SPONSORED POST, NETWORKS & DIGITAL WARFARE

America must adopt a Sixth Domain of warfare doctrine

The Sixth Domain is not defined by geography. It's a new kind of conflict in which autonomy and networked systems allow thousand-dollar consumer electronics to destroy multi-million-dollar conventional weapons systems.

By Epirus on March 24, 2026 2:38 pm Share

presented by EPIRUS

Image courtesy of Epirus.

Over the past 15 years, America's military services and foremost military thinkers have recognized that modern domains of warfare have expanded — from land, sea and air — to space and the virtual realm of cyber. As valuable as this expanded concept of warfighting is, it is no longer enough.

The past 12 months of global armed conflicts have demonstrated clearly that America must adopt a new Sixth Domain way of thinking if it is to successfully defend itself and its interests in the immediate and long-term future.

The Sixth Domain is not defined by geography. It's a new kind of conflict in which autonomy and networked systems allow thousand-dollar consumer electronics to destroy multi-million-dollar conventional weapons systems. Defenses built for one-to-one conflict are ineffective in The Sixth Domain.

The fundamental asymmetry of this new domain requires more than innovative technology. It demands national security expertise that moves at Silicon Valley speed and technology based in hardware and defined by software, rapidly updated with code that can scale and evolve as fast as any threat. Neo-Primes like Epirus that fuse the industry

know-how of defense behemoths with the venture capital funding, corporate agility and rapid system iteration of Silicon Valley, are built specifically for this new type of warfare.

The need to focus on The Sixth Domain was vividly illustrated on June 1, 2025, Russia's Military Transport Aviation Day, a significant holiday for Russian armed forces. In an operation codenamed Spider's Web, the Security Service of Ukraine carried out an unprecedented, coordinated drone strike deep inside Russian territory. The operation targeted four strategic air bases and struck more than 40 high-value aircraft, a major portion of Moscow's long-range bomber fleet representing 34 percent of Russia's strategic cruise missile delivery platforms.

Over 150 small strike drones smuggled into Russia simply bypassed the country's air defenses. Directed by a combination of remote human control with elements of autonomy and AI-assisted functionality, the stunning attack manifested what Epirus CEO Andy Lowery calls "physical cyber," a new asymmetric threat that resembles a cyberattack turned physical that completely caught Russia off-guard. Much like a malicious software overwhelming IT systems during a DDOS cyber-attack, robotic and autonomous Sixth Domain threats swarm and over saturate physical defense systems that are built for linear one-to-one engagements and are ill-prepared to combat asymmetric attacks.

Epirus, the maker of a high-power microwave (HPM) defense platform called Leonidas, is a company built to address the challenge of modern asymmetric warfare, and a leader in conceptualizing The Sixth Domain. Since the company's foundation in 2018, the Epirus team has recognized the potential of combining land, sea and aerial drones with autonomy and novel tactics and strategy.

Even prior to Spider's Web, Israel's Rising and Roaring Lion drone exploits and the drone-heavy Iranian response to Operation Epic Fury, Lowery regularly discussed the core tenet of The Sixth Domain — the threat of asymmetric, robotic, and growingly autonomous systems that light up night skies, bolt over land, skim across seas and relay targeting data from space-based assets — with U.S. military and government personnel. "It dominates most every conversation I have," Lowery confides.

What keeps Lowery, and many national security professionals, awake at night is the specter of saturated swarm attacks on the U.S. homeland. A drone attack on the homeland is well within the realm of the possible, he explains.

Spider's Web, Rising Lion and the ongoing war in the Middle East cast an ominous spotlight on the definitive role of drones in modern conflict. It's imperative that the Department of War builds out our counter-UAS arsenal to stay ahead of the evolving threat environment — before it's too late. A mass-scale drone attack on U.S. soil must not be the catalyst for change when proven, combat-ready counter-UAS capabilities exist today.

Combatting Sixth Domain threats requires a new mentality, a new approach and new organizational infrastructure.

The One-to-Many Imperative

The Sixth Domain is an evolving battlespace, not defined by geography, but new technologies and their effects and, in turn, new tactics, techniques and procedures employed by military strategists. It posits massed, robotic, asymmetric and progressively more autonomous attacks across all domains, similar to cyber attacks that oversaturate and overwhelm virtual defenses. Exploits in The Sixth Domain, however, are also kinetic. They are akin to the "physical cyber attack" Lowery describes.

Current defense systems aren't built to defend against saturating physical cyber. These legacy one-to-one defenses lack sufficient magazine depth, command-control capability and economies of scale to cope with the mass, speed and complexity of Sixth Domain attacks.

Consider that China annually produces millions of aerial drones — the world's majority in 2025 — with leading companies like DJI accounting for nearly 70% of the global commercial and recreational drone market. The country's commercial and military drone sector is projected to exceed $11 billion in value by the end of 2025.

China sells tactical UAS to the Middle East, Pakistan, Africa and Asia. It also supports Russia's war effort in Ukraine, supplying Russia with critical components to increase its drone output. In 2024, Russia boosted its long-range UAS production from 15,000 to over 30,000, alongside 2 million small tactical drones. What's more, the Iranians are able to produce thousands of Shahed 131/136 UAS monthly.

Recommended

New joint intel report warns of cyber threats to growing LEO satellite constellations

Ocean Aero Triton's Minesweepers are ready now

What new weapons could a supplemental buy, plus news on the Army's C5ISR plans

Turned against vulnerable targets, a small fraction of these global totals are sufficient to overwhelm the few defensive systems now in place domestically. The numbers don't count the rapidly expanding land and sea drone populations.

The asymmetry challenge presented to the West by massed aerial drones has been obvious to professional and public observers. In September, Denmark and Norway were forced to close their main airports due to suspected Russian drone sightings, impacting approximately 20,000 airline passengers. In October, Germany's Munich airport shut down twice in response to unidentified drone sightings, impacting around 10,000 passengers.

Across the broader Middle East, cheap drones have already forced the temporary shutdown of one of the world's largest U.S. embassies in Baghdad, with strikes hitting inside the compound. In the opening days following Operation Epic Fury, Iranian one-way attack drones destroyed at least one U.S. THAAD AN/TPY-2 radar in Jordan and badly damaged other long-range sensors in Qatar and the Gulf, blinding portions of the regional missile-defense network at the cost of a few relatively cheap munitions.

These waves of drone attacks come during a time with thousands of confirmed FPV drones, including fiber-optic drones, being used by Mexican cartels, a cross-border threat that will be hard to blunt from both an asymmetry and electronic warfare perspective.

Epirus asserts that defeating asymmetric Sixth Domain threats requires a "one-to-many" technical, tactical, and strategic response. This includes wide-area defense architectures composed of layered systems-of-systems, enabled by human–machine teaming. Last year, Epirus' CEO publicly highlighted the potential dominance of "centaur warfare" where machines handle speed and decision complexity while humans provide strategic and ethical oversight. Blending the strengths of AI and human judgment to meet the demands of distributed warfare is core to The Sixth Domain Doctrine, penned by Epirus.

Networked, autonomous, robotic attacks present a tall challenge but one-to-many defensive systems can overcome it. Epirus' Leonidas platform is designed to knock down drone swarms using HPM energy at a variety of ranges. Its one-to-many capability has often been described as "directed energy" but it is more accurately characterized as Electromagnetic Interference (EMI). If high-power microwave is the *what* behind Leonidas, electromagnetic interference is the *how*: a software-defined, one-to-many method of neutralizing swarms by disabling their internal components via targeted pulses of high-density electromagnetic energy without relying on destructive peak power to physically destroy systems.

Leonidas leverages EMI by transmitting relatively long-pulses of microwave energy across tailorable frequency bands, which overloads the electrical systems of drones that fly into the electromagnetic field it creates. The one-to-many defensive effect it produces is central to defeating swarm attacks, capitalizing on a deep electromagnetic magazine and low cost-per-shot character.

Systems like Leonidas, which impart their own asymmetry, will be critical to defeating electronic saturation attacks. The Sixth Domain Doctrine requires fielding and connecting them, developing architectures that embrace modular, scalable design and fast-reconfiguring software. The new era will require urgency, rapid software-defined development cycles, user-driven design, and continuous operator feedback loops.

The fact that America's contemporary military and defense acquisition organization has thus far proven unable to internalize these imperatives and execute on them has convinced Epirus that The Sixth Domain requires more than incremental change.

"It will require the establishment of an entirely new military service branch, or at least program offices like the new JIATF-401 and PAE Robotic and Autonomous systems, built for this battlespace from the ground up," Lowery affirms.

Epirus is not alone in recognizing the potential of an entirely new service branch focused on autonomous, asymmetric warfare. Calls for creation of a new standalone cyber service have grown in recent years.

The U.S. Navy was first to move in this direction with their announced initial operating capability of a new Portfolio Acquisition Executive for Robotic and Autonomous Systems (PAE RAS), a key component of the Service's Force Design 2028 plan. The PAE RAS is expected to accelerate the development, acquisition, fielding and sustainment of capabilities to address Sixth Domain threats including counter-UAS.

Next-Generation Defense Firms & Acquisition for The Sixth Domain

A new generation of defense companies built around user-centered product design, not merely services contracts and sustainment, will dominate The Sixth Domain.

Emerging Neo-Primes, which anticipate threats and prototype ahead of formal requirements by embedding with warfighters, can succeed with a user-centered, product-focused mission. They respond to capabilities demand rather than programmatic demand, prioritizing rapid and continuous delivery of new, relevant hardware and software to the field over meeting program requirements.

A concurrent shift in government acquisition culture will be necessary to meet The Sixth Domain challenge as well. Epirus proposes reorientation toward capability-demand acquisition, informed directly by warfighter experience.

This approach would see an acquisition model that mirrors special operations development wherein program executive offices merge personnel with warfighters to gain instant feedback and personal experience in the trial and fielding of new capabilities. Embedding Neo-Prime personnel in this loop will foster agile, iterative capability development, provided continuously — a model America leveraged with success to win WWII.

Though The Sixth Domain will require a new kind of industrial base, a new government acquisition and military service approach, Epirus believes legacy platforms and legacy primes remain vital to national defense, deterrence and future warfare.

"While the rise of Neo-Primes like Epirus are transforming defense, traditional contractors remain essential as neutral systems integrators, global-scale partners for production and sustainment, and developers of the exquisite legacy platforms that underpin deterrence and force projection," Lowery reminds. "Their continued success and willingness to embrace partnerships with Neo-Primes is vital to the health of the defense industrial base and the success of the U.S. in The Sixth Domain."

Many of Epirus' proposed reforms laid out in The Sixth Domain Doctrine are included in War Secretary Pete Hegseth's newly introduced Warfighting Acquisition System, which signals an embrace of wartime urgency, a prioritization of accountability and speed to capability delivery, and the demolition of bureaucratic barriers that delay the procurement process.

"An 85 percent solution in the hands of our armed forces today is infinitely better than an unachievable 100 percent solution endlessly undergoing testing or awaiting additional technological development," said Hegseth.

What's at risk if America does not adopt The Sixth Domain Doctrine?

With defense acquisition policy increasingly driven by budget considerations rather than military capability imperatives, many may question the cost of recognizing The Sixth Domain and adopting both a new doctrine and infrastructure to prevail in it.

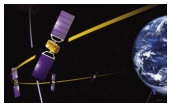
But a more important question cannot be ignored: What's at risk if America does not adopt The Sixth Domain Doctrine?

"Everything," Andy Lowery says. "Western democracy. Our very way of life. You name it. Losing this race for dominance in The Sixth Domain would be equivalent to the Axis powers beating us to an atomic bomb. It's that fundamental to the future of the geopolitical landscape."

Lowery's closing comments, though characteristically more colorful, mimic recent statements by Army Secretary Dan Driscoll who has called drones "the threat of humanity's lifetime." In Lowery and Epirus' mind, the Secretary is spot on.

Topics: cyber security, Drones, Epirus, Epirus March, high power microwave weapons, Navy, networks, Presented by Epirus, Sponsored Content, technology

More from Breaking Defense



New joint intel report warns of cyber threats to growing LEO

'Too early to tell' if timeline holds for delivery of Army's tilt-

Requirements without factories: Why the Pentagon must

Army's digital marketplace for drones is officially open

satellite constellations

rotor MV-75 for testing: Official

reconnect design to production

Sign up and get the latest news in your inbox.

Enter your email address

Subscribe Now

We will never sell or share your information without your consent. See our privacy policy.