



NIGHTDRAGON

MARKET REPORT:
**AUTONOMOUS
DEFENSE**

October 2025

www.nightdragon.com

Table of Contents

Foreword _____ 3

The Challenge _____ 5

The Opportunity _____ 8

The Market _____ 12

Q&A with Epirus CEO _____ 16

NightDragon Perspective _____ 18

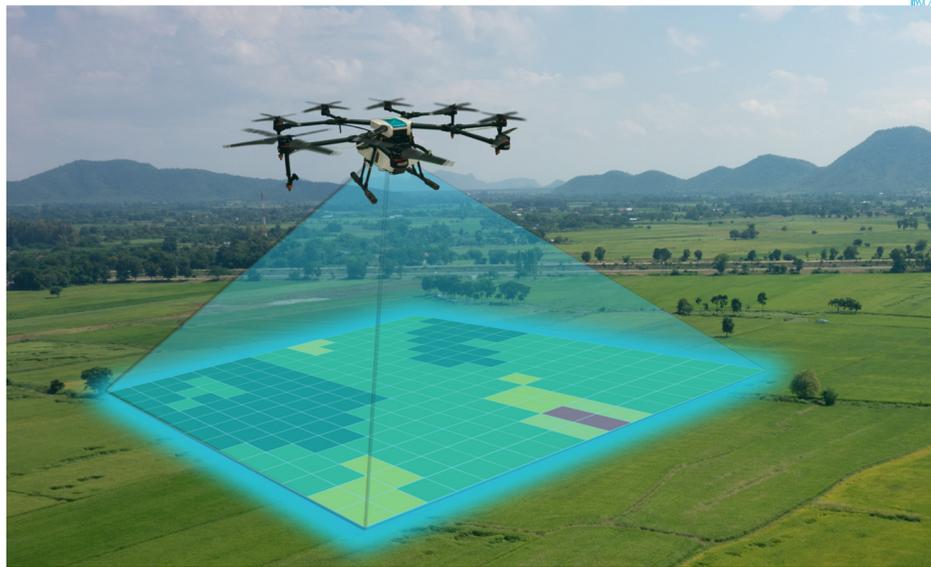
Foreword

The nature of warfare is undergoing a profound transformation. No longer defined by attritional battlefields or purely kinetic engagements, today's conflicts are shaped by rapid tempo, dispersed theaters, and a growing reliance on autonomous systems—ushering in a nonlinear, technology-driven era of operations for defense.

For centuries, military power has been understood through five domains: land, sea, air, space, and—most recently—cyber, which emerged as a defining frontier in the last two decades. Now, the accelerating adoption of autonomous systems demands recognition of a Sixth Domain: autonomy.

The rise of autonomy for defense is forcing a fundamental reimagining of the innovation landscape. Opportunities are emerging across government, industry, and academia to develop solutions that break from traditional models of procurement, integration, and sustainment. Within this new domain, autonomy is not just an additive capability for defense—it is a force multiplier. It changes the calculus for legacy systems by enabling strategies that are faster, cheaper, and more adaptive than ever before.

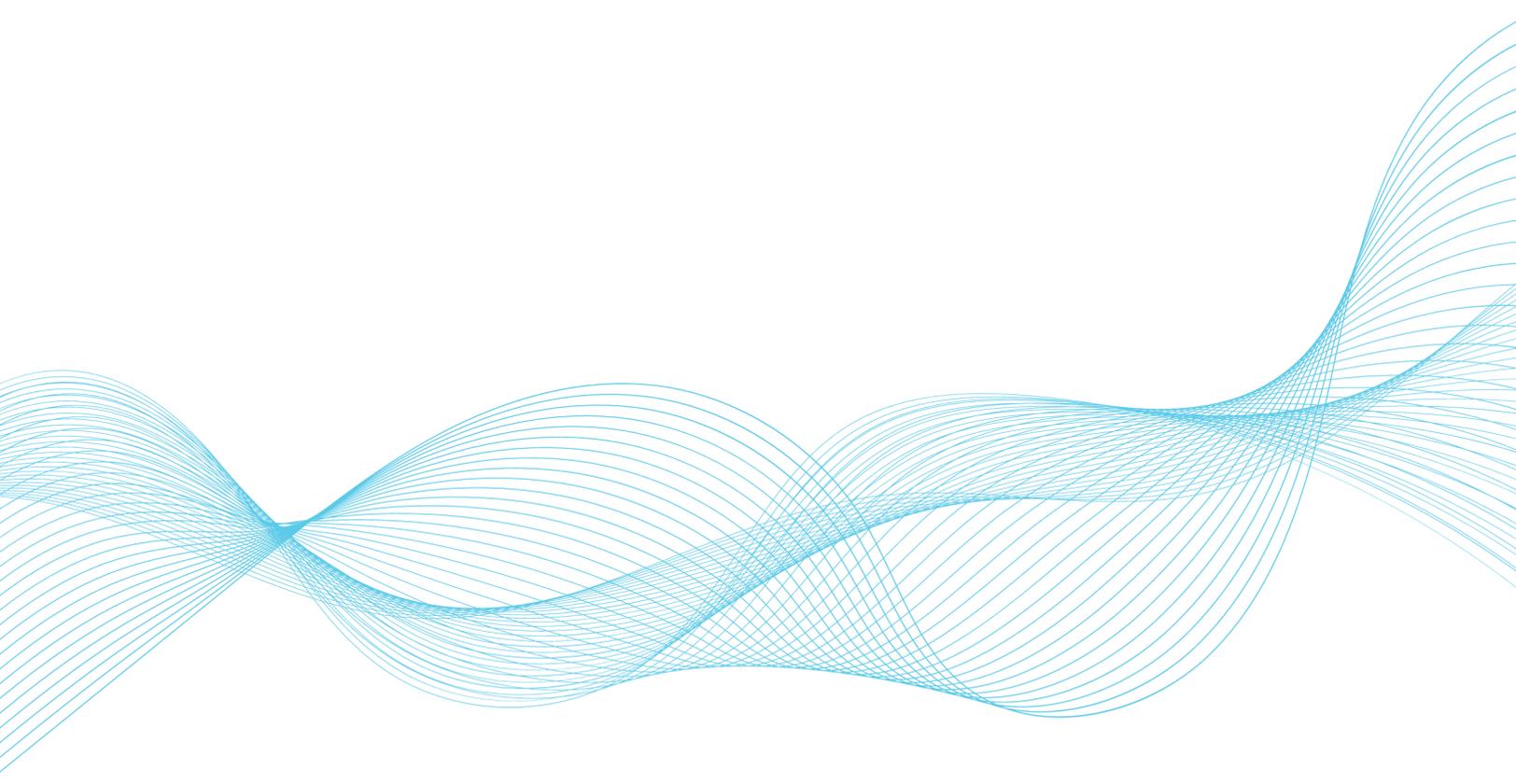
Critically, these capabilities are no longer theoretical. They are being embraced at scale by leading defense organizations. For example, the U.S. Coast Guard recently established a Program Executive Office for Robotics and Autonomous Systems to accelerate the development, acquisition, and sustainment of platforms such as counter-UAS and other unmanned technologies. This initiative



provides dedicated advocacy for resources and reflects the recognition that autonomy represents a technological revolution with far-reaching mission impact.

At the same time, autonomy is sparking a cascade of supporting innovation. The full potential of autonomous systems for defense depends on robust infrastructure: networks of sensors, edge computing platforms, interoperable data architectures, and resilient command-and-control ecosystems. Each of these building blocks is evolving rapidly, with momentum across the ecosystem to ensure autonomy can operate seamlessly—and safely—at scale.

In this report, we explore how autonomy is reshaping the defense technology sector and what that means for innovators, investors, and partners. NightDragon has already made four strategic investments in this space—Epirus, HawkEye360, Horizon3.ai and Saronic—but we believe the horizon of opportunity stretches far wider. As the Sixth Domain comes into focus, it will define the next era of defense innovation and create an enduring market for those positioned to lead.



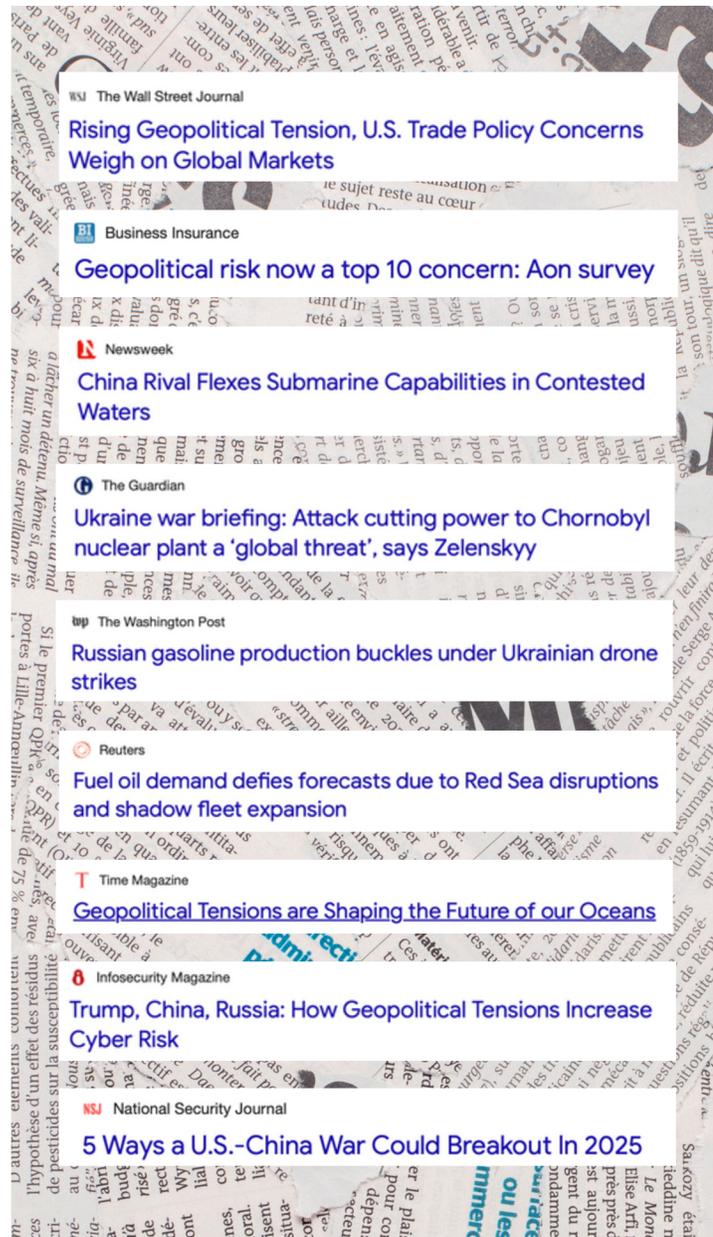
The Challenge

Escalating Geopolitical Landscape

The global security environment in 2025 is marked by escalating tensions and active conflicts that underscore the inadequacy of traditional defense strategies. In Ukraine, the conflict with Russia continues, with Ukrainian forces employing AI-powered drone swarms to conduct autonomous reconnaissance and strikes. These UASs operate in coordinated groups, adapting mid-mission and making real-time decisions without direct human input, highlighting the shift towards autonomous warfare.

In the South China Sea, China's assertive actions continue to challenge regional stability. Recent reports indicate that China has initiated oil and gas drilling operations within Taiwan's Exclusive Economic Zone, deploying large offshore platforms that could potentially serve dual-use purposes, including military applications.

The Red Sea region faces its own set of challenges, with Houthi rebels launching missiles and drones towards Israel and U.S. naval assets, disrupting global trade routes and heightening tensions between Iran and Israel. These developments underscore the interconnectedness of regional conflicts and their broader implications for global security.



Transition in Defense Tech & Domain Warfare

Historically, defense technology has been characterized by long development cycles, centralized procurement, and large-scale, monolithic systems. This approach was effective in a world where threats were more predictable and less dynamic. However, the rapid pace of technological advancement and the nature of modern conflicts demand a shift in how defense capabilities are developed and deployed.

Breakthroughs in artificial intelligence, autonomy, robotics, and advanced sensor systems are redefining the battlefield. For instance, the U.S. Department of Defense's "AI-First" strategic vision aims to embed AI tools across routine and mission-critical workflows to enhance decision-making and resource coordination, reflecting a broader trend towards integrating AI into defense operations.

Moreover, DARPA's Collaborative Combat Aircraft (CCA) program, with a \$8.9 billion investment, seeks to deploy over 1,000 autonomous drones that can operate alongside manned aircraft. This initiative, plus others such as Replicator and Replicator 2.0, represent a significant leap towards integrating autonomous systems into combat scenarios, emphasizing the need for agility and adaptability in modern warfare.



How Defenses Must Evolve

The integration of autonomy into both offensive and defensive strategies necessitates a fundamental transformation in defense operations. Autonomous systems enable rapid, scalable responses to threats, allowing for persistent surveillance, precision strikes, and enhanced situational awareness. However, this shift also introduces new challenges in terms of command and control, interoperability, and ethical considerations.

To counter increasingly sophisticated adversaries, defense forces must adopt autonomous systems that can operate in contested environments, adapt to evolving threats, and integrate seamlessly with existing platforms. This requires not only technological innovation but also changes in organizational structures, training, and procurement processes.

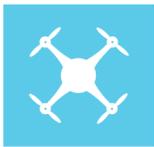
The urgency of this transformation is evident in the growing emphasis on faster procurement models and the acceleration of defense innovation. The establishment of dedicated offices, such as the U.S. Coast Guard's Program Executive Office for Robotics and Autonomous Systems, underscores the commitment to rapidly operationalizing unmanned systems across all statutory missions.

In summary, the convergence of geopolitical instability and technological advancements presents both challenges and opportunities for defense organizations. The ability to rapidly adapt and integrate autonomous systems will be crucial in maintaining strategic advantage and ensuring national security in an increasingly complex global landscape.

The Opportunity

Autonomy for defense is no longer a speculative edge technology – it is a force-multiplier creating immediate, concrete market opportunities across multiple layers of capability. The pivot toward the Sixth Domain, defined by the convergence of low-cost, unmanned robotic systems operating across domains, opens pockets of demand that span hardware, software, integration services, and entire new business models. Below we map the most salient opportunity areas for defense (acknowledging that autonomy is playing a role in other sectors as well), then call out the key inhibitors that must be solved if adoption is to scale.

Where Innovation is Happening



AIR (AUTONOMY IN THE AIR DOMAIN)

Autonomous aerial systems are redefining both ISR and strike missions. From low-cost, expendable drones deployed in swarms to long-endurance UASs, autonomy enables persistent surveillance, rapid targeting, and kinetic or non-kinetic effects at scale. Collaborative combat aircraft (CCA) programs – designed to team autonomous drones with manned fighters – illustrate how autonomy is becoming integral to air dominance.



SEA (AUTONOMY IN THE MARITIME DOMAIN)

Uncrewed surface vessels (USVs) and uncrewed underwater vehicles (UUVs) are transforming maritime operations. Applications include anti-submarine warfare, mine countermeasures, coastal surveillance and persistent blue-water ISR. For navies and coast guards, autonomy extends reach, lowers cost, and reduces risk to crews, while enabling round-the-clock presence across vast maritime theaters.



LAND (AUTONOMY IN THE GROUND DOMAIN)

Autonomous ground vehicles and logistics systems are streamlining supply

chains and protecting troops. Examples include convoy automation, robotic mules that resupply in contested environments, and unmanned ground combat systems for reconnaissance and fire support. Autonomy reduces exposure for personnel and accelerates maneuver, especially in urban or complex terrain.



SPACE (AUTONOMY IN THE SPACE DOMAIN)

Space assets increasingly depend on autonomy for resilience and survivability. Satellites use autonomous navigation, threat detection, and defensive maneuvers to counter anti-satellite weapons and electronic warfare. Autonomous maintenance, collision avoidance, and swarm architectures for satellite constellations are becoming critical to space domain awareness and sustained operations in orbit.



CYBER (AUTONOMY IN THE CYBER DOMAIN)

Autonomous capabilities are equally disruptive in cyberspace. AI-driven cyber defense platforms can detect, attribute, and respond to intrusions at machine speed, mitigating attacks faster than human analysts. On offense, autonomous tools allow adversaries to scale reconnaissance, exploit vulnerabilities, and deploy attacks in highly adaptive ways. Maintaining parity in this domain requires integrating autonomy directly into defensive cyber stacks.

Outside of the platform elements and mission-focused packages outlined above, we are also seeing autonomy innovation happening across other cross-segments of the Defense Tech sector. Some of those areas include:



SOFTWARE, DECISIONING & ORCHESTRATION

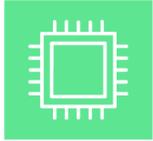
The real value is the software layer that enables distributed, trustable decision-making – autonomy engines, swarm orchestration, safe behavior verification, and explainable AI for human-machine teaming. This is a lucrative, recurring-revenue play (software subscriptions, data pipelines, M&S).



SENSOR FUSION, PERSISTENT SENSING & GEOINT

Autonomy needs high-fidelity, fused sensing (EO/IR, RADAR, SIGINT, AIS, commercial imagery) and rapid GEOINT pipelines. National and operational

customers are investing in GEOINT and generative/AI augmentation to turn high-volume data into timely decisions, creating opportunities for sensor makers, analytics vendors, and edge inference providers.



EDGE COMPUTE, COMMS, & RESILIENT C2

Distributed autonomy requires compute and inference at the edge, resilient mesh communications, and degraded-but-safe command models. Edge-AI hardware, mission-hardened compute modules, and secure data fabrics are critical infrastructure plays with defense and commercial demand.



MANUFACTURING, SUSTAINMENT, & RAPID FIELDING

Rapid prototyping, field-deployable additive manufacturing, and modular componentization enable faster iteration and local sustainment. Systems that shorten lead-times (on-demand printed parts, modular payloads) are becoming force-multipliers for readiness and resilience.



INTEGRATION AND SYSTEMS-OF-SYSTEMS

The greatest near-term demand is for integration: making sensors, platforms, autonomy stacks and C2 work together. Systems integrators, middleware providers, and firms that deliver certified, interoperable bundles will be essential.



STRATEGIC PROJECTS (EX. GOLDEN DOME)

Large, multi-layered national programs (e.g., the proposed “Golden Dome” missile-defense architecture explicitly predicate success on autonomous battle management and integrated, software-defined battle networks. Ambitious national programs of this scale create demand for autonomous BMC2 layers, persistent sensing, and high-assurance autonomy software.

Risks to Innovation and Adoption

Autonomy's runway is long, but it's not unconstrained. Several structural frictions could choke adoption unless addressed:

SUPPLY CHAIN FRAGILITY

Many autonomy enablers depend on rare earths and advanced components concentrated in a small number of suppliers. Geopolitical maneuvers and export controls over processed magnet and alloy components have raised acute worries about production continuity.

POLICY, PROCUREMENT AND BUDGET CONSTRAINTS

While program offices and offices of strategic capital are energizing fast-track buys, traditional congressional cycles and competing priorities create stop-start risk. There are bright spots – some GEOINT and NGA initiatives have successfully piloted AI and commercial imagery partnerships this year – but durable progress requires sustained policy alignment and budget authority that can support agile, iterative buys.

OPEN ARCHITECTURES AND STANDARDS

Open, modular architectures (plug-and-play payloads, common messaging and data models) accelerate integration and reduce vendor lock—yet cultural and contractual inertia often favor closed systems.

INTEGRATION COMPLEXITY AND CERTIFICATION

Military certification (safety, cyber, export control) and the complexity of integrating autonomy into legacy fleets slows fielding. Verification and validation tools, digital twins, and standardized testbeds reduce risk but require upfront investment.

INFRASTRUCTURE

Edge platforms, low-latency comms, and resilient networking fabrics are prerequisites. Without investment in hardened edge compute and mesh-like, contested-environment comms, autonomy will be constrained to permissive environments.

MANUFACTURING SCALE AND PRODUCTION

Scaling from prototypes to production requires industrial capacity and supply-chain diversification. Additive manufacturing and field-deployable printing reduce some pressure; however, traditional production scaling challenges remain and are capital-intensive.

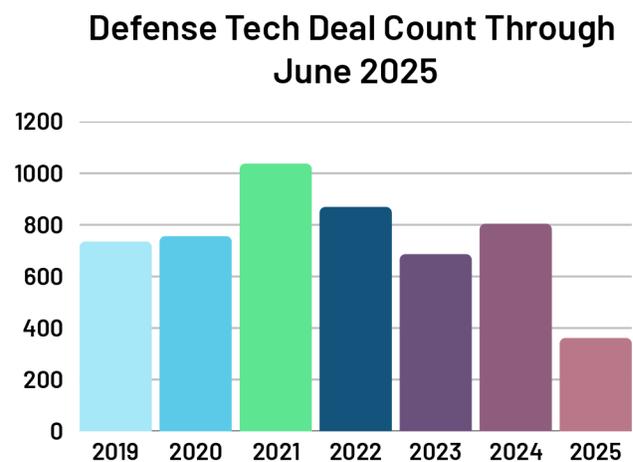
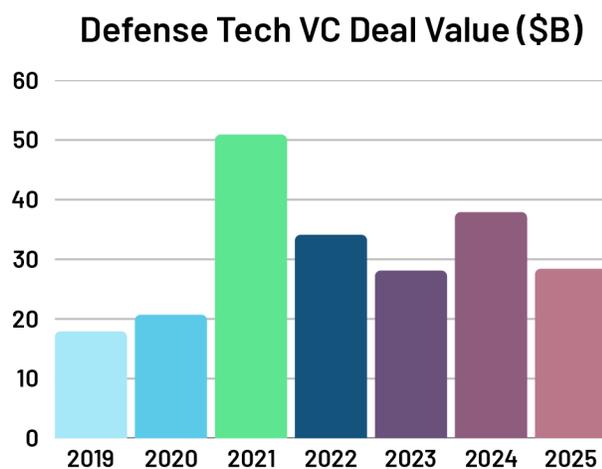
The Market

Investment in Defense Tech

2024 saw a noticeable uptick in venture capital interest in defense and dual-use technologies. Crunchbase reported roughly \$3.0B raised in VC-backed defense startups in 2024 (102 deals), up ~11% year-over-year. Industry trackers and ecosystem reports (SVDG / NatSec100, PitchBook) document continued momentum into 2025 as strategic and generalist investors increase exposure to national-security tech.

Investment in Autonomy

2024–mid-2025 has been notable for a series of very large, autonomy-adjacent raises (examples below). PitchBook and other venture trackers reported a surge in defense vertical funding in H1-Q2 2025 (quarterly records in some trackers), driven by megadeals for autonomous systems and AI/platform companies that serve defense needs. While datasets differ in scope and taxonomy, the signal is consistent: autonomy and autonomy-enabling layers are capturing outsized share of recent defense rounds.



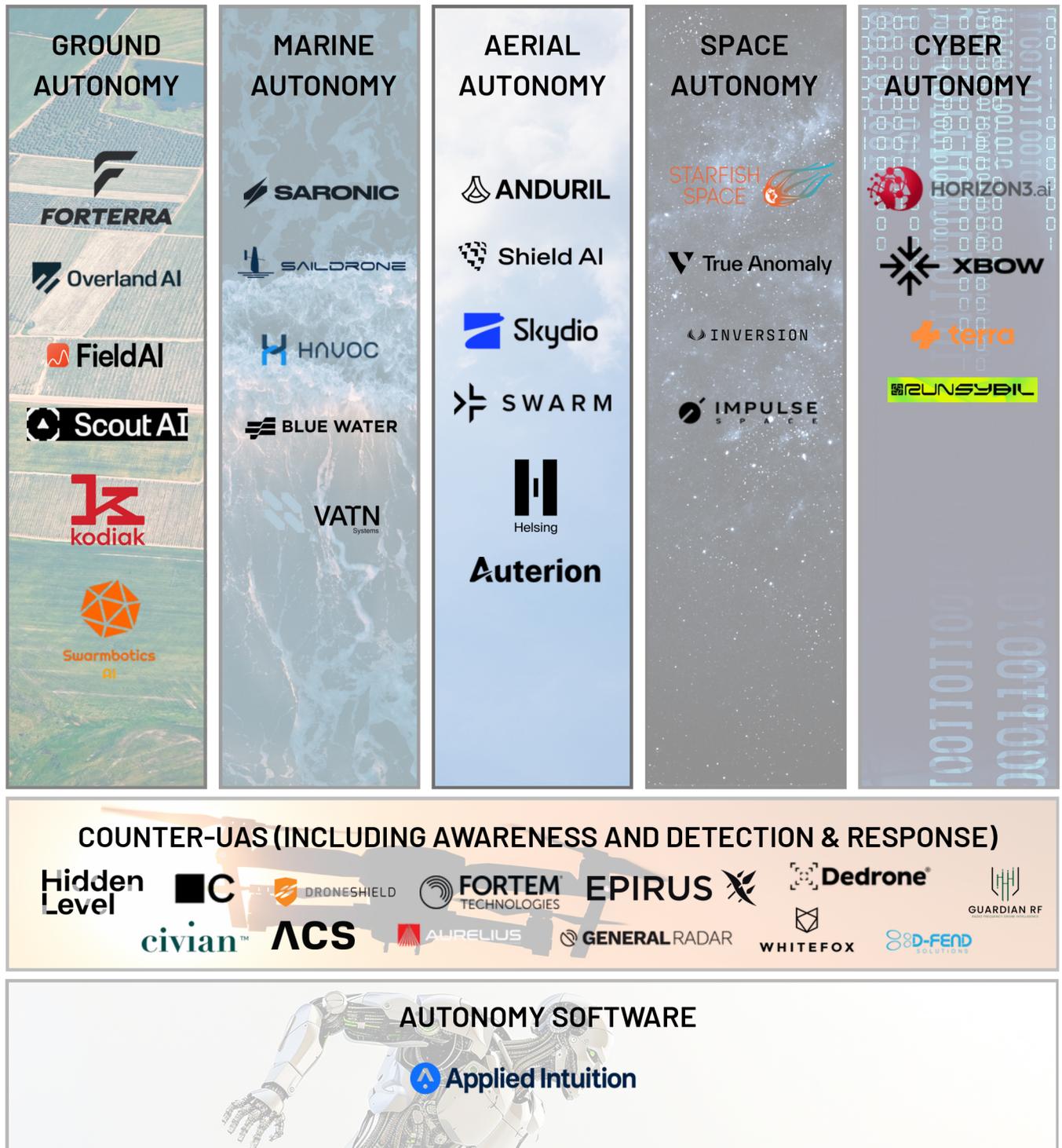
Top Investors

		ANDREESSEN HOROWITZ
 FOUNDERS FUND		
8VC		
		

Notable Rounds

 ANDURIL \$2.5B Series G (June 2025)	 ANDURIL \$1.5B Series F (August 2024)	 SARONIC \$600M Series C (Feb 2025)
 Helsing €450M/~\$487M Series C (July 2024)	 scale \$1.0B Series F (May 2024)	 EPIRUS \$250M Series D (March 2025)
 Shield AI \$240M F-1 Strategic Round (March 2025)	 Helsing €600M Follow-On (2025)	 Capella Space Acquired by IonQ (IONQ) (July 2025)

Market Map



Government Spending & Programmatic Demand

Autonomy, AI, and counter-UAS are explicit line items and priorities in recent Department of Defense budget materials and FY2025 submissions. The FY2025 Defense Budget Overview and associated materials call out investments in “AI & Autonomy,” unmanned systems, and counter-UAS capabilities across Services and Combatant Commands. These are being pursued both through traditional procurement and new, faster authorities and pilot programs.

Additionally, Congress and program offices have been active on counter-UAS authorities and oversight: the FY2025 NDAA and recent bills address counter-UAS funding and authorities, and in 2025 Congress introduced reauthorizations and reforms for counter-UAS authorities (e.g., H.R.5061). The CRS and other Congress-focused summaries document sustained attention and funding authorizations for counter-UAS and related autonomy programs.

Beyond the DoD, service and mission-owners are standing up specialized organizations (for example, the U.S. Coast Guard’s Program Executive Office for Robotics and Autonomous Systems) and accelerating task forces/centers to operationalize unmanned and autonomy capabilities. These institutional moves convert interest and R&D into real procurement pathways.

Q&A: Epirus CEO Andy Lowery

The rise of autonomy and robotic systems has ushered in what many call the “Sixth Domain” of warfare, where unmanned systems play a decisive role in shaping the battlefield. This shift has created urgent new requirements for counter-drone and counter-UAS technologies capable of addressing not just individual threats but coordinated swarms at scale. Epirus CEO Andy Lowery sat down with us to share how his organization is viewing the shift.



As the intersection of autonomy and robotic systems emerges as the Sixth Domain of warfare, how has this shift changed the urgency and requirements for counter-drone and counter-UAS technologies?

The emergence of the Sixth Domain has accelerated the need for counter-UAS systems that are scalable, rapidly adaptable, and capable of defeating swarms. Epirus’ Leonidas High-Power Microwave Platform answers this urgency with a software-defined, one-to-many defense that outpaces autonomous, robotic, asymmetric threats and delivers operational relevance today. Leonidas uses electromagnetic interference to overwhelm a drone’s internal components, making the technology effective against autonomous swarms or fiber-optically guided drones where traditional electronic warfare and kinetic capabilities fall short.

Epirus is pioneering a new approach to directed energy with Leonidas to address drone swarms. What differentiates your weaponized electromagnetic interference capability to more traditional directed energy systems, and why do you believe it’s the right solution for the evolving threat landscape compared to kinetics or lasers or other possible solutions?

Leonidas takes a fundamentally different approach to directed energy by using longer pulses, delivering magnitudes more energy, and relies on weaponized electromagnetic interference instead of on extreme peak power or destructive burn-through. This allows us to deliver precise, scalable, and repeatable effects against entire swarms at once, with no shrapnel, no depletion of interceptors, and minimal collateral risk. Unlike kinetic or laser systems that are costly and limited to one-to-one engagements, Leonidas is a software-defined, one-to-many solution built

for the speed and scale of today's autonomous and ever-evolving electronic threats, making it a needed component for any layered defense in today's evolving battlespace.

We've seen in Ukraine, Israel, and the Red Sea how drones are changing combat in real time. What lessons is Epirus taking from these conflicts?

Ukraine's Operation Spider's Web and Israel's Operation Rising Lion show that cheap, distributed drone campaigns can be coordinated to overwhelm and penetrate air defenses, raising the operational urgency for drone countermeasures. For example, Ukraine claims that about 34% of Russia's strategic cruise missile-carrying bomber fleet were damaged or destroyed in Spider's Web, while in Iran, air defenses and radar batteries were degraded from Israeli drone saturation attack. Houthi attacks in the Red Sea demonstrate the same logic at sea, where commercial and military assets face saturation tactics that traditional interceptors cannot sustain. Epirus' lesson is clear: to "defend the defenders" from drone attack, you need a layered counter-drone defense, focused on one-to-many, software-defined, and scalable systems like Leonidas' weaponized electromagnetic interference, which has an unlimited magazine to neutralize swarms without the cost, magazine-depth concerns, and collateral risk of kinetic interceptors.

How are your customers – whether in the U.S. military, allied governments, or critical infrastructure operators – experiencing the shift to autonomy and drone proliferation?

Customers are already experiencing the shift to autonomy and drone proliferation in tangible ways. At Joint Base Langley-Eustis, drones flew overhead for 17 consecutive nights in December 2023, underscoring the vulnerability of even high-value installations. Across the homeland, the FAA recorded 411 illegal drone flights near U.S. airports in Q1 2025, while U.S. officials report over 1,000 cartel-operated drones crossing the southern border each month. The trends demand counter-drone approach that features proven, one-to-many defenses like Epirus' Leonidas.

Looking five years out, how do you see the autonomy landscape evolving, and what do you see as the greatest opportunities for Epirus? What role will partnerships with government, industry, and investors play in getting there?

As drones adopt onboard autonomy at the edge, traditional counter drone capabilities like electronic warfare jamming lose relevance because there's no external link to disrupt, and serial one-to-one defenses cannot keep pace with massed, coordinated swarms. Epirus built Leonidas for this new reality, enabling one operator to command multiple HPM systems through human-machine teaming to deliver scalable, software-defined counter-swarm effects. Partnerships with government, industry, and investors will be essential to accelerate this shift from concept to fielded capability.

NightDragon Perspective

At NightDragon, we believe the rise of autonomy as the “Sixth Domain” is not a fleeting trend, but a generational shift in defense and security. The pace of conflict in Ukraine, the Red Sea, and the Indo-Pacific makes clear that autonomy is no longer optional – it is foundational to how modern militaries will operate. Just as cyber became a defining domain of warfare over the past two decades, autonomy is now driving a wholesale rethinking of force structure, strategy, and technology. This moment represents both a national security imperative and a historic market opportunity.

Our conviction in this sector is reinforced by what we see across the capital landscape. Record-breaking venture capital rounds for companies like Anduril, Shield AI, and Helsing demonstrate that private capital is increasingly willing to fund dual-use technologies once considered outside the traditional bounds of VC. At the same time, the U.S. federal government is putting real dollars behind this transition: autonomy, counter-UAS, and unmanned systems are explicit priorities in the FY2025 DoD budget, and Congress has moved to reauthorize and expand counter-UAS authorities. This convergence of public and private capital is accelerating adoption and creating a durable foundation for growth.

NightDragon is proud to be an active investor in this domain (with more to come). Our portfolio companies Epirus, Saronic, and Horizon3.ai are emblematic of the type of innovation needed to meet today’s threats. Epirus is pioneering directed energy systems to neutralize drone swarms at scale, while Saronic is building a first-of-its-kind autonomous shipyard to deliver uncrewed surface vessels to the U.S. Navy and allied partners. Horizon3.ai meanwhile offers an autonomous cybersecurity platform. Beyond autonomy itself, we are also actively evaluating opportunities in adjacent enablers – from advanced manufacturing platforms that can help the U.S. scale production at speed, to cutting-edge hypersonic systems that will redefine the offense-defense balance in the years ahead. These areas complement our autonomy thesis and highlight the breadth of innovation we believe is required.

Looking forward, we are deeply optimistic. The innovation occurring across autonomy in the

air, sea, land, space, and cyber domains is not only transforming warfare, but also creating dual-use applications that will spill over into critical infrastructure, logistics, and commercial markets. With entrepreneurs pushing the boundaries of what's possible and investors stepping up to back them, we believe the autonomy market is on the cusp of a new era of scale. NightDragon is committed to fueling this movement – partnering with innovators, government, and industry to ensure the Sixth Domain becomes a source of enduring advantage for the United States and its allies.

Contact

If you're building interesting technology in this sector or have a perspective, reach out to:



Morgan Kyauk
Managing Director, NightDragon
morgan@nightdragon.com



Hannah Huffman
Vice President, NightDragon
hannah@nightdragon.com



NIGHTDRAGON