CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Overview: Trendlines *synthesizes research from across CSIS programs to identify the structural trends and new forces shaping the global economy and geopolitical landscape. Each edition distills research from across CSIS into key signals for policymakers, industry leaders and strategic decisionmakers.*

Issue 3 | New Front Lines | May 2026

A new era of warfare has arrived, and it is rewriting the rules of strategic advantage. Lessons from active conflicts around the world point to three structural shifts: (1) who can produce and replenish at scale, (2) what counts as a target in the modern era, and (3) where are wars set to be fought in future, from cyberspace to outer space. Each factor carries direct implications for logistics, legislation, and long-term policy planning.

The Data:

2 years

The record time it took Ukraine to scale drone production from approximately 800,000 to 5 million unmanned aerial vehicles annually from 2023 to 2025

400%

The percentage increase NATO's secretary general called for in European air and missile defense spending in 2025

>50% vs. 0.1%

China's share of global shipbuilding versus the United States in 2023. One Chinese shipyard alone exceeds the combined annual output of every U.S. shipyard

200,000+

Corporate devices across 79 countries reset simultaneously on March 12, 2026, in a single Iranian cyberattack on medical device manufacturers

$40B/yr

The U.S. Congressional Budget Office projected estimate of the annual cost for the Navy's shipbuilding plan through to 2054

4

Years' worth of key U.S. precision munitions used up after 39 days of the air and missile campaign against Iran in 2026

The Trends:

Trend 1: The New Industrial Contest

Photo: dsheremeta/Adobe Stock

Military advantage is no longer defined solely by the most sophisticated weapons, but also increasingly by the ability to produce, replace, and scale systems rapidly. Warfare has always been a manufacturing and supply chain story as much as a battlefield story.

“Technology is important, but it has never been sufficient to win wars.”

—Seth G. Jones, CSIS

The Trendline: Cheap weapons systems are becoming more effective, and the speed of their development is accelerating. This trend towards high-volume, low-cost systems introduces new players and a new economic calculus to defense planning, procurement, and production. This shift gained greater international attention after Russia launched its invasion of Ukraine in 2022. War and the Modern Battlefield documents that four years ago, Ukraine was expending a month's worth of U.S.-produced 155 millimeter artillery in a single day. Since then, Ukraine restructured its entire acquisition system, and by 2024, commercial technology accounted for nearly half of its defense procurement spending. The result has been a new paradigm in asymmetric warfare: Cheap drones destroyed strategic bombers worth billions of dollars. Russia was quick to adopt this strategy, launching more than 50,000 Shahed-type drones throughout 2025, five times the prior year's rate. The production model—overwhelm through volume and cost—is catching on in new contested spaces in the Gulf and Levant.

What It Means: The production gap is now as strategically significant as any capability gap. "The Next Offset: Winning the Fight Before It Starts" argues that the United States is not adequately prepared for the future nature of warfare, its defense industrial base is not suitably provisioned for a protracted conflict, and that developing an offset to China's advantages in scale and speed is among the most urgent priorities. In today's era, "production is deterrence." Investments in capacity and rapid technical refresh are not just a defense priority but a signal to adversaries of an ability to sustain conflict.

Trend 2: "Dueling"-Use Technology and the Expanding Target Set

Photo: Gallo Images/"USGS/NASA Landsat data processed by Orbital Horizon"

Modern adversaries have concluded that striking the systems that economies run on is as effective as engaging armies directly. The targets in recent conflicts, such as dams, data centers, shipping lanes, undersea cables, and tourism infrastructure, are not incidental to military strategy. They are the strategy. Cyber advancements have made it even easier: The same digital connectivity that makes modern infrastructure efficient also makes it increasingly vulnerable to attack.

"The partnership between the military and tech will only grow [Iran has recognized this trend and is] . . . targeting energy infrastructure and now data. The lines are more than blurred: There are no front lines anymore."

—Emily Harding, CSIS

The Trendline: When critical infrastructure is hit, the second and third order impacts flow downstream. Russia's destruction of Ukraine's Kakhovka Dam in June 2023 eliminated one of the most extensive irrigation systems in Europe. In the Red Sea, Houthi attacks on commercial shipping cut average daily Suez Canal transits from 80 to 29, doubled container costs within a month, and contributed 0.7 percentage points to global core goods inflation in the first half of 2024. In one February 2024 attack, a single Houthi missile strike caused a ship's anchor to sever three Red Sea undersea internet cables, disrupting data flows across the region. In 2026, Iran struck Amazon Web Services (AWS) data centers in the UAE and Bahrain, disrupting banking and consumer services across the region. All of these incidents highlight the emerging dual-use nature of the infrastructure: The same cloud platforms, financial messaging systems, and communications networks that underpin global commerce are the systems adversaries are pre-positioning to disrupt.

What It Means: The boundary between a corporate risk problem and a national security problem is blurring. "Economic Warfare and Military Power," articulates the overlapping dimensions of a new diplomatic, information, military, and economic power framework. Private U.S. companies are now on the frontlines of conflict. Adversaries have developed a distinct approach to targeting civilian infrastructure as a coercive instrument. This bolsters the need for both increased security measures —especially in the cyber domain—and robust business continuity practices for quicker recoveries. For more on this pattern, check out CSIS's Significant Cyber Incidents tracker, which has been updated continuously since 2006.

Trend 3: War Enters the Final Frontier

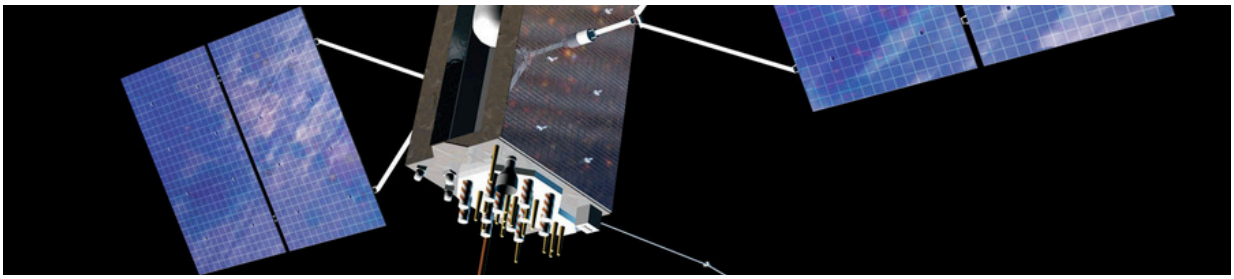

Photo: SMC/GP/U.S. Air Force

War has entered the final frontier, and not metaphorically. Space and cyberspace are now active theaters of conflict, and the assets being targeted and weaponized are overwhelmingly commercial in origin. Lower barriers to entry in low Earth orbit mean that today, nearly any actor that once lacked space capability can now purchase it commercially or build sovereign capability at scale while simultaneously developing tools with the potential to deny that access to others.

"These modern conflicts are normalizing the idea that space . . . like land, sea, air, and cyber . . . is a domain to be exploited, attacked, and defended in wartime."

—Kari A. Bingen, CSIS

The Trendline: The high barriers to entry that once made space and cyberspace the exclusive domain of a few powers, are quickly coming down and introducing new actors and risks. "Extending the Battlespace to Space" documents how Ukraine entered the war with almost no sovereign space infrastructure and immediately mobilized commercial providers: Starlink for command and control; Maxar imagery to track a 40-mile Russian convoy toward Kyiv; and ICEYE radar satellites to image enemy positions through cloud cover at night. The same capability was commercially available to the other side: Russia's Wagner Group purchased satellite imagery from Chinese firms Spacety and HEAD Aerospace, prompting U.S. Treasury sanctions in January 2023. Any actor without sovereign space capability can simply purchase it.

The cyber terrain is evolving in parallel. A Congressional testimony in January 2026 highlighted current deterrence gaps. While the United States has built powerful offensive capabilities through the U.S. Cyber Command, adversaries still too easily control the escalation ladder. Outer space and cyber space are also converging: GPS jamming and spoofing is already affecting systems far outside any military theater. In 2024, Chinese hackers gained access to a U.S. utility's operational technology network for close to a year, not to cause immediate disruption, but to map it for future use. The implication across both domains is the same: adversaries are not preparing for a conflict. They are already inside the infrastructure, waiting.

What It Means: Governments and the private sector are now active partners in space and cyberspace, making those shared assets targets for broader geopolitical conflict. The Space Threat Assessment is one of the most comprehensive open-source records of how counter space weapons are developing. It documents both capabilities and the pace at which adversaries are normalizing their use against the commercial constellations that underpin global logistics, finance, and communications. This trend raises serious new questions about the governments' obligations to the private sector operators in space and cyberspace as these theaters quickly become threat environments. The Commission on U.S. cyber force generation has recently laid out a roadmap addressing the structural, operational, and workforce challenges facing the current cyber ecosystem, including talent shortages, fragmented authorities, and barriers to readiness.

The Trajectory

What connects all three trends is a narrowing gap between military and commercial risk. Over 80 percent of U.S. critical infrastructure is privately owned and operated. The weapons being built run on commercial chips. The targets being struck are commercial infrastructure. The terrains being contested are the same systems the global economy depends on daily including food systems, financial institutions, and communication infrastructure.

Just this week, the Pentagon requested $54 billion to accelerate its autonomous drone warfare program. Speed of adoption and adaptation has become the name of the game in an era of low-cost, high-impact weapons systems. An ability to reimagine and redefine a fit for purpose defense enterprise will likely be the defining organizational challenge in coming decades.

For more information, please reach out to Joyce Bongongo at JBongongo@csis.org or Grace Dereemer at GDereemer@csis.org.