelligence: Intelligence organizations, analysts, or products that are based on all available sources of intelligence collection information, namely open-source intelligence (OSINT).

Alternative Position, Navigation, and Timing (Alt-PNT): Also known variously as A-PNT, assured PNT, and complementary PNT/C-PNT), alt-PNT is the umbrella term describing any PNT technology other than Global Positioning System (GPS)/Global Navigation Satellite Systems (GNSS)/medium Earth orbit (MEO)-based satellites, which are most susceptible to jamming and spoofing attempts.

Android Team Awareness Kit (ATAK): A suite of software, originally developed by AFRL, that provides geospatial information and allows user collaboration over geography.

Anode: The electrode through which conventional current enters a polarized electrical device (i.e., the electrode where oxidation occurs).

Anomalous Pattern-of-Life Detection: Identification of irregular or unexpected behavior in the activities or movements of objects in space, potentially indicating unusual or suspicious events.

Anti-Access/Area Denial (A2/AD): Military strategies preventing adversaries from entering or operating in certain areas.

Application-Specific Integrated Circuits (ASICs): Custom-designed integrated circuits for specific applications.

Artificial General Intelligence (AGI): AI systems with humanlike or greater cognitive abilities.

Atomic Clock: A clock with an electrical oscillator regulated by the natural vibration frequencies of an atomic system, such as a beam of cesium atoms probed with microwaves.

Autonomy: The ability of a system to operate without human intervention.

Battery: A device that stores and converts chemical energy into electrical energy through electrochemical reactions. Batteries typically consist of one or more cells and are commonly used to power electronic devices, vehicles, and various applications.

Beyond Geostationary Earth Orbit (xGEO): Describes objects or activities that occur beyond the orbit of geostationary satellites, typically in regions like medium Earth orbit (MEO) or beyond.

Cathode: The electrode from which a conventional current leaves a polarized electrical device (i.e., the electrode where reduction occurs).

Central Processing Unit (CPU): The main processor in a computer that executes instructions of a computer program, such as arithmetic, logic, controlling, and input/output (I/O) operations.

Chief Digital and Artificial Intelligence Office (CDAO): Executive responsible for digital and AI strategy for DOD.

Code Debugging: The process of identifying and fixing errors in computer code.

Code Snippet: A small piece of reusable code.

Codebases: Collections of source code used to run a software system.

Command and Control (C2): The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. At its most fundamental level, C2 represents how DOD makes operational decisions.

Commercial off-the-Shelf (COTS): Packaged or ready-made hardware or software, adapted aftermarket to the needs of the purchasing organization, rather than the commissioning of custom-made solutions.

Conjunction: In space operations, a conjunction refers to the close approach of two space objects, raising concerns about the potential for collisions and prompting collision avoidance maneuvers.

Consensus Protocols: Algorithms ensuring agreement among distributed systems.

Counter-Swarming: Systems designed to engage and eliminate swarms.

Counter-UAS (c-UAS): Systems designed to detect and neutralize unmanned aircraft.

Crypto-agility: The ability of an IT system to quickly adapt and update its public-key encryption (PKE) protocols in response to emerging threats or advancements in technology. It refers only to the adaptability of the system rather than to any specific algorithms it employs.

Cryptographically Relevant Quantum Computer (CRQC): A quantum computer with sufficient processing power to break widely used cryptographic algorithms, posing a threat to conventional encryption methods.

DARPA Autonomous Multi-Domain Adaptive Swarms-of-Swarms (AMASS): A 2023 program to develop the ability to unleash thousands of autonomous land, sea, and air drones capable of overwhelming and dominating an enemy's area defenses.

DARPA OFFensive Swarm-Enabled Tactics (OFFSET): A DARPA program aiming to develop future small-unit infantry forces using swarms of more than 250 small UASs and/or small unmanned ground systems to accomplish diverse missions in complex urban environments.

Deepfake: A manipulated digital representation, often using AI, to create misleading content.

Directed Energy Weapons: Weapons using focused energy, such as lasers or microwaves.

Electronic Warfare (EW): Military action involving the use of electromagnetic energy to control the electromagnetic spectrum.

Electronics Resurgence Initiative (ERI): A five-year, $1.5 billion initiative by DARPA to ensure U.S. leadership in next-generation microelectronics R&D and manufacturing. DARPA expanded ERI's focus with the announcement of ERI 2.0, which seeks to reinvent domestic microelectronics manufacturing.

Elliptic Curve Discrete Logarithms: The mathematical process of finding the exponent in the elliptic curve equation, a task that, for very large numbers, is believed to be impossible for classical computers in a reasonable timeframe but would be achievable by a CRQC.

Error Correcting Code: Algorithms used to identify and fix errors in quantum computers, aggregating physical qubits into logical qubits.

Factoring: The mathematical process of decomposing a composite number into its prime factors, a task that, for very large numbers, is believed to be impossible for classical computers in a reasonable timeframe but would be achievable by a CRQC.

Field Programmable Gate Array (FPGA): Reconfigurable semiconductor devices for custom logic circuits.

Generative AI: AI capable of producing new content, such as images, text, or music.

Geophysical Sensing: An alt-PNT method based on using unique local gravity or magnetic fields as a "fingerprint" to assess location.

Geospatial Intelligence (GEOINT): Intelligence about the human activity on Earth derived from the exploitation and analysis of imagery, signals, or signatures with geospatial information.

Glide Vehicles: Unpowered vehicles that glide after being released from a launcher.

Global Navigation Satellite System (GNSS): A satellite navigation system with global coverage. As of 2023, four global systems are operational: the U.S.'s GPS, Russia's Global Navigation Satellite System (GLONASS), China's BeiDou Navigation Satellite System, and the European Union's Galileo.

Global Positioning System (GPS): A satellite-based radio navigation system owned by USG and operated by USSF. It is one of the GNSSs that provides geolocation and time information to a GPS receiver anywhere on or near Earth where there is an unobstructed line of sight to four or more GPS satellites.

Graphic Processing Unit (GPU): A specialized electronic circuit initially designed to accelerate computer graphics and image processing.

Gravimetric Energy Density: The available energy per unit mass of a substance.

Harvest Now, Decrypt Later (HNDL): A strategy taken by bad actors and governments in which they harvest classically encrypted data in transit and hold it until quantum technology advances, with the intention of decrypting the data with a CRQC in the future.

High-Density Energy Storage (HDES): A technology or system designed to store a large amount of energy in a compact space or mass, enabling the efficient storage of substantial energy quantities.

High-Energy Lasers (HELs): Lasers producing powerful beams for military applications.

High-Power Microwaves (HPMs): Microwaves used as directed energy weapons.

Hybrid Encryption: The use of multiple algorithms to encrypt data, such that the cracking of one algorithm would not affect the security of the data.

Hypersonic Cruise Missiles (HCMs): A new generation of hypersonic systems that combines the speed of intercontinental ballistic missiles with the accuracy of cruise missiles.

Inertial Navigation: A strategy of achieving relative PNT via the use of accelerometers and gyroscopes.

In-Memory Computing (IMC): Processing data in main memory rather than fetching it from storage.

Integrated Visual Augmentation System (IVAS): An AR headset being developed by Microsoft for the U.S. Army.

Intelligence, Surveillance, and Reconnaissance (ISR): Provides the foundation for all military operations. The individual elements are: intelligence, the final product derived from surveillance and reconnaissance fused with other information; surveillance, the persistent monitoring of a target; and reconnaissance, information-gathering conducted to answer a specific military question.

Internet of Military Things (IoMT): The application of IoT in military contexts.

Internet of Things (IoT): The interconnected network of physical devices with embedded sensors and software.

Joint All-Domain Command and Control (JADC2): A program aimed at connecting sensors from all branches of the armed forces into a unified network powered by AI.

Kinetic c-UAS: c-UAS methods involving physical effects.

Large Language Models (LLMs): AI models with vast amounts of parameters for natural language understanding.

Legion-X: An autonomous networked combat solution based on robotic platforms and heterogeneous swarms, developed by Israeli defense contractor Elbit Systems.

LEO Satellite-Based PNT: An alt-PNT method based on signals from low Earth orbit (LEO) satellites (vs. GPS satellites, which exist in medium Earth orbit [MEO]).

Lithium-Ion Battery: A type of rechargeable battery that uses the reversible intercalation of Li+ ions into electronically conducting solids to store energy.

Logical Qubit: Groups of physical qubits working together to perform a computation. By grouping with error-correcting code, the error rates of physical qubits can be ameliorated. As of 2023, the estimated number of physical qubits required for one error-corrected logical qubit is about 1,000.

Mach: A dimensionless metric in fluid dynamics representing the ratio of flow velocity past a boundary to the local speed of sound. By definition, Mach 1 is equal to the speed of sound. A hypersonic speed is one that exceeds Mach 5 (five times the speed of sound).

Metadata: Data providing information about other data.

Modeling and Simulation (M&S): Creating virtual representations of systems for analysis and testing.

Modular Open Software Architecture: Software design promoting modular and open systems.

Modular Open Systems Approach (MOSA): Design approach emphasizing interoperability and flexibility.

Multivariate Model: A statistical model with multiple variables.

National Cybersecurity Center of Excellence (NCCoE): A public-private partnership that is developing a framework to help industry with the post-quantum cryptography (PQC) migration.

National Defense Authorization Act (NDAA): The NDAA provides authorization of appropriations for DOD, nuclear weapons programs of the Department of Energy, and other defense-related activities. In addition to serving as an authorization of appropriations, it establishes defense policies and restrictions, and addresses organizational administrative matters related to the DOD..

National Security Memorandum 10 (NSM-10): Released in May 2022, NSM-10 requires an inventory of all federal IT systems, particularly those which are vulnerable to a CRQC.

Neural Networks: Computing systems modeled after the human brain's neural structure.

Neuromorphic Computing: Computing inspired by the human brain's neural structure, which often includes IMC.

Non-Earth Imaging (NEI): The observation and imaging of celestial objects beyond Earth, such as other planets, moons, stars, and space phenomena, and also man-made resident space objects, particularly those in Earth's orbit.

Non-Kinetic c-UAS: c-UAS methods that do not involve physical effects.

Non-Von Neumann Architecture: Any compute architecture that cannot be classified as von Neumann and in which one or more functions may be one and the same (e.g., in-memory computing). In particular, in non-von Neumann architectures, data and instructions are stored in separate memories, multiple data buses may be used, and instructions can be executed concurrently, allowing for parallel processing.

Optical Clock: A subset of atomic clocks that uses optical transitions for high precision and, as a result, achieves 100 times higher accuracy than today's SOTA atomic clocks.

Orbit Propagation: The calculation and prediction of the future positions and trajectories of objects in orbit based on their current state, often used for space situational awareness and collision avoidance.

Photonics: Optical computing or photonic computing uses light waves produced by lasers or incoherent sources for data processing, data storage, or data communication for computing. For decades, photons have shown promise to enable a higher bandwidth than the electrons used in conventional computers.

Physical Qubit: The basic unit of quantum information, typically a quantum two-level system, like the spin of an electron or the polarization of a photon, physically realized in a quantum computer. A physical qubit on its own is not error corrected.

Platform-agnostic: Compatible with various hardware or software platforms.

Post-Quantum Cryptography (PQC): Cryptographic algorithms believed to be resistant to decryption by quantum computers.

Predictive Maintenance: Anticipating equipment failures to perform maintenance before issues arise.

Project Convergence: A U.S. Army initiative to advance capabilities through integration and experimentation. It is the Army's version of the JADC2 concept.

Public-Key Encryption (PKE): A cryptographic system that uses a pair of keys (public and private) for secure communication, where the public key is shared openly, while the private key is kept secret. PKE is based on the difficulty of solving certain mathematical problems.

Quantum Clock: While an atomic clock measures a cloud of randomly oscillating atoms, a quantum clock instead measures atoms that have been entangled. The resulting correlation of the atoms allows their vibrations to be measured more accurately.

Quantum Computing (QC): An emerging type of computing that leverages the principles of quantum mechanics, allowing quantum bits (qubits) to exist in multiple states simultaneously, potentially solving complex problems exponentially faster than classical computers.

Quantum Computing Cybersecurity Preparedness Act: Signed in 2022, the act orders an examination of all USG agencies' cryptography.

Quantum Encryption: A form of encryption that uses the principles of quantum mechanics, the primary example being quantum key distribution (QKD). It is distinct in principle, application, and outcome from PQC, which relies on mathematics rather than physics.

Quantum Key Distribution (QKD): A quantum encryption protocol that uses quantum properties to secure the exchange of cryptographic keys between parties, providing a means to detect eavesdropping.

Quantum Supremacy: The point at which a quantum computer can perform a specific computational task faster than the best classical computers, showcasing the superior computational power of quantum systems. Quantum supremacy was achieved in 2019 by Google's Sycamore quantum computer; however, the particular task completed by Sycamore was not considered a "useful" problem.

Quantum Utility: The theoretical point at which a quantum computer can perform a task of practical economic or military value to humans faster than the best classical computers.

Relative PNT: A PNT system that can navigate in the absence of external signals and based only on relative position as determined by a variety of on-platform sensors, such as inertial sensors and chip-scale atomic and/or optical clocks.

Replicator: A Pentagon program that aims to produce multiple thousands of attritable autonomous systems across multiple domains by 2026.

Resident Space Objects (RSOs): Objects in space that reside in a particular orbit for an extended period, often referring to satellites or other man-made objects.

RF Jamming: Using RF signals to interfere with or block communication.

RF-Based PNT: An alt-PNT method based on intentional and/or opportunistic radio frequency signals. Enhanced long-range navigation (eLORAN) is an example.

Scramjet: An air-breathing engine designed for hypersonic flight.

SDA Tools, Applications, and Processing (TAP) Lab: The lab's Accelerator program provides the opportunity for Space Systems Command, AFRL, and the USAF Office of Scientific Research to work together to convert cutting-edge software prototypes into commercial products.

Silicon-Anode (SiA): An anode made of silicon, which can hold approximately 10 times as many lithium-ions by weight as graphite.

Software Tests: Procedures to verify that software functions correctly.

Solid-State Battery (SSB): A battery that uses solid electrodes and a solid electrolyte instead of liquid or polymer gel electrolytes found in lithium-ion or lithium polymer batteries.

Space Battlespace Awareness: A term often used in military contexts, referring to the awareness and understanding of the space environment, including potential threats and opportunities for military operations.

Space Domain Awareness (SDA): The ability to rapidly predict, detect, track, identify, warn, characterize, and attribute threats to U.S., commercial, allied, and partner space systems.

Space Situational Awareness (SSA): The ability to detect, track, and predict the movement of objects in Earth's orbit, primarily focusing on man-made objects such as satellites and space debris.

Space Traffic Management (STM): The coordination and regulation of space activities through the monitoring and control of space objects to prevent collisions and ensure the responsible and sustainable use of space.

Sub-Modality: A specific mode or attribute within a broader category.

Swarm: A group of entities working together in a coordinated manner.

Taiwan Semiconductor Manufacturing Company (TSMC): A Taiwanese multinational semiconductor contract manufacturing and design company and the global leader in the pure-play wafer foundry market, particularly for advanced-node processes.

Task Force Lima: Led by CDAO, a generative AI task force charged with monitoring, developing, evaluating, and recommending the responsible and secure implementation of generative AI capabilities across DOD.

Tensor Processing Unit (TPU): Google's custom ASIC designed to accelerate neural networks, such as computer vision models.

Testing and Evaluation (T&E): Assessing the performance and capabilities of systems.

Tip and Cue: A process in space surveillance where information (tip) from one sensor is used to direct another sensor (cue) to focus on a specific area of interest, enhancing the efficiency of space observation.

Training Data: Data used to train ML models.

U.S. Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act: A federal statute signed into law by President Joe Biden on August 9, 2022. The act authorizes roughly $280 billion in new funding to boost domestic research and manufacturing of semiconductors in the U.S., of which it appropriates $52.7 billion.

U.S. Joint Counter-Small Unmanned Aircraft Systems Office (JCO): An office established by the Secretary of the Army in 2020 to lead and direct joint counter-small UAS doctrine, requirements, materiel, and training to address current and future small UAS threats.

Unmanned Aerial System (UAS): Pilotless aircraft controlled autonomously or via remote human operators.

USAF Advanced Battle Management System: A USAF system for integrated C2. It is the USAF's version of the JADC2 concept.

Visual Positioning Systems (VPSs): An alt-PNT method based on visual cues, which can include terrain-based visuals (e.g., mountains, oceans, other Earth-based landmarks) or celestial-based visuals (i.e., the relative position of the stars).

Volumetric Energy Density: The available energy per unit volume of a substance.

Von Neumann Architecture: A computing architecture that consists of distinct processing, control, memory, input, and output functions. Data and instructions share the same memory, typically use a single data bus, and execute instructions sequentially.

Years to Quantum (Y2Q): The number of years between present day and the advent of a CRQC.

Zumwalt Destroyer: A class of guided missile destroyers in the U.S. Navy.

References

Introduction

"'The Changing Methods of Warfare' at Ft. Leavenworth, KS, Oct. 23, 2023 by COL (R) John Antal." *YouTube,* uploaded by John Antal, 30 Oct. 2023, www.youtube.com/watch?v=TcHnZxlHj0M.19 Apr. 2024.

1. AI Chips Citations

"Analyzing NVIDIA's growth strategy: How the semiconductor leader is powering generative AI and the future of computing." *CB Insights*, Apr. 2023, https://app.cbinsights.com/research/nvidia-strategy-map-investments-partnerships-acquisitions/.

Budryk, Zack. "China Imposes Export Controls on Rare Minerals Used to Make Semiconductor Chips." *The Hill*, 3 July 2023, www.thehill.com/policy/energy-environment/4079680-china-imposes-export-controls-on-rare-minerals-used-to-make-semiconductor-chips.

Burke, Brendan and Matthew Nacionales. "Inferring the Future of AI Chips." *PitchBook*. Emerging Tech Research, Nov. 2022, https://files.pitchbook.com/website/files/pdf/Q4_2022_PitchBook_Analyst_Note_Inferring_the_Future_of_AI_Chips_1281.pdf#page=1.

"Expanding Domestic Manufacturing of Secure, Custom Chips for Defense Needs." *DARPA*, Mar. 2021, https://www.darpa.mil/news-events/2021-03-18.

"ERI Overview and Structure." DARPA, Mar. 2023, https://www.darpa.mil/work-with-us/electronics-resurgence-initiative.

Fazzari, Saverio, et al. "Interview with Saverio Fazzari, Senior Lead Engineer/Engineering Fellow for Microelectronics at Booz Allen Hamilton." 15 Sept. 2023.

Gulati, Kanu, et al. "Interview with Kanu Gulati, Ph.D., Partner at Khosla Ventures." 19 Oct. 2023.

Hadland, Erik, et al. "Interview with Erik Hadland, Ph.D., Director of Technology Policy at the Semiconductor Industry Association." 13 Oct. 2023.

Heath, Ryan. "China fears are driving a new 'AI industrial complex.'" *Axios*, 23 Jan. 2024, https://www.axios.com/2024/01/23/china-taiwan-nvidia-ai-chatgpt-industrial-complex.

Kahn, Saif M. "AI Chips: What They Are and Why They Matter." *Center for Security and Emerging Technology (CSET)*, Apr. 2020, https://cset.georgetown.edu/publication/ai-chips-what-they-are-and-why-they-matter/.

Leopold, George. "DARPA Chip Effort Advances AI Hardware." *Datanami*, Aug. 2020, https://www.datanami.com/2020/08/21/darpa-chip-effort-advances-ai-hardware/.

Ordun, Catherine, et al. "Interview with Catherine Ordun, Ph.D., Vice President at Booz Allen Hamilton." 1 Dec. 2023.

Palmer, Doug, et al. "Interview with Doug Palmer, Microelectronics and Supply Chain Practice Lead at Booz Allen Hamilton." 7 Sept. 2023.

Pati, Suchita, et al. "Computation vs. Communication Scaling for Future Transformers on Future Hardware." *Advanced Micro Devices, Inc. and University of Wisconsin-Madison*, https://arxiv.org/ftp/arxiv/papers/2302/2302.02825.pdf.

Raff, Edward, et al. "Interview with Edward Raff, Ph.D., Director of Emerging AI at Booz Allen Hamilton." 12 Sept. 2023.

Rao, Fernando, et al. "Interview with Fernando Rao, Lead Associate at Booz Allen Hamilton." 18 Sept. 2023.

Rizzo, Anthony, et al. "Transferring Data with Many Colors of Light Simultaneously." *Columbia University Engineering*, June 2023, https://www.engineering.columbia.edu/news/transferring-data-with-many-colors-of-light-simultaneously.

Sargent, John F. Jr., et al. "Frequently Asked Questions: CHIPS Act of 2022 Provisions and Implementation." *Congressional Research Service*, Apr. 2023, https://crsreports.congress.gov/product/pdf/R/R47523.

Stanford University. "Summary of AI Provisions from the National Defense Authorization Act 2023." *Stanford University Human-Centered Artificial Intelligence*, 2023, https://hai.stanford.edu/summary-ai-provisions-national-defense-authorization-act-2023.

Swanson, Ana. "Defense Department Awards Chip Funding to Fuel Domestic Research." *The New York Times*, Sep. 2023, https://www.nytimes.com/2023/09/20/us/politics/defense-chips-taiwan-semiconductors.html.

United States, Executive Office of the President [Joseph R. Biden Jr.]. Executive Order 14105: Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern. 9 Aug. 2023. *Federal Register*, vol. 88, no. 154, pp. 54867–71, www.govinfo.gov/content/pkg/FR-2023-08-11/pdf/2023-17449.pdf.

Warchall, Julian, et al. "Interview with Julian Warchall, Ph.D., Lead Associate – Semiconductor Electronics at Booz Allen Hamilton." 19 Sept. 2023.

2. Alt-PNT Citations

Burke, John, et al. "Interview with John Burke, Principal Director of Quantum Science for DOD." 8 Jan. 2024.

Cozzens, Tracy. "Russia Issues Threat to GPS Satellites - GPS World." *GPS World*, 29 Nov. 2021, www.gpsworld.com/russia-issues-threat-to-gps-satellites/.

"Defense Budget Overview: United States Department Of Defense Fiscal Year 2023 Budget Request." Office Of The Under Secretary Of Defense (Comptroller)/Chief Financial Officer, Apr. 2022, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.

Farinholt, Jacob, et al. "Interview with Jacob Farinholt, Ph.D., Chief Quantum Scientist; Ryan Caulfield, Lead Scientist; and Adam Iaizzi, Ph.D., Quantum Physicist at Booz Allen Hamilton." 22 Sept. 2023.

Farinholt, Jacob, et al. "Interview with Jacob Farinholt, Ph.D., Chief Quantum Scientist at Booz Allen Hamilton." 19 Sept. 2023.

"FY2022 National Defense Authorization Act: Context and Selected Issues for Congress." Congressional Research Service, 20 May 2022, https://sgp.fas.org/crs/natsec/R47110.pdf.

Goward, Dana. "NSC director: GPS 'Still a Single Point of Failure.'" *GPS World*, 4 Jan. 2022, https://www.gpsworld.com/nsc-director-gps-still-a-single-point-of-failure/.

"GPS Alternatives: DOD Is Developing Navigation Systems But Is Not Measuring Overall Progress." *U.S. Government Accountability Office*, 5 Aug. 2022, www.gao.gov/products/gao-22-106010.

Hansen, Andrew, et al. "Complementary PNT and GPS Backup Technologies Demonstration Report." *U.S. Department of Transportation*, Jan. 2021.

Khuzadi, Mbuyi, et al. "Interview With Mbuyi Khuzadi, Chief Engineer at Booz Allen Hamilton." 22 Sept. 2023.

Martinez, Isabella, and Dylan Rudy. "Quantum Tech for Positioning, Navigation, and Timing." *Booz Allen Hamilton*, 6 Oct. 2023, www.boozallen.com/expertise/analytics/quantum-sensing.html.

Memmen, Sean, et al. "Interview with Sean Memmen, Senior Associate at Booz Allen Hamilton." 21 Sept. 2023.

O'Connor, Alan C., et al. "Economic Benefits of the Global Positioning System (GPS)." *National Institute of Standards and Technology*, June 2019.

Pedrozo-Peñafiel, Edwin, et al. "Entanglement on an optical atomic-clock transition." *Nature*, vol. 588, no. 7838, 2020, pp. 414–418, https://www.nature.com/articles/s41586-020-3006-1.

"Positioning, Navigation, and Timing." *Cybersecurity and Infrastructure Security Agency*, www.cisa.gov/topics/risk-management/positioning-navigation-and-timing.

"Quantum Sensing Enters the DOD Landscape in First-of-a-Kind, High-Performance Atomic Gyroscope Space Demonstration." *Defense Innovation Unit*, 27 Sept. 2023, www.diu.mil/latest/quantum-sensing-enters-the-DOD-landscape-in-first-of-a-kind-high-performance.

Ronat, Odile. "Alternative PNT Solutions Patch GNSS Vulnerabilities," *Microwave Product Digest*, 24 Oct. 2022, https://www.mpdigest.com/2022/10/24/alternative-pnt-solutions-patch-gnss-vulnerabilities/.

Schwindt, Peter, et al. "Interview With Peter Schwindt, Ph.D., Scientist at Sandia National Lab." 19 Oct. 2023.

Shipp, Jac, et al. "Interview With Jac Shipp, Principal at Booz Allen Hamilton." 21 Sept. 2023.

United States, Executive Office of the President [Donald J. Trump]. Executive Order 13905: Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services. 12 Feb. 2020. *Federal Register*, vol. 85, no. 32, 18 Feb. 2020, pp. 9359–61, www.govinfo.gov/content/pkg/FR-2020-02-18/pdf/2020-03337.pdf.

Zerkle, Roderick, et al. "Interview With Rick Zerkle, Principal at Booz Allen Hamilton." 28 Sept. 2023.

3. Autonomous Swarm Citations

Azulay, Yuval. "Advanced Israeli Weaponry Playing Major Role in Azerbaijan's Nagorno-Karabakh Offensive." *CTech*, 10 Feb. 2023, www.calcalistech.com/ctechnews/article/rjhofzoet.

Blais, Marc-André and Moulay A. Akhlou. "Reinforcement Learning for Swarm Robotics: An Overview of Applications, Algorithms and Simulators." *Cognitive Robotics*, vol. 3, 2023, pp. 226–256. https://doi.org/10.1016/j.cogr.2023.07.004.

Dhapte, Aarti. "China and the United States Military Comparison in 2023." Market Research Future, 9 Feb. 2023, www.marketresearchfuture.com/news/china-and-the-united-states-military-comparison-in-2023.

Dorigo, Marco, et al. "Swarm Robotics: Past, Present, and Future." *Proceedings of the IEEE*, vol. 109, no. 7, 2021, pp. 1152–1165. https://doi.org/10.1109/JPROC.2021.3072740.

Eckstein, Megan. "US Marines Are Developing Air-Launched Swarming Munitions for Helos." *Defense News*, 5 June 2023, www.defensenews.com/unmanned/2023/06/05/us-marines-are-developing-air-launched-swarming-munitions-for-helos/.

Editorial Board. "The Pentagon's New Drone Program Would Make Even More Sense with Money Attached." *The Washington Post*, 13 Oct. 2023, www.washingtonpost.com/opinions/2023/10/13/replicator-pentagon-kathleen-hicks-drones/.

Garamone, Jim. "Hicks Discusses Replicator Initiative." U.S. Department of Defense, 7 Sept. 2023, www.defense.gov/News/News-Stories/Article/Article/3518827/hicks-discusses-replicator-initiative/.

Hambling, David. "Israel Rolls Out Legion-X Drone Swarm for the Urban Battlefield." *Forbes*, 24 Oct. 2022, www.forbes.com/sites/davidhambling/2022/10/24/israel-rolls-out-legion-x-drone-swarm-for-the-urban-battlefield/?sh=5ef90a084f49.

Kallenborn, Zachary. "InfoSwarms: Drone Swarms and Information Warfare." *The US Army War College Quarterly: Parameters*, vol. 52, no. 2, summer 2022, pp. 87–102. https://doi.org/10.55540/0031-1723.3154.

Lappas, Vaios, et al. "Swarming: A Disruptive, Game Changing Technology for Defense Applications." *EDA Research, Technology, and Innovation Papers Award 2023*. European Defence Agency. www.eda.europa.eu/docs/default-source/brochures/eda-rti-papers-award-2023_web.pdf.

Legion-X. Elbit Systems Ltd., www.elbitsystems.com/product/legion-x/.

McMillan, Tim. "Pentagon Secretly Working to Unleash Massive Swarms of Autonomous Multi-Domain Drones to Dominate Enemy Defenses." *The Debrief*, 3 Feb. 2023, https://thedebrief.org/pentagon-secretly-working-to-unleash-massive-swarms-of-autonomous-multi-domain-drones-to-dominate-enemy-defenses/.

OFFensive Swarm-Enabled Tactics (OFFSET) (Archived). Defense Advanced Research Projects Agency, www.darpa.mil/work-with-us/offensive-swarm-enabled-tactics.

Sabbagh, Dan. "Houthis Call West's Bluff with Renewed Red Sea Drone Assault." *The Guardian*, 10 Jan. 2024, www.theguardian.com/world/2024/jan/10/houthis-call-wests-bluff-with-renewed-red-sea-drone-assault.

Saffre, Fabrice, et al. "Self-Swarming for Multi-Robot Systems Deployed for Situational Awareness." *New Developments and Environmental Applications of Drones*, edited by Tarmo Lipping, et al., Springer, Cham, 2022, pp 51–72. https://doi.org/10.1007/978-3-030-77860-6_3.

Scharre, Paul [@paul_scharre]. "This is a thread about #swarms." *Twitter*, 12 Sept. 2018, twitter.com/paul_scharre/status/1039973204192886784.

Science & Tech Spotlight: *Drone Swarm Technologies*. U.S. Government Accountability Office, 14 Sept. 2023, www.gao.gov/products/gao-23-106930.

"Science & Technology Strategy for Intelligent Autonomous Systems." *Department of the Navy*, 2 July 2021, https://www.nre.navy.mil/media/document/department-navy-science-technology-strategy-intelligent-autonomous-systems.

Shahzad, Muhammad Muzamal, et al. "A Review of Swarm Robotics in a NutShell." *Drones*, vol. 7, no. 4, 2023, p. 269. www.mdpi.com/2504-446X/7/4/269.

Uppal, Rajesh. "DARPA's AMASS Initiative Empowers Command and Control of Swarms-of-Swarms against Potential Threats." *International Defense Security & Technology*, 4 Aug. 2023, www.idstch.com/military/unmanned/darpas-amass-initiative-empowers-command-and-control-of-swarms-of-swarms-against-potential-threats/.

4. Gen AI SW Citations

"10 Quotes by Generative AI Experts." Skim AI, https://skimai.com/10-quotes-by-generative-ai-experts/.

Currier, James. "Generative AI Market Map and 5-Layer Tech Stack - NFX." NFX, Dec. 2022, 1.

Davies, Nahla. "Copilot: GitHub's AI Tool Speeds Up Development, but Comes with Risks." *Rewind*, 30 Aug. 2022.

DeLong, Lois Anne. "CCS Researchers Find GitHub CoPilot Generates Vulnerable Code 40% of the Time." *NYU Center for Cybersecurity*, 15 Oct. 2021, https://cyber.nyu.edu/2021/10/15/ccs-researchers-find-github-copilot-generates-vulnerable-code-40-of-the-time/.

Ferrari, John, and Charles Rahr. "Army of Coders Needed to Make Replicator Drone Initiative a Success." C4ISRNET, Sightline Media Group, 14 Sep. 2023, https://www.c4isrnet.com/opinion/2023/09/14/army-of-coders-needed-to-make-replicator-drone-initiative-a-success/.

Hunt, Louis. "GitHub Copilot: AI-based Code Generation and the Future of Software Engineering: Digital Innovation and Transformation." *Harvard Business School Digital Initiative*, 29 Nov. 2022.

"IT Systems Annual Assessment: DOD Needs to Improve Performance Reporting and Development Planning." U.S. Government Accountability Office, 13 June 2023, www.gao.gov/products/gao-23-106117#:~:text=According%20to%20the%20Department%20of,FY%202021%20through%20FY%202023.

Little, John W. "Ai-Driven Transformation: A Strategy for the U.S. Intelligence Community." *Blogs of War*, Blogs of War, 19 May 2023, blogsofwar.com/ai-driven-transformation-a-strategy-for-the-u-s-intelligence-community/.

Shani, Inbal. "Survey reveals AI's impact on the developer experience." *The GitHub Blog*, 13 June 2023.

"What is a large language model?" AWS, https://aws.amazon.com/what-is/large-language-model/.

Zhang, Jingqiao and Andrew Bell. "Making LLMs cheaper & faster to train with HPO-Oracle Blogs." Oracle Blogs, 22 Feb. 2023.

5. HDES Citations

Army Climate Strategy. United States Army. 2022_army_climate_strategy.pdf.

Benson, Thomas R., et al. "Hydrothermal Enrichment of Lithium in Intracaldera Illite-Bearing Claystones." Science Advances, vol. 9, no. 35, Aug. 2023, p. eadh8183. DOI.org (*Crossref*), https://doi.org/10.1126/sciadv.adh8183.

Casimir, Anix, et al. "Silicon-Based Anodes for Lithium-Ion Batteries: Effectiveness of Materials Synthesis and Electrode Preparation." Nano Energy, vol. 27, Sept. 2016, pp. 359–76. *ScienceDirect*, https://doi.org/10.1016/j.nanoen.2016.07.023.

Ellenby, Dani. "Silicon Anode Structure Generates New Potential for Lithium-Ion Batteries." *ScienceDaily*, 8 Feb. 2021, https://www.sciencedaily.com/releases/2021/02/210208145916.

Garsten, Ed. "Archer EVTOL Deal with Air Force Could Ground Choppers." *Forbes*, 31 July 2023, www.forbes.com/sites/edgarsten/2023/07/31/archer-evtol-deal-with-air-force-could-ground-choppers/?sh=2d376e795bec.

GovWin Contract. Anthro Energy, Lithium-Ion Batteries.

GovWin Contract. NEOEX Systems Inc., Integrated Liquid Hydrogen Energy Systems for Long Range Unmanned Aerial Vehicles.

Innovates, Dallas, and David Seeley. "Defense Department Awards $30M to Create UT Dallas 'Energy Storage Systems Campus.'" *Dallas Innovates*, 18 Sept. 2023, https://dallasinnovates.com/defense-department-awards-30m-to-create-ut-dallas-energy-storage-systems-campus/.

National Blueprint for Lithium Batteries 2021-2030 - Department of Energy, www.energy.gov/sites/default/files/2021-06/FCAB%20National%20Blueprint%20Lithium%20Batteries%200621_0.pdf.

Patel, Prachi. "The Age of Silicon Is Here…for Batteries." *IEEE Spectrum*, 4 May 2023, https://spectrum.ieee.org/silicon-anode-battery.

Recovery Act: Archive | SmartGrid.Gov. 16 Dec. 2019, https://www.smartgrid.gov/archive/recovery_act.

Soderberg, Angus. "Battery Technology and the Military EV Transition." *American Security Project*, 9 Feb. 2023, https://www.americansecurityproject.org/battery-technology-and-the-military-ev-transition/.

The Power Transfer Cohort: Help the U.S. Army Bring Power to Electric Vehicles. Army Applications Laboratory, https://aal.army/assets/files/pdf/infosheet-power-transfer-cohort.pdf.

Uppal, Rajesh. "DARPA MINT Developing Long-Lasting and High-Performance Solid-State Batteries That Power Everything in US DOD." *International Defense Security & Technology*, https://idstch.com/technology/energy/darpa-mint-developing-long-lasting-and-high-performance-solid-state-batteries-that-power-everything-in-us-DOD.

"What's Next for Batteries." *MIT Technology Review*, https://www.technologyreview.com/2023/01/04/1066141/whats-next-for-batteries/.

Wu, Yingqiang, et al. "An Exploration of New Energy Storage System: High Energy Density, High Safety, and Fast Charging Lithium Ion Battery." Advanced Functional Materials, vol. 29, no. 1, Jan. 2019, p. 1805978. *DOI.org (Crossref)*, https://doi.org/10.1002/adfm.201805978.

6. Hypersonics Citations

Bitten, Ronald, et al. "Interview with Barrett McCann, Lead Engineer; Patrick Braker, Chief Engineer; and Ronald Bitten, Principal/Director at Booz Allen Hamilton." 26 Sept. 2023.

Brose, Christian. *The Kill Chain: Defending America in the Future of High-Tech Warfare*. Hachette Books, 2022.

"General Says Countering Hypersonic Weapons Is Imperative." U.S. Department of Defense, www.defense.gov/News/News-Stories/Article/Article/3391322/general-says-countering-hypersonic-weapons-is-imperative/.

Gomez del Campo, Felipe, et al. "Interview with Felipe Gomez Del Campo, CEO at Specter Aerospace." 3 Oct. 2023.

Harder, Donald, et al. "Interview with Donald Harder, Distinguished Engineer at Booz Allen Hamilton." 18 Sept. 2023.

Lewis, Mark J. "Critical Technologies: Hypersonics Interview with Dr. Mark Lewis, Ph.D., CEO at Purdue Applied Research Institute." *Institute for Defense and Government Advancement*, 2023.

McCann, Barrett, et al. "Interview with Barrett McCann, Lead Engineer at Booz Allen Hamilton." 22 Sept. 2023.

Memmen, Sean, et al. "Interview with Sean Memmen, SBosbotinis, James. Institute for Defense and Government Advancement, 2023, *Hypersonic Systems 2023 Key Developments Report*.

Office, U.S. Government Accountability. "Faster than the Speed of Sound: U.S. Efforts to Develop Hypersonic Weapons." U.S. GAO, 15 Sept. 2022, www.gao.gov/blog/faster-speed-sound-u.s.-efforts-develop-hypersonic-weapons.

Scully, Tim, et al. "Interview with Tim Scully, Senior Lead Engineer at Booz Allen Hamilton." 30 Sept. 2023.

Secretary of the Air Force Public Affairs. “Air Force Announces Hypersonic Missile Contract Award.” *Air Force Public Affairs*, 22 Sept. 2022, www.af.mil/News/Article-Display/Article/3167976/air-force-announces-hypersonic-missile-contract-award/.

U.S. Government Accountability Office. “Hypersonic Weapons: DOD Should Clarify Roles and Responsibilities to Ensure Coordination across Development Efforts.” *U.S. Government Accountability Office*, 8 Apr. 2021, www.gao.gov/products/gao-21-378.

U.S. Government Accountability Office. “Science & Tech Spotlight: Hypersonic Weapons.” *U.S. Government Accountability Office*, 3 Oct. 2019, www.gao.gov/products/gao-19-705sp.

“U.S. Hypersonic Weapons and Alternatives.” *Congressional Budget Office*, www.cbo.gov/publication/58924#_idTextAnchor098.

Van Wie, David M., et al. “Hypersonic Airbreathing Propulsion.” *Johns Hopkins Apl Technical Digest*, vol. 26, no. 4, 2005, sec www.jhuapl.edu/techdigest/content/techdigest/pdf/V26-N04/26-04-VanWie.pdf.

Vergun, David. “Official Describes DOD Hypersonics Development, Strategy and Opportunities.” *U.S. Department of Defense*, 24 Feb. 2021, www.defense.gov/News/News-Stories/Article/Article/2514498/official-describes-DOD-hypersonics-development-strategy-and-opportunities/.

7. MMAI Citations

Bonelli, Enzo, et al. “Interview with Enzo Bonelli, Lead Technologist at Booz Allen Hamilton.” 19 Oct. 2023.

Brawner, Keith Ph. D., et al. “Interview with Dr. Keith Brawner, Senior Scientist and Program Manager at U.S. Army Futures: CCDC Soldier Center.” 12 Oct. 2023.

Brenton, Cutter, et al. “Interview with Cutter Brenton, Principal at Booz Allen Hamilton.” 3 Oct. 2023.

Daigle, Lisa. “AI program from DARPA aims to transform multimedia analysis.” *Military Embedded Systems*. 19 Sept. 2022. https://militaryembedded.com/ai/big-data/ai-program-from-darpa-aims-to-transform-multimedia-analysis.

Edwards, Ted, et al. “Interview with Ted Edwards, Lead Technologist at Booz Allen Hamilton.” 19 Sept. 2023.

Harper, Jon. “Pentagon planning joint development efforts for ‘multimodal’ generative AI.” *Defense Scoop*. 15 June 2023. https://defensescoop.com/2023/06/15/pentagon-planning-joint-development-efforts-for-multimodal-generative-ai/.

“Multimodal Learning Explained: How It’s Changing the AI Industry So Quickly.” ABI Research: *The Tech Intelligence Experts*. https://www.abiresearch.com/blogs/2022/06/15/multimodal-learning-artificial-intelligence/

Ordun, Catherine, et al. “Interview with Catherine Ordun, Executive Advisor at Booz Allen Hamilton.” 25 Oct. 2023.

Ordun, Catherine. “NIH Combats Cancer Pain Using Artificial Intelligence.” *Booz Allen Hamilton*. https://www.boozallen.com/insights/ai/nih-combats-cancer-pain-using-artificial-intelligence.html.

Paran, Collin, et al. “Interview with Collin Paran, Senior Lead Technologist at Booz Allen Hamilton and Karis Courey, Staff Technologist at Booz Allen Hamilton.” 19 Oct. 2023.

Patch, George, et al. “Interview with George Patch, Principal at Booz Allen Hamilton. 27 Sept. 2023.

Shwartz-Ziv, Ravid and Yann LeCun. “To Compress or Not to Compress- Self-Supervised Learning and Information Theory: A Review.” *Cornell University*. 21 Nov. 2023. https://arxiv.org/abs/2304.09355.

“Small Business Innovation Research (SBIR) Program SBIR 23.2 Program Broad Agency Announcement (BAA).” *Department of Defense*. https://media.defense.gov/2023/Apr/11/2003197777/-1/-1/1/DOD_23.2_FULL.PDF.

Tabassi, Elham. “NIST AI Update: Information Security Privacy Advisory Board.” *National Institute of Standards and Technology*. 4 Mar. 2021. https://csrc.nist.gov/CSRC/media/Presentations/ai-and-ndaa-requirements-nsc-ai-commission-report/images-media/AI%20and%20NDAA%20Requirements_%20NSC%20AI%20Commission%20Report%20Tabassi.pdf.

Wade, Ethan, et al. “Interview with Ethan Wade, Chief Engineer at Booz Allen Hamilton.” 29 Sept. 2023.

8. NK-cUAS Citations

“Anduril and Epirus Integration Leads to New Counter-UAS Capability.” *Epirus*, 27 July 2023, www.epirusinc.com/news-item/anduril-and-epirus-integration-leads-to-new-counter-uas-capability.

Demarest, Colin. “Directed Energy Weapons Making Jump from Sci-Fi to Real World.” *Defense News*, 18 Sept. 2023, www.defensenews.com/battlefield-tech/2023/09/18/directed-energy-weapons-making-jump-from-sci-fi-to-real-world/.

Easley, Mikayla. “Army Piloting Pentagon’s Counter-UAS Efforts.” *National Defense*, 6 Oct. 2022, www.nationaldefensemagazine.org/articles/2022/10/6/army-piloting-pentagon-counter-uas-efforts.

“Global Counter-UAS Directory and Buyer’s Guide.” *Unmanned Airspace*. www.unmannedairspace.info/counter-uas-industry-directory/.

Harper, Jon. “JCO Aims to Shoot Down up to 50 Drones in Counter-Swarm Demo.” *DefenseScoop*, 11 Oct. 2023, www.defensescoop.com/2023/10/11/jco-aims-to-shoot-down-up-to-50-drones-in-counter-swarm-demo/.

Lonsdale, Joe. “Disruptive Defense Tech: A New Dawn for Directed Energy.” *C4ISRNET*, 6 Oct. 2023, www.c4isrnet.com/opinion/2023/10/06/disruptive-defense-tech-a-new-dawn-for-directed-energy/.

Monahan, Dennis, et al. “Interview with Dennis Monahan, Senior Lead Engineer, Booz Allen; Patrick Shannon, Principal/Director, Booz Allen; and David Stoudt, Senior Executive Advisor, Booz Allen.” 3 Oct. 2023.

Moore, Alex, et al. “Interview with Alex Moore, Partner, 8VC.” 20 Oct. 2023.

Sayler, Kelley M., et al. *Department of Defense Directed Energy Weapons: Background and Issues for Congress*. Congressional Research Service, 22 Aug. 2023, https://sgp.fas.org/crs/weapons/R46925.pdf.

Science & Tech Spotlight: Directed Energy Weapons. U.S. Government Accountability Office, 25 May 2023, www.gao.gov/products/gao-23-106717.

Soule, Greg, et al. “Interview with Greg Soule, Senior Associate, National Cyber Platform, Booz Allen.” 17 Oct. 2023.

Stewart, Emilie B. *Survey of PRC Drone Swarm Inventions*. China Aerospace Studied Institute, Oct. 2023, www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2023-10-09%20Survey%20of%20PRC%20Drone%20Swarm%20Inventions.pdf.

9. PQC Citations

Barker, William, and Murugiah Souppaya. “Migration to Post-Quantum Cryptography.” *National Cybersecurity Center of Excellence*, National Institute of Standards and Technology, Aug. 2021, https://csrc.nist.gov/pubs/pd/2021/08/04/migration-to-postquantum-cryptography/final.

Beach-Westmoreland, Nathaniel, and Meghan Hauser. “Interview With Nate Beach-Westmoreland, Head of Strategic Cyber Threat Intelligence at Booz Allen Hamilton.” 6 Sept. 2023.

Blackwell, Wes, et al. “Interview with Wes Blackwell, Principal, Booz Allen Ventures.” 24 Oct. 2023.

Brady, Taylor, et al. “Interview with Taylor Brady, Senior Lead Quantum Scientist at Booz Allen Hamilton.” 13 Sept. 2023.

“Committees - H.R.7535 - 117th Congress (2021-2022): Quantum Computing ...” *Congress.Gov*, 21 Dec. 2022, www.congress.gov/bill/117th-congress/house-bill/7535/committees.

DiBartolomeo, Stephen, et al. “Interview with Stephen DiBartolomeo, Principal at Scout Ventures.” 26 Oct. 2023.

Farinholt, Jacob, et al. “Interview with Jacob Farinholt, Ph.D., Chief Quantum Scientist; Jordan Kenyon, Ph.D., Senior Lead Scientist; and Isabella Martinez, Senior Lead Technologist at Booz Allen Hamilton.” 15 Sept. 2023.

Goodwin, Phil, and Heather West. “IDC TechBrief: Applying Post-Quantum Cryptography to Data Protection to Enhance Digital Trust.” IDC, via AlphaSense, 30 June 2023.

Harris, Briony. “This is the biggest risk we face with AI, by Google CEO Sundar Pichai.” *The World Economic Forum*, 23 Jan. 2020, https://www.weforum.org/agenda/2020/01/this-is-how-quantum-computing-will-change-our-lives-8a0d33657f/.

Kingsbury, Nick, et al. “Interview With Nick Kingsbury, Partner at Amadeus Capital Partners.” 27 Oct. 2023.

Kumar, Manish. “Post-quantum Cryptography Algorithm’s standardization and performance analysis.” *Array*, vol. 15, Apr. 2022, https://doi.org/10.1016/j.array.2022.100242.

“Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.” T*he White House*, The United States Government, 19 Jan. 2022, www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.

Moody, Dustin, et al. “Interview ith Dustin Moody, Ph.D., Mathematician at NIST.” 13 Oct. 2023.

Mosca, Michele, and Marco Piani. “Quantum Threat Timeline Report 2022.” *Global Risk Institute*, Dec. 2022. https://quantum-safe.ca/wp-content/uploads/2023/01/2022-quantum-threat-timeline-report-dec.pdf.

“Post-Quantum Cryptography Initiative: CISA.” *Cybersecurity and Infrastructure Security Agency CISA*, www.cisa.gov/quantum.

Reiter, Bob, et al. “Interview with Greg Starkey, Executive Advisor and Bob Reiter, Chief Scientist at Booz Allen Hamilton.” 6 Sept. 2023.

“SandboxAQ Awarded Contract to Bolster US Defense Infrastructure with Quantum-Resistant Cryptography.” *HPCwire*, SandboxAQ, 27 June 2023, www.hpcwire.com/off-the-wire/sandboxaq-awarded-contract-to-bolster-us-defense-infrastructure-with-quantum-resistant-cryptography/.

Schneider, Jacob W. S. “Quantum Computing: Examining the Quantum Computing Cybersecurity Preparedness Act: Insights.” *Holland & Knight*, 17 Jan. 2023, www.hklaw.com/en/insights/publications/2023/01/quantum-computing-examining-the-quantum-computing-cybersecurity.

Sideco, Francis. "Quantum Safe Cryptography—a Quantum Leap Needed Now." *Forbes*, Forbes Magazine, 27 Jan. 2023, www.forbes.com/sites/tiriasresearch/2023/01/25/quantum-safe-cryptography--a-quantum-leap-needed-now/?sh=5cf70eff49ea.

West, Heather. "IBM Quantum Safe Roadmap and Quantum Safe Technologies and the Urgency to Become Quantum Resilient." IDC, via AlphaSense, 10 May 2023.

West, Heather. "IT Infrastructure for Storage and Data Management Survey." IDC, via AlphaSense, Jan. 2023.

"Workshops and Timeline—Post-Quantum Cryptography: CSRC." *Computer Security Resource Center*, National Institute of Standards and Technology, csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline.

10. SDA Citations

Anderson, Chad, et al. "Interview with Chad Anderson, Founder and Managing Partner at Space Capital." 16 Oct. 2023.

Beck, Fred, et al. "Interview with Fred Beck, Principal at Booz Allen Hamilton." 12 Oct. 2023.

Biltgen, Patrick, et al. "Interview with Dr. Patrick Biltgen, Vice President at Booz Allen Hamilton." 17 Oct. 2023.

Bloom, Amelia, et al. "Space and Ground-Based SDA Sensor Performance Comparisons." *Amostech.Com*, 2022, amostech.com/TechnicalPapers/2022/Poster/Bloom.pdf.

Bracken, Phillip, et al. "Interview with Phillip Bracken and Ben Reed, CSO and CTO at Quantum Space." 19 Oct. 2023.

Ceperley, Daniel, et al. "Interview with Dr. Daniel Ceperley, COO at LeoLabs." 16 Oct. 2023.

Craig, Ron, et al. "Interview with Ron Craig, Vice President at Booz Allen Hamilton." 12 Oct. 2023.

Crowe, William, et al. "Interview with William Crowe, CEO at HEO." 25 Oct 2023.

Crusey, Jeff, et al. "Interview with Jeff Crusey, Partner at 7Percent Ventures." 17 Oct. 2023.

Cummings, Christopher, et al. "Interview with Dr. Christopher Cummings, Senior Lead Technologist at Booz Allen Hamilton." 26 Oct. 2023.

Day, Katherine, et al. "Interview with Katherine Day and Kate Fraser, Principal and Senior Associate at Booz Allen Hamilton." 24 Oct. 2023.

Department of Defense, United States Air Force Research Laboratory, et al. A Primer on Cislunar Space, *United States Air Force Research Laboratory*, May 2021, www.afrl.af.mil/Portals/90/Documents/RV/A%20Primer%20on%20Cislunar%20Space_Dist%20A_PA2021-1271.pdf?ver=vs6e0sE4PuJ51QC-15DEfg%3D%3D.

Department of Defense, United States Space Force, and John W. Raymond. https://www.spaceforce.mil/, June 2020, www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

Department of Defense. Space Policy Review and Strategy on Protection of Satellites, Sept. 2023, media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/comprehensive-report-for-release.pdf.

Erwin, Sandra. "Air Force: SSA Is No More; It's 'Space Domain Awareness'." *SpaceNews*, 14 Nov. 2019, spacenews.com/air-force-ssa-is-no-more-its-space-domain-awareness/.

Erwin, Sandra. "Keeping Watch on Aggressor Satellites a Key Challenge for U.S. Space Force." *SpaceNews*, 17 Apr. 2023, spacenews.com/keeping-watch-on-aggressor-satellites-a-key-challenge-for-u-s-space-force/.

Erwin, Sandra. "L3Harris Wins $1.2 Billion Contract to Maintain, Upgrade Space Surveillance Systems." *SpaceNews*, 29 Feb. 2020, www.spacenews.com/l3harris-wins-1-2-billion-contract-to-maintain-upgrade-space-surveillance-sensors/.

Erwin, Sandra. "Slingshot Aerospace Harnessing AI to Track Suspicious Satellites." *SpaceNews*, 6 Oct. 2023, spacenews.com/slingshot-aerospace-harnessing-ai-to-track-suspicious-satellites/.

European Space Agency, ESA Space Debris Office, and ESA Space Debris Office. https://www.Sdo.Esoc.Esa.Int, 2023, www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf.

Fielding, Alex, et al. "Interview with Alex Fielding, CEO and Chairman at Privateer Space." 31 Oct. 2023.

Haddad, Topher, et al. "Interview with Topher Haddad, CEO at Albedo Space." 19 Oct. 2023.

Hartman, Joshua. "Space Domain Awareness, Protection Requires More Space-Based Systems." *C4ISRNet*, 14 Apr. 2023, www.c4isrnet.com/thought-leadership/2023/04/14/space-domain-awareness-protection-requires-more-space-based-systems/.

Hesar, Siamak, et al. "Interview with Siamak Hesar, CEO at Kayhan Space." 18 Oct. 2023.

Hitchens, Theresa. "Along with New Office, Space Force Plots New Funding Pot for Commercial Buys by 2025." *Breaking Defense*, 6 June 2023, breakingdefense.com/2023/06/along-with-new-office-space-force-plots-new-funding-pot-for-commercial-buys-by-2025/.

Hitchens, Theresa. "At Hawaii Space Conference, DoD Space Monitoring Challenges in the Spotlight." *Breaking Defense*, 18 Sept. 2023, breakingdefense.com/2023/09/at-hawaii-space-conference-dod-space-monitoring-challenges-in-the-spotlight/.

Hitchens, Theresa. "China's SJ-21 'Tugs' Dead Satellite out of GEO Belt: Trackers." *Breaking Defense*, 26 Jan. 2022, breakingdefense.com/2022/01/chinas-sj-21-tugs-dead-satellite-out-of-geo-belt-trackers/.

Hitchens, Theresa. "The 5 Big Worries the Commerce Department Has about Space Traffic Management." *Breaking Defense*, 27 Feb. 2023, breakingdefense.com/2023/02/the-5-big-worries-the-commerce-department-has-about-space-traffic-management/.

Jones, Lewis, et al. "Interview with Lewis Jones, Vice President at Generation Space." 12 Oct. 2023.

Kowalski, William, et al. "Interview with William Kowalski, COO at Atomos Space." 21 Nov. 2023.

"L3Harris Selected to Integrate, Accelerate US Space Force's ATLAS Space Domain Awareness Project." *L3Harris*, 3 Feb. 2022, www.l3harris.com/newsroom/press-release/2022/02/l3harris-selected-integrate-accelerate-us-space-forces-atlas-space.

Lo, Eric, et al. "Interview with Eric Lo, Chief Engineer at Booz Allen Hamilton." 9 Oct. 2023.

Ludwigson, Jon, and Alissa Czyz. Space Situational Awareness: DOD Should Evaluate How It Can Use Commercial Data, Government Accountability Office, Apr. 2023, www.gao.gov/assets/gao-23-105565.pdf.

Marquez, Peter, et al. "Interview with Peter Marquez, Head of Space Policy at Amazon Web Services." 27 Oct. 2023.

McClintock, Bruce, et al. "The Time for International Space Traffic Management Is Now." *Rand.Org*, 5 June 2023, *www.rand.org/pubs/research_briefs/RBA1949-1.html*.

McDowell, Jonathan. "Satellite Statistics: Satellite and Debris Population." Jonathan's Space Report, 29 Mar. 2024, https://www.planet4589.org/space/stats/active.html.

Moreno, Michael, et al. "Interview with Michael Moreno, Global VC & Startup Partner Strategy at Amazon Web Services." 20 Oct. 2023.

Office of the President of the United States, Trump, Donald J. https://trumpwhitehouse.archives.gov/, 2018, trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/.

Oltrogge, D. L., et al. "Addressing the Debilitating Effects of Maneuvers on SSA Accuracy and Timeliness." Comspoc.Com, *COMSPOC*, Sept. 2023, comspoc.com/uploads/contents/C-20230920T000708/paper/addressing-the-debilitating-effects-of-maneuvers-on-ssa-accuracy-and-timeliness_paper.pdf.

"Northrop Grumman Awarded US Space Force Contract for Deep-Space Advanced Radar Capability." *Northrop Grumman*, 23 Feb. 2022, https://news.northropgrumman.com/news/releases/northrop-grumman-awarded-us-space-force-contract-for-deep-space-advanced-radar-capability.

"Northrop Grumman-Built Space Sensor Satellites Launch in Support of US Space Force-8 Mission." *Northrop Grumman,* 21 Jan. 2022, https://news.northropgrumman.com/news/releases/northrop-grumman-built-space-sensor-satellites-launch-in-support-of-us-space-force-8-mission.

Paran, Collin, et al. "Interview with Collin Paran and Dr. Erin Ryan, Senior Lead Technologist and Senior Lead Scientist at Booz Allen Hamilton." 20 Oct. 2023.

Pollpeter, Kevin. "Space Domain Awareness as a Strategic Counterweight." https://www.cna.org/, Nov. 2021, www.cna.org/archive/CNA_Files/pdf/space-domain-awareness-as-a-strategic-counterweight.pdf.

Pultarova, Tereza. "SpaceX Starlink Satellites Had to Make 25,000 Collision-Avoidance Maneuvers in Just 6 Months — and It Will Only Get Worse." Space.Com, 6 July 2023, www.space.com/starlink-satellite-conjunction-increase-threatens-space-sustainability.

Reilly, Jim, et al. "Interview with Dr. Jim Reilly, Executive Advisor at Booz Allen Hamilton." 26 Oct. 2023.

Rogers, Even, et al. "Interview with Even Rogers, CEO at True Anomaly." 2 Nov. 2023.

Rothzeid, David, et al. "Interview with David Rothzeid, Vice President at Shield Capital." 13 Oct. 2023.

Tuttle, Benjamin, et al. "Interview with Benjamin Tuttle, CTO at EOI Space." 24 Oct. 2023.

United States Space Force. Stratcom.Spaceforce.Mil, *United States Space Force*, Nov. 2023, https://www.starcom.spaceforce.mil/Portals/2/SDP%203-100%20Space%20Domain%20Awareness%20(November%202023)_pdf_safe.pdf?ver=jcB9D6t8Pq-tzgBdoESmww%3d%3d.

Weeden, Brian, and Victoria Sampson. "Global Counterspace Capabilities: An Open Source Assessment." https://Swfound.Org/, *Secure World Foundation*, Apr. 2023, swfound.org/media/207567/swf_global_counterspace_capabilities_2023_v2.pdf.

Wikan, Michael, et al. "Interview with Michael Wikan, Senior Lead Technologist at Booz Allen Hamilton." 23 Oct. 2023.

ABOUT BOOZ ALLEN

Trusted to transform missions with the power of tomorrow's technologies, Booz Allen Hamilton advances the nation's most critical civil, defense, and national security priorities. We lead, invest, and invent where it's needed most—at the forefront of complex missions, using innovation to define the future. We combine our in-depth expertise in AI and cybersecurity with leading-edge technology and engineering practices to deliver impactful solutions. Combining 110 years of strategic consulting expertise with the perspectives of diverse talent, we ensure results by integrating technology with an enduring focus on our clients. We're first to the future—moving missions forward to realize our purpose: **Empower People to Change the World®**.

Booz Allen®