OFFSET-X EVOLVED

SEPTEMBER 2025

SPECIAL COMPETITIVE STUDIES PROJECT

OFFSET-X EVOLVED

SEPTEMBER 2025

SPECIAL COMPETITIVE STUDIES PROJECT

The Special Competitive Studies Project is a bipartisan, non-profit project with a clear mission: to make recommendations to strengthen America's long-term competitiveness as artificial intelligence (AI) and other emerging technologies are reshaping our national security, economy, and society. We want to ensure that America is positioned and organized to win the techno-economic competition between now and 2030, the critical window for shaping the future.

Offset-X Evolved (Offset X^{e}) reflects a continuum of Defense Panel activities conducted since the release of Offset-X in 2022 and the evolution of warfare, technology, and the global security environment that demand urgency and decisiveness.

SCSP Leadership

Dr. Eric Schmidt
Chair

Ylli Bajraktari
President

Board of Advisors

Dr. Nadia Schadlow

William "Mac" Thornberry

Robert O. Work

Michele Flournoy

Authors

Dr. Paul Lyons
Senior Director

James Ryseff
Director

Luke Vannurden
Director

Kian Molani
Associate Director

Dennis Mayes
Air Force Fellow

Abigail Cleveland
Fellow

Jaehyoung Ju
Research Assistant

Ylber Bajraktari
Vice President, Policy

Senior Advisors

Ms. Christine Fox

LtGen (ret) Michael Groen

The Honorable James Langevin

RADM (ret) Mark Montgomery

Dr. Andrew Moore

Mr. Michael Brown

Mr. Mircea Geoana

Lt. Gen. (ret) Jack Shanahan

Lt. Gen. (ret) Clint Hinote

MG (ret) Mick Ryan, Australian Army

The Honorable Ely Ratner

This report benefited greatly from insights from more than one hundred experts, to whom we are deeply grateful. It aims to reflect many, though not all, of those insights. It was prepared by the SCSP staff and, as such, is not a consensus document of all the experts who assisted.

Contents

A Letter from the Chair & the President

In one of our first reports in 2019, when we led the Congressionally-mandated National Security Commission on Artificial Intelligence (AI), we forewarned that the convergence of AI revolution and the re-emergence of great power competition would fundamentally test the military superiority of the United States. By 2022, the Russian invasion of Ukraine and the release of chatGPT underscored this new reality. The emergence of new technologies—under the shadow of great power clashes—combined with operational concepts that harness them in innovative ways was ushering new ways to apply military force. The character of war was fundamentally changing and if the United States were to go to war this decade, it would likely face a new kind of warfare.

In response to this new reality, in one of our first reports after establishing the Special Competitive Studies Project in 2021, we proposed a new approach—an Offset-X strategy. This competitive strategy, we argued, would seek to restore America's military-technological superiority for this new era, and in the process undermine our adversaries' considerable military advancements and thwart their theories of victory. The principal recommendations of this competitive strategy were for the U.S. military to (1) fully embrace distributed, network-based operations; (2) lead in human-machine teaming; (3) gain and maintain software advantage; and (4) ensure resilience in sensing, communicating, attacking, and supplying.

In the years since then, the criticality of these four pillars—distributed operations, autonomy, software, and resilience—has been validated. But the global security environment has deteriorated further—tilting away from competition and rivalry towards confrontation. China, Russia, Iran, and North Korea have coalesced around a new Axis of Disruptors—intent on waging an active and often coordinated campaign of confrontation and coercion against the United States and its allies. And as geopolitics have deteriorated, technological advances—particularly in AI—have accelerated. Few doubt anymore that the Age of AI is here—the only questions that remain are what are its limits and its full implications, and whose values will shape it.

Mindful of these dynamics, and the dangers associated with this decade, we decided to revisit and evolve the original Offset-X strategy. Countless visits to Ukrainian frontlines, repeated engagements with Taiwanese officials, a series of novel table top exercises with technologists and military planners, four summits on innovation and national security with senior most defense leaders of the United States, and insights from more than one hundred officials from

government, industry, private capital, allies, and academia fed into the revisions to our original Offset-X report. The shared sentiments were clear:

- The future of warfare is not coming in five or ten years. It is already here, unfolding most obviously and daily in the battlefields of Ukraine, as well as across the digital domain. And allied militaries are not ready for this type of warfare. Our defense institutions and processes are slow to adapt, our defense procurement remains overly invested in current capabilities, and our hard-earned lessons from Iraq and Afghanistan are quickly losing relevance.

- In today's warfare, there is no place to hide. With ubiquitous sensors and pervasive signals intelligence, surprise attacks and amassing of forces are becoming incredibly difficult. You cannot hide aircraft carriers, runways or hangars with airplanes, or columns of tanks. Furthermore, cognitive warfare can reach anyone—from national leaders to military commanders to teens scrolling through short reels online. This transparency paradoxically raises the risk of preemption while favoring defense.

- The fastest learner, iterator, and adaptor wins. The military overmatch in today's warfare is the velocity of adaptation. The force that can learn and iterate on its capabilities and tactics overnight will crush the side that is stuck in a multi-year procurement cycle.

- We are witnessing the dawn of automated warfare. The paradigm of a human in a machine is breaking down. We are moving from a war with machines to a war of machines. Drones and the ecosystem that produces them are becoming the most important weapon on the battlefield and a true measure of one's strategic depth.

- Software is the new high ground. Information, decision, and lethality advantage now depend on the quality of software that powers them. The militaries with platforms and capabilities whose operating systems—along with their tactics—can be updated in near real time will edge those with rigid hardware.

- In this type of warfare, decision superiority can only be achieved with the help of AI. Since the 1950s, the OODA loop framework—Observe, Orient, Decide, Act—has guided military decisionmaking. But that loop is now collapsing from human speed to machine speed. No human or group of humans can absorb all the analysis, much less all the information they have access to. No military leader, no matter how battlehardened, can plan and conduct a global battle with a million drones and other assets under his command. At the warfighter level, AI-powered software is the only way to bypass human cognitive limitations to process the massive amounts of incoming data and orchestrate all military assets. More importantly, AI will find patterns that humans cannot detect, giving us the critical early warnings we need to act first. And AI may identify new vectors of attack that may initially appear counterintuitive

to military leaders, but end up being tactically and operationally decisive.

- The commercial tech ecosystem is the new strategic depth for this form of warfare. The most advanced technologies no longer come out of government labs; they come from the commercial sector. Moreover, many of the technological innovations no longer bestow lengthy or enduring advantages; they require continuous iterating, updating, and adapting. In this new reality, militaries should avoid trying to build most of their capabilities themselves and get much better at orchestrating and integrating innovation from the outside.

In decades past, and in response to similar, existential geopolitical challenges and rapid technological advances, the U.S. military adopted a series of successive concepts—Air-Land Battle, Air-Sea Battle, Full Spectrum Dominance, Network-centric Warfare, Multidomain Operations, and others. We believe that the time has come for a new concept that stands on a triad of three core capabilities—**sensors**, **artificial intelligence**, and **autonomy**. If fully incorporated and mastered, they provide three advantages essential to the future of warfare—informational, decisional, and lethality advantage.

Mastering this triad isn't just an upgrade; it's a paradigm shift. It is about creating a single, integrated, and largely automated warfighting system that functions like a living organism. The proliferated sensing layer acts as the system of receptors and nerves, constantly observing the environment and feeding a torrent of data to the AI brain. This cognitive layer then processes that information at machine speed, bypassing human limitations to find patterns and identify opportunities in seconds, not hours. It then directs the muscles—swarms of low-cost machines—to execute complex missions with speed and precision. This creates a self-reinforcing loop of sensing, learning, adapting, and acting that operates at a tempo no human-centric adversary can possibly match.

We hope that the analysis and the recommendations we present here will be informative to policymakers, commanders, entrepreneurs, and allied partners alike. As in years past, the Special Competitive Studies Project stands ready to assist them—so that the destinies of free nations remain secure, prosperous, and self-determined.

Eric Schmidt
Chair, SCSP

Ylli Bajraktari
President and CEO, SCSP

Executive Summary

The United States faces transformative change across strategic, technological, and warfare realms. The era of Great Power competition is giving way to an era of confrontation, with a new axis of disruptors—China, Russia, Iran, and North Korea—waging a relentless campaign against U.S. interests, America's leadership position, and the vision of free nations as the destiny of humankind. In the realm of technology, the age of AI is here with direct implications not only for our economy, education, health, and society, but also national security and warfare. The United States ushered in the age of AI and continues to be at the forefront of innovation, but the race for the final frontiers of AI and values that will govern it remain a fulcrum of competition. And when it comes to war, we are witnessing the dawn of automated wars. Informational, decisional, and lethal advantage are increasingly being powered by and dependent upon algorithmic and autonomous systems. This is not just the promise of technology, it is the battlefield dynamics that are necessitating it.

Each of these three drivers of change are transformational in their own right. And while not all three are transpiring along identical timelines, their confluence and interconnectedness makes them monumentally challenging. This report seeks to provide a blueprint for how to navigate these challenges and do so with a sense of urgency. It recommends four fundamental actions:

- The United States, and our allies and partners, must recognize that we are now in an **Era of Confrontation**. We are not merely competing with our rivals and adversaries. China, Russia, Iran, and North Korea are uniting in their intent and harmonizing their disruptive actions to end America's global leadership. They are undermining not just U.S. interests abroad, but actively attacking our public square, jeopardizing our critical infrastructure, and waging cognitive warfare on our leaders and our people. Understanding this new reality is a fundamental point of departure for any national security and defense strategy.

- At a time of monumental challenges and overtaxed resources, the United States should adopt an **Offset Strategy.** The age of American hyperpower ended with the war on terror. Primacy and overmatch against all adversaries require allocation of significant amounts of resources over a sustained period of time. And restraint fundamentally misunderstands the nature of today's challenges—their interconnectedness and their potency to cross national boundaries. In contrast, by leveraging strengths in technology and innovation, the United States could develop or rebuild asymmetric advantages against our adversaries and, in turn, offset their capabilities and theories of victory. Like

its successful Cold War predecessors, a new Offset Strategy does not require an all-exhausting commitment of resources. It does not require America to abdicate global leadership. And it does not set out as an endstate the pursuit of presently unrealistic supremacy.

- The United States military needs to rapidly resource and execute a new Joint Warfighting Concept that rests on a triad of advantages in **Sensing**, **Artificial Intelligence**, and **Autonomy**. This conceptual framework promises to deliver three advantages that are fundamental to prevailing in the type of warfare that the United States could face this decade—informational, decisional, and lethality advantage.

- Finally, the U.S. defense enterprise must evolve to meet the demands of speed, relevance, scale, and coherence required in modern warfare. This evolution needs to include creation of a **flexible and dedicated innovation budget,** beginning with at least 1% of the Department of War topline and increasing over future years. The new defense enterprise will also need to **embrace a production mindset,** shifting from stockpiling to producing, including building up latent capacity to quickly scale capabilities. The defense enterprise is also in need of cohering innovation endeavors; with one potential model being the establishment of a **Joint Warfare and Innovation Command**, empowered with authorities to drive integrated concept development, emerging capability acquisition, and force design. Lastly, as warfare moves beyond land, sea, air, cyber, and space into the digital and cognitive domain, the U.S. defense enterprise would be well-served to stand up a **Digital Warfare Corps** and a **U.S. Digital Command** to defend and fight in the digital domain.

The decisive decade we are in is not a horizon—it is a closing window. The United States must move with the urgency of a nation already under attack, because in many domains—cyber, cognitive, economic—we already are. The path to strategic advantage lies in seizing the initiative, creating dilemmas on our adversaries, and fielding a lethal force designed for the world we face, not the one we remember. Offsetting the capabilities of our adversaries with American ingenuity, industriousness, and innovation is a winning hand. America always answers the challenge. It's here.

Introduction

Three years ago, SCSP published Offset-X to warn and mobilize America at a time of growing danger. The United States had entered a decisive decade in which its longstanding military superiority was going to be at real risk. China's rapid buildup of advanced capabilities, its deliberate focus on exploiting U.S. vulnerabilities, and its stated goal of integrating mechanization, informatization, and intelligentization by 2027 were expected to pose a direct threat to U.S. interests in the Indo-Pacific and to the U.S. leadership that has underpinned global stability for nearly 80 years. While Beijing had been designing its forces specifically to counter the United States, Washington was lacking focus and urgency, moving at bureaucratic speed to adapt to this new reality. Offset-X was written to set forth a decisive path—by warning of the stakes, highlighting the limits of past approaches, and proposing a technology-centered defense strategy to restore deterrence, deny China's theory of victory, and preserve America's ability to project power in the Indo-Pacific and beyond.

Offset-X made several key recommendations for how the U.S. military could maintain or regain its advantage. First, it recommended that the U.S. military should adopt distributed, network-based operations that empower small, multi-domain units to act independently while still contributing to larger joint effects. Second, it recommended that the U.S. military become the premier human-machine teaming force by combining the unique strengths of its people—intuition, creativity, and contextual judgment—with the advantages of machines—speed, precision, and the ability to process vast amounts of data at scale. Finally, it recommended that the U.S. military gain and maintain software advantage in order to outpace adversaries in adapting to the fast-changing character of war. With superior software, the Joint Force can rapidly update systems, integrate new capabilities, and respond dynamically to emerging threats. Together, these reforms would give the U.S. military the adaptability, resilience, and speed needed to sustain its dominance.

Over the past three years, accumulating evidence from recent conflicts—particularly the undeniable evolution in the speed and automation of warfare—has underscored the urgent need to accelerate these reforms. Conflicts in Ukraine, Gaza, Iran, and the Red Sea have vividly demonstrated how advances in sensing, artificial intelligence, and autonomy are reshaping tactical and operational practices on the battlefield. Traditional notions and timelines of intelligence and warning, force generation, build-up, and deployment, and determining the

correlation of forces have been upended. Today's battlespace is increasingly transparent, dynamic, networked, autonomous, machine-teamed, and largely defensive dominant.

The Department of War appears to be recognizing these shifts, but progress has been uneven in adapting to these changes in the character of warfare, and particularly in integrating new technologies and capabilities into its force design, structure, and operations. Building and sustaining U.S. military advantage requires more than incremental adaptation—it demands accelerating structural, budgetary, cultural, and conceptual change across the Department of War. Without a decisive shift in how the U.S. military adopts game-changing technologies and prepares for future operations, adversaries will continue to design against American vulnerabilities faster than Washington adapts. **Offset-X Evolved** provides a roadmap for closing this gap and ensuring that the United States preserves its warfighting edge, displays credible deterrence, and builds the resilient, adaptable force required for the decisive period ahead.

This report is structured as follows:

- **Part 1** provides a bellwether example of how the United States' current competition-minded approach to our adversaries could lead to a military and strategic defeat.

- **Part 2** explains the battlefield dynamics and technological advancements that underpin the impetus for change in U.S. military concepts, capabilities, and institutions.

- **Part 3** outlines the strategic options the United States can potentially choose from—and explains why an Offset Strategy is the most viable way to forge America's military advantage in this new era.

- **Part 4** presents actions to design and execute an Offset Strategy that harnesses evolving technology, reinforces proven capabilities, bets on emerging technology, and reimagines institutions, funding, and processes for success.

PART ONE

The Taiwan War of 2027: One Potential Version of a Future

The following is a strictly hypothetical, but also plausible scenario that can unfold in the near-term along with attendant consequences and implications.

In hindsight, America's defeat in the Taiwan war of 2027 should have come as no surprise. U.S. defense experts had long warned that Taiwan's military needed to move faster to restructure its military forces, increase its spending, and acquire new capabilities better suited for the growing threats from the People's Liberation Army. Yet when war came, those same deficiencies became obvious in America's own military.

The onset of the conflict took the United States by surprise—tactically and operationally. Chinese confrontation tactics had long encircled Taiwan with warships, fighter jet sorties, and realistic military drills. American military commanders had warned that these tactics were not mere exercises, they were rehearsals. Yet, in the months preceding the outbreak of open hostilities, People's Liberation Army (PLA) tactics escalated—in front of American and allied watchful eyes. To be sure, China's expanded activity raised alarms in Washington and American military forces began to increase their readiness for battle in response. But the U.S. military could not keep its ships and aircraft on high alert indefinitely. As the months passed, repairs and refurbishments took more and more equipment offline. Other global hotspots also required American attention and resources, distracting senior officials from the ongoing Chinese buildup and discerning the new normal of large scale exercises and coercion from precursor rehearsals. While the alarms in Washington were still sounding, fewer and fewer heeded their warning.

The opening days of the conflict brought unpleasant surprises for American planners. Chinese cyber attacks wreaked havoc across critical infrastructure in East Asia and even in the continental United States, disrupting key logistical nodes needed to support U.S. combat operations. Swarms of Chinese autonomous drones, advanced satellites, and unmanned vessels provided Beijing with effective long-range precision strike and anti-submarine capabilities—eroding advantages that for decades underwrote U.S. primacy and freedom of maneuver. Repeated and relentless salvos

of surface-to-surface and anti-ship missiles created a hellscape in the Taiwan straits and in the island itself. American forces suddenly found themselves vulnerable even in areas once assumed to be safe havens. China's low-cost, attritable drones, unmanned ships, and smart mines were lost in large numbers, but each U.S. F-35 fighter, Virginia-class submarine, or B-21 bomber they damaged or destroyed was a loss that could not be replaced during the conflict. With relatively few high-end weapons available to begin with, every loss sapped strength from the American defense.

One new American capability brought hope that the Chinese onslaught could be slowed, and possibly defeated. Thousands of prepositioned cheap, attritable unmanned systems—pursued through Project Replicator and its successors—helped defend Taiwan against the PLA assault. Replicator's drones performed exactly as intended—providing an initial mass to disrupt Chinese amphibious landing on the island and inflict attrition on PLA attackers. Yet—as expected—this attrition cut both ways. Tens of thousands of drones fell to earth in the first days of the conflict. As the last of the Replicator drones scrambled to intercept incoming attackers, American factories were just beginning to ramp up to manufacture their replacements. On the Chinese side, the supplies of drones appeared endless, and their manufacturers went into production overdrive—prepared by years of dominating the global drone market.

Disconnects within the U.S. military and between America and its allies further hampered the war effort. The United States had spent years talking about "integrated deterrence" and "interoperability," but in practice, no true joint or combined concept of operations ever proved influential enough to coordinate real-world operations or innovation efforts. There were vague agreements, periodic exercises, even some co-developed technologies — but no unified doctrine for how to fight a high-end war together across the Indo-Pacific. Meanwhile, each U.S. military service had pursued its own vision of how autonomy would work in its domain with little alignment into a cohesive and credible whole. Similarly, each had pursued their own service-centric command and control systems, with little regard for interoperability under stress. Likewise, U.S. submarines, Japanese destroyers, and Australian fighter jets each performed well individually, but they fought in silos rather than as a seamless team—often hampered by national caveats on what targets they could engage. Throughout the conflict, joint and allied capabilities proved to be less than the sum of their parts.

A final, self-inflicted wound crippled the American response: our inability to adapt in real time. Though prior to the conflict the U.S. military was viewed as more battlehardened than the PLA, many of America's commanders with warfighting experiences from Iraq and Afghanistan had retired, a few were dismissed, and others struggled to adapt to the new character of near-peer conflict. As the conflict wore on, U.S. personnel needed to rapidly adjust their tactics and modify equipment—both to exploit Chinese weaknesses and to respond when the PLA nullified American advantages. But these battlefield insights rarely made it back on time to the engineers and technologists who could implement them. When front-line operators reported software bugs or

vulnerabilities through official channels, the fixes bogged down in weeks of planning, development, testing, and approval before deployment. By the time changes made it back to the front lines, the battlefield realities had already shifted—often not in America's favor.

In the aftermath of the conflict, defense experts bemoaned America's missed opportunities. Too often, the weaknesses that felled a once-mighty superpower had been well-known in advance. Yet peacetime complacency paralyzed leaders across the government from making the changes they knew were necessary. The U.S. defense ecosystem had come to resemble the very command-and-control rigidity and central planning that America had once outmaneuvered in the Cold War. American leaders lost sight of the culture of ingenuity and public-private industrial teaming that had propelled the United States to victory on these same Pacific battlefields in the past. The irony was tragic; American companies were leading the AI revolution. But the American government was too sclerotic to incorporate these and other capabilities in its ranks. Ultimately, only the catastrophic consequences of indecision finally galvanized the American government into action—but by then, it was too late. China achieved its war aims.

Postmortem: Why Did We Lose?

This American failure was not borne out of USINDOPACOM headquarters—it was the predictable consequence of deep structural deficiencies within the U.S. defense and budgetary enterprises. The seeds of defeat were sown long before the first missile was launched. They took root in peacetime decisions about which technologies to invest in, how (and how quickly) to experiment, iterate, and adapt; in an aversion to "failing" (and thus learning) in peacetime and to taking calculated risks, and in how to conceive of and build a truly integrated joint force despite nearly $1 trillion a year in defense spending.[1] Five critical failings contributed the most to this outcome.

1. Underinvestment in Critical & Evolving Technologies

Central to the U.S. loss was the Department of War's lack of investment in and serious fielding of critical and evolving technologies. Despite the bipartisan consensus that the Department of War needed to better leverage the rapid technological advancements originating in America's vibrant commercial sector, startups persistently captured less than 1% of all defense procurement.[2] Instead, most resources remained tied up in legacy platforms and

[1] FY2025 Defense Appropriations: Summary of Funding, Congress.gov (2024).

[2] Heather Somerville, Investors are Betting on Defense Startups. The Pentagon Isn't, Wall Street Journal (2024).

large primes rather than fueling the very ecosystem that could have restored America's technological edge. Air Force budgets continued to prioritize the replacement of its existing manned fighters, long-range bombers, and ICBM fleet. Similarly, the Navy budget was consumed by purchases of aircraft carriers, conventional surface warships, nuclear submarines, and fighter jets. Overall, the story was consistent: instead of betting on the weapon systems of the future and integrating them with still-viable legacy systems, the Department of War devoted the bulk of its investments into systems that were essentially modernized incarnations of those systems that won us the Cold War.

Even worse, where investment in innovative technologies did occur, the Pentagon too often remained stuck in old habits. For one, the Department of War often continued to treat these technologies as a promising R&D project long after they had advanced to the point where they should have been procured and deployed to operational units as a viable capability. Perhaps the most striking example of this phenomenon has been the treatment of UAVs within the defense budget. Despite the centrality of drones to the conflicts in Ukraine, and the Red Sea,[3] the overwhelming majority of Pentagon's funding for UAVs (more than 80%) remains in R&D budgets with a minuscule amount left over for procurement.[4] Moreover, too often Pentagon's acquisitions went to established companies without leaving room for the possibility that new entrants might bring new capabilities. The pattern is visible even in marquee efforts like the Replicator Initiative: its first tranche devoted approximately a fifth of its budget towards purchasing fifteen-year-old loitering munitions[5] even as UAV technology radically advanced monthly or even weekly on the battlefields of Ukraine.[6] Ultimately, the imbalance between R&D and acquisition of viable technologies resulted in prototypes, whereas adversaries moved to mass production.

China, by contrast, benefited from two advantages. First, Beijing wasn't shackled to an inventory of legacy platforms. Because they didn't have as many "exquisite" Cold War systems to sustain, China could behave like a disruptive upstart while the United States acted like a complacent incumbent. True to the innovator's dilemma, the United States was hesitant to let go of its proven but aging strengths even as China seized the future with a clean slate. Second, China exploited its second-mover advantage. Because the United States largely stayed moored to an unchanging force structure, China could precisely target U.S. strengths

[3] Benjamin Jensen, Fewer Soldiers, More Drones: What Ukraine's Military Will Look Like After the War, Center for Strategic and International Studies (2025).

[4] Maggie Grey, Follow the Money: What the Pentagon's Budget Data Tells Us About AI and Autonomy Adoption, Gray Matters (2025).

[5] Howard Altman, Switchblade 600 Kamikaze Drone is the First Named Replicator Program Weapon, The War Zone (2024).

[6] Mick Ryan, The New Adaptation War, Futura Doctrina (2025).

and weaknesses. While the United States leaned on the tools it knew best, China developed a creative array of asymmetric counters using rapidly improving technologies.

2. Insufficient Experimentation with Game-Changing Technologies

As the United States learned to its detriment, the outcome of war, now more than ever, is predicated on the ability of military institutions to absorb battlefield feedback and adapt their systems. No matter how rigorous the peacetime testing, the first hours of real combat expose surprises: a pilot's cockpit display freezes just when situational awareness matters most; radios that survived laboratory jamming collapse under an adversary's full-spectrum electronic-warfare barrage. The Department of War did not build flexibility in its force structure and units to evolve software and hardware continuously, to respond to real-time data from the front. In other words, the Department of War lacked the experimentation loop linking operators, designers, technologists, and manufacturers in near-real time. Forward units *were not enabled to* push telemetry and after-action notes directly to the engineers who wrote the code or built the sensor; those engineers did not have the option to rapidly field-test fixes within relevant speed; and the updated capability did not return to the fight while the tactical problem persisted. Delivery of warfighting capability onto the field was unacceptably late, and experimentation loops stretched out across months and years instead of days and weeks, driven largely by compliance-driven, serial process-laden acquisition processes.[7]

The war in Ukraine offers a vivid modern example of why rapid experimentation and adaptation are so critical. As retired Major General Mick Ryan states, "the pace of change in Ukraine is probably incomprehensible to western defence bureaucrats," and "the character of the fight is now liable to change every six months." [8] The drone and counter-drone contest there illustrates this clearly. Drone software updates occur *daily*, and drone hardware and tactics evolve weekly.[9] Since 2022, Ukraine has built hundreds of small, closed-loop drone factories and workshops, boosting its domestic output of drones from essentially zero pre-war to nearly two million units in 2024.[10] This surge was enabled by government incubators and crowd-sourced funding that embedded engineers with fighting brigades and treated quick "good-enough" fixes as victories. A nightly routine emerged: infantry platoons upload combat video and electronic warfare logs after each day's fighting; overnight, civilian

[7] Hannah Hunt, The Defense Department has a User Experience Problem (2025).

[8] Mick Ryan, The New Adaptation War, Futura Doctrina (2025).

[9] Mick Ryan, The New Adaptation War, Futura Doctrina (2025).

[10] Kateryna Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare, Center for Strategic and International Studies (2025).

volunteers manufacture new airframes, flash updated flight-controller firmware, and hand back improved drones within 24–72 hours. Moreover, when Russian drone barrages jumped significantly in volume from 2024 to early 2025, the Ukrainian's successfully adapted by fielding AI-enabled mobile "Shahed-hunter" teams equipped with robotic gun-trucks and automated C2 systems.[11] In contrast, new American weapons systems can take years and even decades to deliver. By the time they arrive, the missions they had been designed for and the threat environment they face have radically changed.

While the need for a fast-cycle experimentation loop has always existed, it has become absolutely essential today given the dynamic speed and character of warfare, and the short-lived nature of advances that technological innovations bestow. Fortunately, modern software-centric systems (sensors, communications, AI, etc.) make rapid iteration feasible. Commercial tech firms push code updates dozens of times per day;[12] large AI models double their performance every few months;[13] a $200 hobbyist quadcopter can be turned into a precision strike asset over a single weekend with a firmware hack.[14] None of these innovations wait for the ponderous acquisition paperwork that still governs most U.S. programs. The 2018 National Defense Strategy itself warned that victory will go to the side that can "deliver performance at the speed of relevance.'[15] In short, the currency of military dominance has shifted from massed steel to learning velocity. Unless the United States radically restructures its acquisition culture around rapid, operator-adjudicated iteration, it will watch more agile rivals redraw the battlespace at a pace we cannot match.

3. Failure to Adopt Winning Warfighting Concepts

Another critical reason for America's defeat lay in the Pentagon's inability to operationalize viable concepts of operations. On the eve of war, the Department of War had no single entity responsible for this vital task. Instead, this responsibility was diffused and federated—with no clear or centralized accountability.

[11] Myroslava Tanska-Vikulova, et al., Nighttime with Ukraine's Drone Hunting Teams, The Counteroffensive with Tim Mak (2024); Benjamin Jensen & Yasir Atalan, Drone Saturation: Russia's Shahed Campaign, Center for Strategic and International Studies (2025).

[12] Software Acquisition and Practices Study, Defense Innovation Board (last accessed 2025).

[13] Thomas Kwa, et al., Measuring AI Ability to Complete Long Tasks (2025).

[14] Kateryna Bondar, Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare, Center for Strategic & International Studies (2025).

[15] Summary of the 2018 National Defense Strategy, U.S. Department of Defense (2018).

The Joint Staff nominally has the responsibility for some aspects of this function, but being mostly an advisory body with limited capacity and no budget authority to actually acquire new warfighting capabilities, it is significantly humstrung. The geographic Combatant Commands are responsible for contingency plans for their domains, but because they must focus on being ready to "fight tonight," they lack a forward-looking mandate (or the acquisition authorities) to explore promising new technologies at scale. Like the Joint Staff, the COCOMs have virtually no ability to field capabilities on their own. Lastly, while the Secretary of War in theory has the authority to unify these efforts, in practice any given Secretary is pulled in many directions and typically serves only a few years – not long enough to institutionalize major new concepts across administrations and budget cycles.

Ultimately, the job of building and fielding warfighting capacity falls to the individual military services through the budgets they control (under oversight by the U.S. Congress). But each Service is structurally incentivized to innovate for its own domain, preparing independently for its own fight. That is not the world we live in today. Warfare is now all-domain, global, at range, and largely agnostic to Service boundaries. Only innovative employment of evolving and emerging technology—harnessed across the Services—can produce the level of cohesion and lethality needed for the future fight.

Lastly, while capability development pathways such as the Joint Capabilities Integration and Development System (JCIDS) and the Joint Requirements Oversight Council (JROC) were intended to systemically integrate "jointness" into the acquisition process, their focus is at the programmatic development-level and not driving suites of joint force design capabilities that manifest in winning, lethal warfighting concepts. The Department of War's rescission of JCIDS (August 2025) is a prudent first step, though incomplete. The Department of War still lacks the central authority, oversight, and accountability needed to coherently drive capability development supporting the joint warfighting concept. This leaves Combatant Commanders to fight with the forces they get rather than the forces they need.

4. Slow to Counter Coercive Confrontation by the PRC

The Taiwan conflict was preceded by the PRC's long-running asymmetric campaign that set favorable conditions for Beijing and secured decisive advantages before the first shot was even fired. China's irregular warfare tactics spanned the full spectrum of cognitive, cyber, informational, psychological, electronic, and electromagnetic operations—similar to what the United States and our allies endured for years during the era of so-called great power "competition."

- **Cyber Operations:** Coordinated hacking campaigns by Chinese state-sponsored groups quietly seeded malware into the routers and unpatched servers of Taiwan's critical infrastructure—ports, rail hubs, airports, power grids. By the time conflict

loomed, PLA cyber units had hands on the switches of much of the island's civilian backbone.

- **Electronic Warfare:** Beijing practiced aggressive jamming and sensor interference well beforehand, much as seen in incidents when Chinese forces jammed Philippine naval and even civilian communications during routine operations at Second Thomas Shoal. When the time came, the PLA was ready to disrupt allied communications and radar on demand.

- **Information & Influence:** The PRC orchestrated AI-generated deepfakes and coordinated social media disinformation during Taiwan's 2024 presidential election, portraying China's rise as benign and American involvement as a grave security and economic risk. Beijing also repeated incessantly—through officials and state media—that Taiwan *belongs* to China and any resolution must be "China-only." This cognitive warfare softened the ground for actual conflict.

- **Sabotage & Subversion:** Limited but effective covert attacks—like unexplained "accidents" that severed undersea cables linking Taiwan to the global internet—continued at a steady drumbeat. These incidents sowed uncertainty and intermittently cut off Taiwan's access to outside information. At the same time, China's legal warfare (lawfare) dismissed international legal rulings (e.g., the South China Sea tribunal) and norms, signaling Beijing's intent to ignore global rules when inconvenient.

- **Conventional Posturing:** All the while, China persisted with coercive military demonstrations—larger and more frequent exercises, encroachments into Taiwan's maritime and air space, even high-altitude balloon flyovers—to highlight Taiwan's vulnerabilities and normalize PLA presence.

By the time Washington sought emergency basing and overflight rights at the outbreak of war, several Southeast Asian partners—spooked by Chinese economic leverage and inflammatory propaganda—withheld permission. Their parliaments, swayed by anxious public opinion and Beijing's threats, delayed or denied U.S. requests, giving the PLA a further edge in seizing the initiative.

Because each move fell just short of open aggression, Washington treated them as discrete irritants rather than pieces of a choreographed confrontation campaign. Inter-agency warning cables piled up, but there was no single "tripwire" event dramatic enough to push the machinery of government into crisis mode. Instead, the United States countered each in isolation and on bureaucratic timelines measured in months; fearful of escalation. Taken together, however, they built a battlespace that overwhelmingly favored the initiator. When deterrence shattered, China did not need years of attrition; it needed only days in which

maritime chokepoints were held at risk, logistics were hobbled, datalinks went dark, allies were shaken, and critical spare parts were stuck in export-license limbo. The United States lost the war in part the same way it lost the peace: by recognizing too late that the PRC's constant coercive pressure was not background noise but the first, decisive phase of Beijing's campaign.

5. Lack of Capability from Allies & Partners

One final weakness contributed to the American defeat. Years of underinvestment in critical and emerging military capabilities, left America's allies and partners in East Asia poorly equipped to contribute meaningfully to joint operations. While Chinese forces fielded autonomous systems, integrated sensor networks, and AI-driven command and control tools capable of reacting at machine speed, American friends in the region remained reliant on legacy platforms and slow, human-in-the-loop targeting processes.

Lacking the computational infrastructure, data-sharing architectures, and software-defined capabilities that had become essential in modern multi-domain warfare, allies and partners struggled to integrate with U.S. forces or operate independently in contested environments. Their inability to process real-time intelligence, automate defensive responses, or coordinate with U.S. battle networks under degraded conditions rendered them strategically sidelined. What might have been a regional coalition capable of imposing distributed dilemmas on the PLA instead became a patchwork of disconnected forces—well-intentioned but technologically obsolete—unable to blunt China's initial offensive or sustain high-tempo operations in the critical early days of the conflict. Ultimately, our allies and partners could only crawl in areas where the United States and China could run.

PART TWO

Technology, Rivalry, and the Future of War

Understanding the strategic context within which the U.S. defense enterprise operates is essential to grasping both the challenges which can set the United States up for defeat and the opportunities the United States must seize to achieve success. The deficiencies hampering the US military did not emerge in a vacuum—they were deeply influenced by America's broader geopolitical position, its assumptions about military power, and the evolving character of warfare itself. This chapter situates the choices facing the Department of War within the larger backdrop of a world characterized by rapidly advancing technology, intensified great power rivalry, and adversaries who exploit the seams between peace and war. By tracing the evolution of the modern battlespace, this chapter lays the foundation for understanding both the scale of the challenge posed by China and the conceptual recalibrations the United States must undertake to meet it.

Established, Emerging, and Evolving Technologies

When considering how to exploit the technologies driving these changes in warfare, it is important to recognize that not all tech is advancing at the same pace. Some fields are moving explosively fast, while others have matured and improve more slowly. Understanding these differences allows policymakers to prioritize investments wisely.

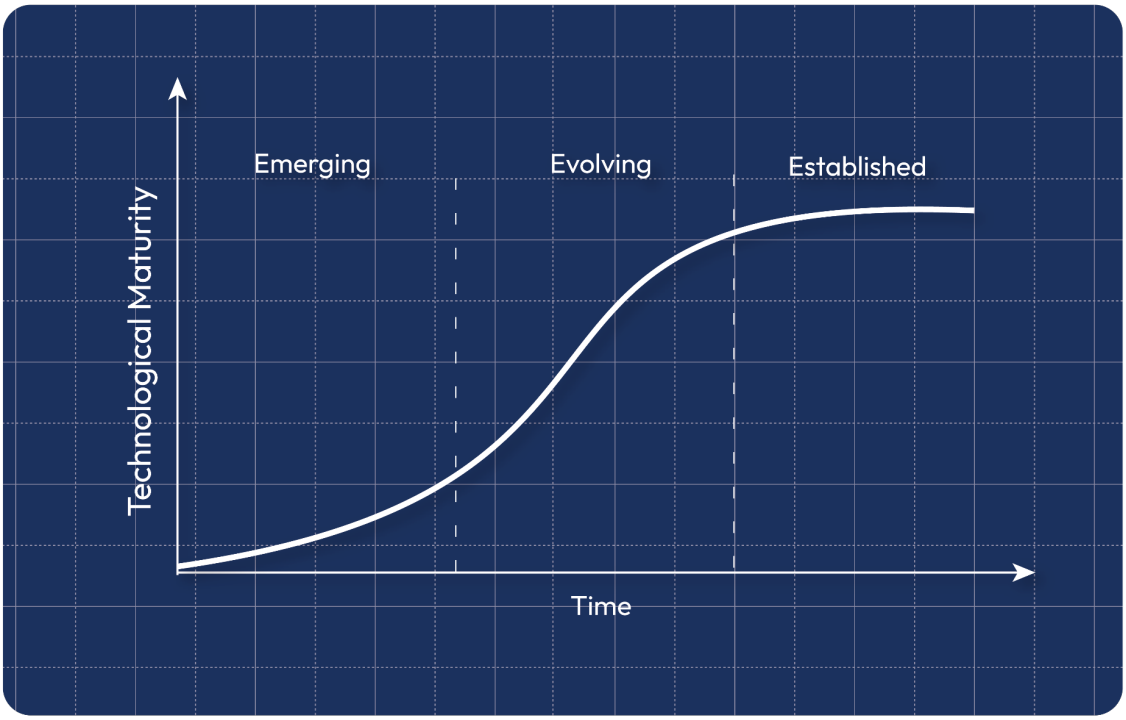
Most technologies progress along an S-curve over time.[16] We can classify them into three groups along this curve:

- **Emerging technologies:** These sit at the early stage of the curve. They have high potential but currently deliver little (if any) operational value. Examples might include experimental quantum sensors or early-stage fusion power. They are largely unproven in the field.

[16] CM Christensen, The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail, Harvard Business Review Press at 39-56 (1997).

- **Evolving technologies:** These occupy the steep middle portion of the S-curve. They have matured beyond the lab and become viable tools for end-users. More importantly, they are improving rapidly with each iteration. At this stage, major enhancements can be achieved quickly. Prior versions of an evolving tech can become obsolete in just a few years or even months as new features and better designs are rolled out.

- **Established technologies:** These sit near the top of the S-curve. They have gone through many generations of improvement and reached a high level of maturity and performance. Established tech (e.g. fourth-generation fighter aircraft or main battle tanks) delivers reliable, well-understood capability for its intended mission. However, further improvements are increasingly difficult, slow, and costly to achieve—each incremental upgrade yields diminishing returns until performance plateaus entirely.



Within this taxonomy, military organizations often focus their resources into perfecting and fielding established technologies.[17] This is for several reasons. For one, pursuing established technologies presents the least acquisition risk. Additionally, the success of established technologies makes them essential to the future plans of the military. Thus, military operators and planners will demand improvements in these technologies to overcome the problems they know

[17] Thomas McNaugher, New Weapons, Old Politics, The Brookings Institution at 96-99 (1989).

all too well. Furthermore, established technologies typically deliver a more reliable capability compared to an evolving technology which is improving but not yet achieving its full potential. Finally, large organizations looking to widely adopt new technological capabilities face a significant overhead cost from developing new doctrine to take advantage of the capability, training their personnel to perfect that doctrine, and devising other rules and procedures to maintain and integrate the technology. While military organizations will often establish small units to experiment with new technologies and doctrinal concepts, they often hesitate to embrace and fully exploit evolving technologies prior to the outbreak of conflict.[18]

However, these traditional approaches to technological investments can lead military organizations astray. In practice, prioritizing established technologies over evolving technologies results in stagnation. The investments contained within the military budget are zero-sum; money spent on procuring established technologies cannot also be spent on programs delivering evolving technologies. Minor, incremental improvements in established technologies, especially when combined with sustainment costs, become more expensive to achieve and can require longer timeframes to deliver. The U.S. military knows this all too well as it watches its fleet of aircraft, helicopters, ships, and vehicles age while their replacements routinely bust their predicted budgets and schedules.[19] If the Department of War instead increased its investments in evolving technologies, it could potentially buy far more rapid improvements at a potentially lower cost.

Evolution of the Character of War

Modern warfare is evolving rapidly, as evidenced by three ongoing conflicts—Russia's war in Ukraine, Israel's war against Hamas terrorists in Gaza, and the Houthi threat—sponsored by Iran—against the free flow of commerce and information in the Red Sea. Each of these wars features new technologies and tactics that are showcasing and further shaping the new character of war at the tactical and operational levels. Leveraging unmanned systems, AI applications, and intelligent sensing to achieve scaled, massed, or precise effects are key attributes of operational designs across these geographically dispersed conflicts. These factors demonstrate the technological and multi-domain complexity of waging modern warfare. While each conflict has its own unique dynamics and other theaters will differ in some of the details, they collectively reveal enduring trends in the character of war that will manifest in distinct ways in future conflicts.

[18] Williamson Murray, Military Innovation in the Interwar Period, Cambridge University Press at 6-49 (1996).

[19] Steven Kosiak, Is the U.S. Military Getting Smaller and Older, Center for a New American Security (2017).

Unmanned Systems

Unmanned systems—especially aerial drones—are dominant tactical tools across contemporary conflicts. In Ukraine's war, the scale, purpose, and effectiveness of drone use is unprecedented. Both Russia and Ukraine rely on millions of drones a year for reconnaissance, artillery spotting, strike missions, and even counter-drone missions. Ukraine has also succeeded in altering the balance of seapower in the Black Sea via the use of surgical, autonomous sea drones.

In Israel's response to Hamas' terrorist attacks of October 7, Israel has employed drones as a core component of its ISR and targeting capability. The Israel Defense Force's (IDF) Hermes 450 and Heron drones have provided constant surveillance over Gaza and carried out precision strikes against Hamas targets hiding in urban areas. Israel has also leveraged artificial intelligence to identify and nominate targets, significantly increasing the tempo of its military operations. Unmanned systems have also been used by Hamas. The terrorist group used readily available quadcopters as cheap "air forces" to support ground attackers and deployed at least 35 larger *Zouari* loitering drones to rove over Israeli territory and strike targets with explosive charges. Meanwhile, in Yemen, the Houthi rebels have employed drones and unmanned systems extensively as a core element of their asymmetric warfare strategy launching hundreds of drone strikes against Saudi Arabian infrastructure, and U.S. Navy forces and commercial shipping in the Red Sea, demonstrating the lethality of inexpensive unmanned systems for strategic effect.

AI at War

AI systems have been widely employed across today's battlefields. In Ukraine, both sides are experimenting with AI-driven capabilities and have begun employing "last-mile" targeting AI to guide drones in their final approach to a target, enabling greater strike precision and survivability of platforms against countermeasures. Following tactical success with first-person view (FPV) drone employment to blunt Russian freedom of maneuver, semi-autonomous and fully autonomous drone swarms are emerging as a key R&D priority. Beyond drones, Ukraine's military has also deployed digital command systems like the *Delta*[20] and *Kropyva*[21] platforms that incorporate AI models for situational awareness and rapid targeting, giving Ukrainian units a decision-making edge despite Russia's larger size. Russia, for its part, has tested robotic platforms such as the "Marker" unmanned ground vehicle and is integrating more automation into intelligence processing and electronic warfare.

In the Israel–Hamas conflict, the use of autonomy has been most apparent in Israel's high-tech arsenal. The IDF has leveraged Project Maven-like AI systems to sift through vast troves of

[20] What is the Delta System and How Does It Set Trends for NATO Countries, Ministry of Defense of Ukraine (2024).

[21] Seth Jones, et al., Ukrainian Innovation in a War of Attrition, Center for Strategic & International Studies (2023).

intelligence – intercepted communications, surveillance feeds, and more—to identify targets in Gaza. Israel's AI-based systems, codenamed "Gospel" and "Lavender", suggested strike targets by analyzing live data and accelerated the IDF's ability to classify potential threats and make targeting decisions. Across each of these theaters, AI has made unmanned systems more deadly and proved essential to conducting military operations at the pace and scale required by the modern era.

Intelligent Sensing and ISR

On today's battlefield, the very idea of concealment is under attack. In an era when nearly everything doubles as a sensor, hiding has become nearly impossible. Devices once designed for convenience or commercial use—health rings, smartwatches, smartphones, even modern vehicles—emit constant streams of location, biometric, and usage data that can be harvested and exploited.[22] Layered on top of this are dedicated military and commercial sensing systems: radars, drones overhead, satellites in orbit, electronic eavesdropping networks, and ubiquitous cameras. The result is a battlespace that is increasingly transparent, one in which the old art of moving unseen has given way to the hard science of detection.[23]

Nowhere is this more apparent than in Ukraine, where the density of sensors—old and new—has largely stripped away the protective fog of war. From the outset of the war, soldiers on both sides quickly discovered that any electronic signature—whether from a personal phone call,[24] a heat signature picked up by infrared drones, or the noise of tracked vehicles—could be detected and targeted within minutes. Ukrainian forces developed digital platforms like *Delta*[25] to fuse inputs from drones, radars, and human observers into a real-time operational picture, creating a multilayered awareness that denies Russia the element of surprise. With ever-watchful drones in the sky, the movement of troops and equipment has become exceedingly dangerous. Even small shifts along the front risk triggering a devastating response.

Similar patterns have emerged in the Middle East, where combatants from state militaries to insurgent groups exploit cheap drones and networked sensors to illuminate the battlefield. Israel has repeatedly located and quickly struck leadership targets in Lebanon, Gaza, Yemen, and Iran through a combination of human sources and technical means[26] paired with incredible strike

[22] Stuart Thompson & Charlie Warzel, Twelve Million Phones, One Dataset, Zero Privacy, New York Times (2019).

[23] The Added Dangers of Fighting in Ukraine When Everything is Visible, The Economist (2025).

[24] Alan Yuhas, et al., For Russian Troops, Cellphone Use is a Persistent, Lethal Danger, New York Times (2023).

[25] What is the Delta System and How Does It Set Trends for NATO Countries, Ministry of Defense of Ukraine (2024).

[26] Farnaz Fassihi, et al., Targeting Iran's Leaders, Israel Found a Weak Link: Their Bodyguards, New York Times (2025).

platforms. In Gaza, Israel has relied on persistent drone surveillance[27] and AI-assisted analysis[28] to maintain a near-constant watch for Hamas fighters, while Hamas itself has used commercial quadcopters to track Israeli units and launch precision attacks.[29] In Yemen, Houthi forces have leveraged drones and intelligence collected from various platforms to strike naval vessels and regional infrastructure, demonstrating that even non-state actors can now wield reconnaissance-strike capabilities once limited to major powers. The effect has been to erode safe havens: forces can be tracked, fixed, and struck with unprecedented speed.

The consequence of this pervasive transparency is profound. Strategic surprise—the ability to mask large-scale movements, conceal preparations for war, or disguise intentions over time—has become vanishingly rare. Adversaries are able to detect buildups long before they culminate in conflict, as intelligence feeds from satellites, commercial sensors, and open-source data converge to reveal patterns. Yet while strategic surprise is nearly impossible, tactical or operational surprise remains achievable. With careful preparation, deception, and rapid execution, commanders can still overwhelm defenders at a point of attack or exploit fleeting weaknesses. But such advantages are increasingly measured in hours or minutes, not weeks or months. In this new environment, the margin for error is thinner than ever, and the ability to outpace detection—not to escape it altogether—has become the defining challenge of modern warfare.

Scaling and Massing Effects

Despite the high-tech precision of modern weapons, quantity and mass effects remain decisive in these conflicts. The ability to *scale capacity is a capability in and of itself,* overwhelming even advanced defenses. All three conflicts underscore how mass can be used both in the physical sense (troops, drones, rockets in large numbers) and in the industrial sense (scaling production and logistics to sustain the fight). In particular, the mass deployment of unmanned systems has fundamentally changed battlefield dynamics—often resulting in a defensive advantage.[30]

In Ukraine, the evolution of the conflict has exemplified how hard it is to achieve a breakthrough against a massed defense. Russian forces had emplaced layered minefields, tank traps, and dense trench lines across hundreds of kilometers. Attempts to mass Ukrainian armored units for

[27] How Israel is Using Drones in Gaza, The Economist (2023).

[28] Sheera Frenkel & Natan Odenheimer, Israel's AI Experiments in Gaza War Raise Ethical Concerns, New York Times (2025).

[29] Kerry Chavez & Ori Swed, How Hamas Innovated with Drones to Operate Like an Army, Bulletin of the Atomic Scientists (2023).

[30] T.X. Hammes, The Tactical Defense Becomes Dominant Again, National Defense University Press (2021).

a decisive counteroffensive were detected and met with concentrated fires, causing heavy losses. One emerging view is that the attacker now needs *localized mass plus stealth* to succeed – essentially, concentrating effects faster than the enemy can respond. Without surprise, massed assaults become costly. This will require new operational concepts to "allow the survivable concentration of military forces" that can punch through defenses and exploit breakthroughs. Finding ways to mass combat power *without* suffering mass attrition (e.g. through better suppression of enemy sensors, or dispersal until the moment of attack) will be key.

In Gaza, Hamas demonstrated the power of mass, tactical surprise, *and* the strategy of saturation. On Oct 7, Hamas fired *an exceptionally large volley of rockets – over 3,000* in the first day – toward Israeli cities, deliberately aiming to saturate the Iron Dome defense system, achieving a temporary local superiority by concentrating its efforts en masse at one sudden point in time – overcoming the qualitative and technological edge of the IDF through sheer volume and surprise. However, Hamas could not *sustain* that mass across multiple fronts and extended supply lines. For policymakers, the Gaza fighting suggests that even high-tech militaries like the IDF must never underestimate an opponent's ability to generate mass effects. Saturation attacks – whether through rockets, drones, or cyber means – can strain the best defenses if not anticipated. Planners should ensure critical systems have redundancy and surge capacity to blunt initiative and stem adversary momentum.

In Yemen and the Red Sea theater, scaling and massing have taken a different form. The October 2023 barrage attack on the USS *Carney* where the Houthis fired a near simultaneous salvo of cruise missiles and drones challenged *Carney's* advanced Aegis radar and depth of interceptors. The *economics* of this exchange favor the offense: the Houthis can afford to throw multiple cheap drones and missiles, forcing the defender to expend many expensive interceptors or accept the risk of leakers.

Across all these cases, a clear theme emerges: *"Mass matters"*. War-winning capability rests not only on having advanced weapons, but on industrial and innovation resiliency to both surge and continuously supply both hardware and software capability at relevant speed. Future conflicts with existential stakes will likely be protracted, stressing operations at the tactical edge as well as the supporting functions of capability development, innovation, logistics, and hyperscaling. Modern militaries must learn how to balance investments in a few exquisite platforms against cost-effective investments that enable mass deployment—be it large fleets of drones, abundant smart munitions, or the capacity to mobilize and train additional manpower. Furthermore, adaptability in command and control will be essential to handling mass combat: commanders will need to rely on mission command or command-by-negation to react to swarms or large attacks instantly, rather than waiting for centralized decisions. In summary, massing isn't obsolete— it's evolving. Success in future wars will go to those who can concentrate decisive force at critical points *without* suffering prohibitive losses from the enemy's sensors and fires. It will also go to those whose industrial base can ramp up output to sustain that force over time.

The Spectrum of Conflict

In today's complex, competitive, and confrontational and contested global environment, national security policymakers must correctly diagnose the character of interactions between rival states. These interactions don't fall neatly into "peace" or "war," but instead span a **continuum of conflict** that includes phases of competition, confrontation, crisis, and conflict. Each phase represents a deeper level of hostility and risk, with different objectives, behaviors, and escalation thresholds. Understanding these phases—and how adversaries deliberately shift between them—is critical to appreciating the true nature of the threats we face and devising effective deterrence strategies.

- **Competition:** A state of affairs in which actors vie to achieve advantages, sometimes over each other, while (at least ostensibly) adhering to certain rules and norms. For example, countries compete in areas like economic growth, technological development, military capacity building, or global influence. There may be rivalry and tension, but each side stays within recognized bounds and direct conflict is not imminent.

- **(new) *Confrontation*:** A phase beyond competition, where a state undertakes actions that circumvent rules and norms, and engages in coercive activities intended to achieve advantages and unilaterally improve its position from the status quo. Confrontation includes disruptive actions, as well as threats of further escalation to violence to achieve objectives.

- **Crisis:** A juncture at which two states face a time-critical decision about whether to escalate into open conflict or step back via some agreement or concession. In a crisis, war is a very real and near-term possibility unless de-escalatory measures are taken.

- **Conflict:** Active armed hostilities. This phase is unambiguous—nations are engaging in direct action to harm and destroy the other's forces—but it may occur without a formal declaration of war. Modern conflicts might begin with "grey zone" tactics and escalate into full combat without a clear break.

Mindful of the disruptive campaigns and aggressive actions by the Axis of Disruptors, as well as the new, technology-enabled means to apply coercive effects, it would be prudent for the United States government to recognize **Confrontation** as a distinct and likely persistent phase of the spectrum of conflict—and the reality that America is in one. America's adversaries – particularly China and Russia—have never subscribed to *Competition*, rallying to *Confront* American global leadership.

American policymakers correctly diagnosed in 2017 that the United States was facing a new era of great power rivalries with revisionist powers, particularly China and Russia. But the

developments that have transpired since, suggest that competition has transitioned to confrontation. Chinese hackers have infiltrated and pre-positioned malware inside America's critical domestic infrastructure[31] and at vital military installations.[32] In the South China Sea, China Marine Surveillance (CMS) vessels routinely ram and harass ships navigating through the area, protecting unilateral PRC claims to terrain and features under claimancy by other states.[33] In the Taiwan Strait, China has conducted large-scale military exercises simulating blockades and missile strikes—actions meant to rehearse for escalation rather than peaceful competition.[34] China has weaponized access to its market and deployed capital to harvest vital intellectual property. Meanwhile, Russia has not only invaded Ukraine, but continues to engage in acts of sabotage in Europe that target defense companies. The Russian military has also flown drones into Poland, while its ballistic missiles have veered off course to impact on allied territories. Moscow has also invested diplomatic capital to prop up BRICS, and openly pushed for currency alternatives to the U.S. dollar. And Russian security services and their co-opted criminal hackers have been behind some of the most severe hacks of U.S. government systems. Iran, on the other hand, has actively assisted the Houthi terrorists with intelligence and missiles to attack U.S. naval and merchant vessels in the Red Sea, and threaten the free flow of commerce. Iran has also developed, armed, trained, and financed a wide array of terrorist groups in Iraq, Syria, Lebanon, and Yemen, leveraging them to create weak states in each and as an attack force against the United States, Israel, Saudi Arabia, and other countries in the region. Iran has also actively sought to conduct assassination operations in the United States, including against senior leaders of the U.S. government, while using cyber operations against both government and civilian targets.

These are just some illustrative examples of confrontational actions that China, Russia, and Iran have undertaken over the past years. But the case is clear, the United States does not find itself in the midst of a sports-like competition. It is confrontation—with the real possibility of transitioning to a crisis and conflict.

The picture is clear: technology is accelerating, adversaries are adapting, and the boundaries between peace and war are eroding. The task ahead is to translate insight into posture—choosing a strategy that exploits U.S. advantages, blunts adversary strengths, and can be executed at speed and scale. Part 3 turns squarely to this challenge. It lays out the major strategic pathways available to the United States and weighs the advantages, drawbacks, and long-term viability of each.

---

[31] Ryan Lucas, Wray Warns Chinese Hackers are Aiming to 'Wreak Havoc' on U.S. Critical Infrastructure, NPR (2024).

[32] David Sanger, Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?, New York Times (2023).

[33] Aaron-Matthew Lariosa, Chinese Frigates Harass Philippine Navy Warship Near Scarborough Shoal, USNI News (2025).

[34] Huizhong Wu & Johnson Lai, Chinese Military Conducts Large-Scale Drills Around Taiwan, Associated Press (2025).

PART THREE

America's Strategic Choices

The United States now stands at the threshold of a new geopolitical era—one defined by intensifying great power confrontation, rapid technological disruption, and the resurgence of authoritarian powers determined to rewrite global norms. The assumptions that once underpinned American security policy are being challenged in real time. As this volatile, confrontational international environment takes shape, Washington must carefully choose its next strategy. Below, we outline some of the potential strategic choices, provide an assessment of benefits and drawbags of each, and recommend what we judge to be the most viable choice.

Hyperpower

With the close of the Cold War, the United States experienced an era of unrivaled—and historically unprecedented—power. With the collapse of the Soviet Union, the United States faced no serious rivals. Its military could simultaneously defeat, in a conventional fight, any plausible combination of potential adversaries anywhere on the globe. This hyperpower era offered unparalleled strategic flexibility. The United States could project power rapidly, dissuade other nations from taking unwelcome actions, and enforce norms without the counterbalancing behavior that had defined the Cold War. Deterrence was achieved through the sheer disparity of American capabilities in every domain. Washington enjoyed the luxury of strategic initiative, and setting the global agenda on terms largely favorable to its interests.

Today, that hyperpower era is long past—at least in the military domain. In part, this is due to the rising strength of America's adversaries. China's sustained economic growth and military modernization have transformed it into a viable peer competitor. Adversaries' investments in asymmetric capabilities (like precision munitions, cyber weapons, and anti-satellite systems) have eroded America's historical advantages and now threaten our reliance on legacy power-projection platforms. At the same time, the United States has overinvested in some regions of the world—particularly the Middle East, as well as Europe to a lesser extent. Meanwhile, bureaucratic inertia led the Pentagon to keep pouring money into slightly improved—but vastly more expensive—versions of the similar core capabilities. The result is a world where American military power is no longer supremely ascendant. The U.S. military would struggle to simultaneously fight

two major wars, and would be hard pressed to defeat its pacing challenge in the Indo-Pacific region.

Overmatch

As the United States' ability to remain the world's unchallenged military power faded, it fell back on an overmatch strategy. Under this concept, even if the United States could no longer defeat all global adversaries simultaneously, it could still overpower any single adversary—including China—individually. The overmatch strategy promised victory by pledging to maintain or even grow the size and capability of the American military to such a degree that any enemy would fear provoking its overwhelming wrath.

However, the overmatch strategy has shown clear limits. China and Russia have invested in new technologies and tactics that undercut the traditional strengths America has invested so heavily in. North Korea has developed a nuclear arsenal, while holding much of South Korea at risk of destruction. Iran has pioneered mass drone production, has developed a robust arsenal of missiles, and continues to maintain a network of proxies that threatened a range of U.S. interests—from embassies in the region, to the free flow of commerce. U.S. Navy admirals most certainly recognize that American aircraft carriers can no longer safely operate their air wings within strike range of the Chinese mainland. American strategic planners likely worry about the vulnerability of our critical airbases and logistics hubs on Okinawa and Guam under China's massive arsenal of ballistic, cruise, and hypersonic missiles. Meanwhile, lessons from the battlefields of Ukraine are rapidly advancing Russia's UAV fleet and the sophistication of its tactics, techniques, and procedures, while China has become the leading producer and exporter of drones.

Historically, military strength has been measured by counting the number and types of military equipment on each side and then comparing such orders of battle. However, this approach no longer captures the true correlation of forces. In a world where military equipment will be destroyed in massive quantities and will evolve rapidly over the course of any conflict, any military net assessment must also consider a nation's potential to evolve and adapt its military equipment and its ability to quickly scale up the ability to produce and deploy those innovations. We cannot assume that we will be able to wage a quick and decisive war on a peer competitor, particularly in a geographic terrain that favors the adversary. Thus, the weapons a nation can produce before the conflict ends have as much value as the weapons they possess at its start. This is now the decisive measurement of a country's strategic depth.

Isolationism / Restraint

At the opposite end of the policy spectrum, some policy experts have suggested the United States pursue a strategy of restraint and isolationism, in large part as a reaction to decades of engagements in the Middle East, free riding by select allies and partners, and deteriorating public debt in the United States. From their perspective, decades of interventionist foreign policy have yielded questionable or intangible returns, entangling the United States in costly conflicts with limited strategic benefit. America's underwriting of global security has burdened the American taxpayers and servicemembers, while other countries have focused on building their social and medical services, or developing energy and trade ties that are self-defeating over a medium-term. Persistent challenges at home—including an expanding national debt, infrastructure decay, and deindustrialization—have sapped the political will for a military buildup. Advocates argue that a more restrained posture would allow the United States to rebuild national strength and prosperity, reduce overextension, and build a hemispheric fort that stretches from Greenland in the north to Chile in the south. This orientation does not necessarily signal full disengagement but reflects a growing desire to reassess traditional assumptions about America's role in the world, prioritizing homeland security, and emphasizing selective involvement and a renewed focus on core national interests.

The resurgence of restraint and isolationist sentiment in U.S. foreign policy reflects legitimate concerns about overextension, domestic priorities, and public skepticism toward international commitments. Yet, while a recalibrated global role may yield benefits, a wholesale retreat from international engagement poses significant national security risks. Four risks in particular stand out.

First, an isolationist turn in American foreign policy would weaken America's ability to deter its enemies. For over seven decades, U.S. global presence and alliance commitments have served as a cornerstone of deterrence against hostile actors. The credibility of U.S. security guarantees, reinforced through forward deployments, joint exercises, and economic partnerships, has discouraged aggression and fostered stability. The result has been the longest peaceful era in European history and a similarly pacific stretch for the major industrial economies of East Asia. An American retreat could invite aggression by its enemies worldwide, not necessarily against the homeland, but most certainly against geographies, assets, and nations that are fundamentally important to American prosperity.

Second, strategic disengagement by the United States would create vacuums in critical regions—voids that adversaries like China, Russia, and Iran would eagerly fill, if not necessarily with their presence, then with their disruptive activities and actors. These bad actors would not merely fill this space with influence; they would actively reshape the global balance of power to undermine American interests. From expanding territorial claims and building anti-access military

capabilities to forging coercive economic dependencies, adversaries use these openings to weaken America's national security, undermine its economic prosperity, and limit America's ability to respond effectively to emerging threats. Strategic disengagement may offer short-term relief but risks long-term disaster.

Third, strategic disengagement can create space for national security threats to gather strength. As the United States learned from the hard-won lessons of the First and Second World Wars, as well as state failure in the Middle East at the beginning of this century, threats abroad do not stay contained. By the time direct attacks forced American military involvement in those conflicts, enemy strength had grown to the point where it required a massive commitment of American power to defeat their aggression. Early, decisive action—or even better, the ability to deter enemies before they act—is far less costly than delayed intervention.

Fourth, an isolationist foreign policy would undercut America's economic strength, weakening both the resilience of its supply chains and its ability to secure critical resources. Global engagement has long enabled the United States to shape the rules of international trade, invest in developed and emerging markets, and diversify the sources of essential inputs—from semiconductors and rare earth minerals to pharmaceuticals and energy. Retreating from these relationships would allow competitors to lock in exclusive access to these strategic assets, while leaving the United States vulnerable to chokepoints, shortages, and coercion. Disengagement would forfeit key opportunities to forge new trade and innovation partnerships—particularly in the Indo-Pacific—precisely at a time when adversaries are aggressively expanding their economic influence.

Major conflicts across the globe have always eventually drawn American intervention, even when the American government has fervently tried to avoid becoming entangled in them. There is little reason to believe that future conflicts between major powers would unfold any differently. Ultimately, retreat offers no guarantee of security; instead, it simply presents a different and untested form of danger.

Offset

If the days of hyperpower are gone, overmatch is unattainable, and isolationism risks inviting self-defeat, what may a viable strategic choice look like?

To meet the moment, we recommend that the United States military adopt an offset strategy. Offset strategies are strategies that tend to leverage technological innovation to develop unique capabilities and qualitative strengths that can be applied against an adversary's weaknesses or to nullify its quantitative strengths. During the early days of the Cold War, American offset strategies enabled the United States to leverage nuclear weapon superiority to offset Soviet numerical advantage in Europe. In concluding years of the Cold War, American offset strategies

leveraged the development of sophisticated intelligence, surveillance, and reconnaissance systems, with stealth technology, and precision guided munitions to hold adversary forces at risk, including Soviet troops. In other words, the United States leveraged technological superiority and innovative doctrines as a force multiplier to counterbalance the Soviet Union's conventional numerical advantage in Europe and globally. By investing in advanced capabilities and integrating them into its defense posture, the United States maintained credible deterrence while avoiding a costly build up of large formations. While the specific technologies and tactics changed over time, each offset strategy pitted unique American strengths against critical Soviet weaknesses to deter aggression through the most effective and efficient means.

The Offset-X Evolved that we are proposing provides a strategy for the United States military to counter People's Liberation Army's strengths without engaging in a costly and risky attempt at a symmetrical arms race or escalation. Rather than trying to overmatch China ship-for-ship or missile-for-missile, the U.S. can invest in capabilities that undermine the foundation of China's anti-access/area denial and information dominance strategies. Importantly, an offset strategy could be more sustainable over the long term. Rather than a resource-intensive buildup, it emphasizes high-leverage investments that can be scaled with allied contributions and adapted over time. This approach encourages innovation while avoiding the risks of entrapment or overextension. Crucially, it maintains the initiative—forcing China to respond to American moves rather than allowing it to continue to dictate the pace and character of *Conflict*. Ultimately, only an offset strategy offers a viable path for the United States to preserve its military advantage over the PRC, rapidly counter PRC moves, and fully leverage America's private sector strengths and ingenuity.

Having weighed the spectrum of strategic pathways—from renewed bids for primacy to calls for strategic restraint—Part 3 converges on a central conclusion: an Offset Strategy can better exploit U.S. innovation strengths and impose intolerable dilemmas on a pacing adversary that now rivals America on capabilities. This choice, however, is not self-executing; it must be operationalized, institutionalized, and funded before the window of advantage closes. Part 4 lays out critical steps the United States should take to achieve success with an offset strategy.

PART FOUR

Achieving Offset

America's ability to *achieve* strategic offset will hinge not on any single breakthrough but on a system-wide undertaking that fuses technology dominance, production rejuvenation, budgetary focus, and institutional boldness. This section lays out that undertaking: outlining the pillars of a new Joint Warfighting Concept to guide America's future concept of operations; proposing a dedicated commitment of resources and attention to sensing, artificial intelligence, and autonomy; nurturing an industrial base designed for surge rather than stockpile; undertaking institutional reforms to accelerate innovation and position the U.S. military to fight in new domains; and turning allied cooperation and continuous forward presence into a state of dynamic deterrence. It is, in effect, the operations order that converts strategic intent into sustained, scalable advantage.

Future Joint Warfighting Concept: Achieving Information, Decision, and Lethality Advantage

The United States faces a deteriorating security environment, threatened by a coalescing group of adversaries, with principal antagonists being China, Russia, Iran, and North Korea. This deterioration is currently most acute in the European theater, where Russian invasion of Ukraine and threats to European security have undermined enduring American interests. But the deterioration has the potential to spread to and be even more consequential in the Indo-Pacific theater, where China's growing military capabilities and assertiveness threaten regional stability and U.S. interests. At the same time, technological advances—from ubiquitous sensors and big data to artificial intelligence and autonomy—are changing the character of warfare at an unprecedented pace. History shows that those who best adapt to and harness such changes gain the greatest advantages in battle. In response, SCSP proposes an outline for a Joint Warfighting Concept (JWC) to serve as a roadmap for how the Joint Force should prepare to fight and win against adversaries across all domains. This JWC is *threat-informed* and *theater-focused*—prioritizing China as the pacing threat and the Indo-Pacific as the primary theater of effort—and it provides an integrated vision to maintain U.S. warfighting overmatch.

Core Organizing Principles: The JWC is built around three core pillars of advantage that the future Joint Force must achieve: (1) Information Advantage, gained by proliferating sensors and

data across all warfighting domains; (2) Decision Advantage, enabled by leveraging AI to observe–orient–decide–act faster and more effectively than the adversary; and (3) Lethality Advantage, generated by fielding autonomous capabilities at hyperscale to deliver overwhelming mass, effects, and combat power with lower cost and risk. Together, this triad of capabilities can enable U.S. and allied forces to sense, decide, and act with unmatched speed and effectiveness—ensuring any conflict is fought on our terms, not the enemy's. The sections below detail each pillar of the concept, illustrating how they work in concert to deter aggression or win decisively if conflict occurs.

Proliferated All-Domain Sensors: Information Advantage

Information advantage has always been a precursor to victory. In the modern era, achieving it requires harvesting data from every domain of warfare (land, sea, air, space, cyberspace, and the electromagnetic spectrum). This entails deploying vast numbers of sensors—from satellites and high-altitude drones to undersea hydrophones and cyber monitoring—all linked via resilient networks. The goal is to attain "real-time awareness across all domains . . . understanding emerging events, anticipating the future, discerning operational anomalies, and maintaining decision advantage."[35] In a conflict with a high-tech adversary like China, such omnipresent sensing is crucial to perceive threats coming, to pierce the fog of war, and to develop a faster and dynamic understanding of the battlespace than the adversary.

The JWC proposed here defines "information advantage" as the rapid collection, processing, and sharing of information using advanced technologies across all warfare domains. Achieving this requires an advanced command-and-control (C2) ecosystem – such as the Joint All-Domain Command and Control (JADC2) – which connects "any sensor to any shooter" via a so-called kill web.[36] Instead of siloed service-specific sensor-to-shooter chains, the kill web envisions a meshed network where data from any sensor (for example, a Navy ship's radar or an Air Force UAV's camera) can be routed to any shooter or decision node that needs it. Whoever can see the battlespace first can decide and act first—and thus seize the initiative.[37] In addition, the proposed JWC goes a step further and proposes that sensors also observe changing battlefield dynamics, and feed insights back to the R&D labs and manufacturing sites where capability enhancements can be pursued and scaled rapidly. In other words, sensor-to-shooter web must be reimagined and expanded to incorporate elements of strategic depth at home.

[35] Scott Berrier, Deterring Chinese Aggression Takes Real-Time Intelligence, Atlantic Council (2025).

[36] Scott Berrier, Deterring Chinese Aggression Takes Real-Time Intelligence, Atlantic Council (2025).

[37] Jack Shanahan, Reimagining Military C2 in the Age of AI - Revolution, Regression, or Evolution, Special Competitive Studies Project (2024).

However, gaining a sustained information advantage against a formidable adversary like China is no simple task. China and other rivals will fiercely contest the information domain—through jamming, cyber attacks, anti-satellite weapons, and deception— to deny the American military the ability to see and communicate. The proposed JWC therefore underscores that our sensor networks and data links must be resilient, able to "fight through" disruption and continue providing actionable information even under attack. This entails building redundancy and adaptability into our systems: a distributed, self-healing network that can reroute data if one pathway is cut. It also means embracing an operational mindset that does not assume perfect connectivity. The United States cannot harbor expectations of complete information dominance and should instead focus on connecting enough sensors to enough shooters under combat conditions. Degradation and disruption are endemic to modern warfare, so military networks must degrade gracefully rather than fail catastrophically. By deploying a dense web of sensors and communication nodes—many of them small, mobile, or low-cost—the Joint Force can ensure that no single attack or failure blinds our entire force.

Consider a crisis in the Indo-Pacific. A constellation of small satellites spots unusual movements of adversary's missile units on land; undersea sensors detect submarines leaving port; and cyber intelligence flags increased chatter on adversary networks. These feeds funnel into an AI-enabled fusion system that correlates and deconflicts the multi-domain inputs. Thanks to a resilient communications mesh (including satellite links, high-frequency radio, and line-of-sight datalinks), these data points reach all relevant forces in seconds, despite the adversary's attempts to jam or spoof it. Armed with the right information, U.S. and allied commanders begin the process of capitalizing on Information Advantage to generate "decision-quality" information and Decision Advantage. This is the power of information advantage: turning the proliferation of sensors and data into a clarity of insight that the enemy cannot match.

Information Advantage in action can take many forms. It can be knowing that terrain is traversable when your enemy believes it is impassable. It can be accumulating and processing the data required to more precisely realize that the weather tomorrow will be favorable for an invasion when your enemy believes there will be cloudy skies and stormy conditions. It can be knowing the size, strength, and disposition of the enemy or knowing whether enemy reinforcements will arrive in time for the battle or a day too late. It can be knowing the exact location, speed, and direction for every enemy aircraft or naval vessel. Regardless of the form, properly leveraged, Information Advantage can be the difference between victory and defeat.

Artificial Intelligence: Decisional Advantage

Information by itself is not enough—it must translate into faster, better decisions than the adversary's. The Decision Advantage pillar of the JWC focuses on leveraging artificial intelligence to compress and outpace the enemy's OODA loop (the observe–orient–decide–act process). In essence, if we can process battlefield data and coordinate responses at "machine

speed," we can seize the initiative and keep the enemy off-balance. As former Deputy Secretary of Defense Robert Work argues, achieving a warfighting edge will require "AI-enabled algorithmic operations"[38] that allow our battle networks to operate better and faster than those of the adversary. The Joint Force must field AI-powered, human-machine collaborative networks to sift through intelligence, identify targets, propose courses of action, and drive effects and outcomes—all far faster than human staff processes alone.

The end state is a force that makes consistently better decisions, faster than any adversary. Concretely, this might involve AI-driven decision aids that can instantaneously analyze incoming sensor data, compare it to historical patterns, and recommend optimal responses (for example, suggesting the best interceptor for an incoming missile, or flagging which unfolding enemy maneuver is a feint versus the main attack). It also involves pushing decision authority downward and outward—empowering edge units and automated systems to act on commander's intent without waiting for higher headquarters, especially if communications are degraded. This concept of "command autonomy"[39] means front-line elements (human or machine) can carry on the fight and coordinate even when cut off from centralized control, using pre-defined doctrine and on-board AI to guide them. Such distributed decision-making not only adds resiliency but also speeds up responses dramatically, as decisions are made at the lowest possible level with the best available information. Command autonomy, mission command, and command by negation have always provided tactical and operational advantages for the U.S. military. Technology will only enhance and emphasize the criticality of this comparative, military advantage.

Achieving decision advantage will require significant training and cultural adaptation, not just new tech. The Joint Force needs to build confidence in and exploit AI-enabled systems, training with these systems so that human operators and commanders understand how to best supervise and employ them. Crucially, humans remain directly involved in strategy formulation and intent-setting, while machines handle rapid data crunching and even some tactical decisions. This human–AI teaming can yield decisions that are superior to those made by either alone. As a result, American forces would more rapidly sense and understand the battlespace, develop a common operating picture, generate and decide upon courses of action, and disseminate those decisions to forces for execution. In short, speed becomes a weapon in itself: by the time an adversary reacts, our forces have already shifted to the next move.

Imagine a U.S. carrier strike group at sea and an Army Patriot battery on allied soil are monitoring a tense situation. Suddenly, a swarm of adversary anti-ship missiles launches at the strike group, while land-based ballistic missiles threaten the Army battery. In a legacy model, each unit might handle its threat separately, relying on human controllers to coordinate—an inherently slow

[38] Robert Work, A Joint Warfighting Concept for Systems Warfare, Center for a New American Security (2020).

[39] Robert Work, A Joint Warfighting Concept for Systems Warfare, Center for a New American Security (2020).

process. Under an AI-enabled C2, however, the joint force reacts in moments. Networked sensors alert an AI battle manager, which instantaneously prioritizes the threats and suggests a synchronized response. Air Force fighters on combat air patrol are retasked *within seconds* to intercept launch platforms identified by space assets; Navy Aegis systems automatically launch layered interceptors at the incoming missiles; the Army's Patriot battery receives targeting data from Air Force radars and prepares counter-fire on enemy launch sites.

All of this happens with minimal manual intervention—the AI orchestrator has already weighed feasible options and presented commanders with the best course of action at machine speed. The humans approve the plan (or adjust if needed), and the response is executed almost *immediately*, before the enemy's missiles reach their targets. Simultaneously, the Joint Force's cyber and electronic warfare units (guided by AI analysis of enemy communications) launch proactive measures to disrupt the adversary's command networks, further slowing their decision cycle. This vignette illustrates how AI-driven decision-support tools and integrated kill-web networks can yield a decision-making and action speed that the enemy simply cannot match. In warfare, time is life—and by stealing time from the adversary, decision advantage translates directly into battlefield advantage.

Autonomy: Lethality Advantage

While better information and faster decisions set the stage, victory in combat still requires the ability to deliver lethal effects on the adversary. The Lethality Advantage pillar of the JWC envisions leveraging autonomous systems and new manufacturing paradigms to maximize combat power in a cost-effective, sustainable way. In practical terms, this means rebalancing from today's reliance on a limited number of ultra-expensive, manned platforms toward a mix of abundant, low-cost, autonomous or semi-autonomous systems (drones, robotic vehicles, smart munitions, etc.). By hyperscaling production of such systems—i.e., harnessing advanced manufacturing, modular design, and commercial components to produce massive quantities of warfighting assets quickly and cheaply—the United States can restore strategic depth and capacity for a high-intensity conflict. This is crucial in light of the China threat: a war in the Indo-Pacific could involve intense combat losses, and the side that can continually replace and surge its combat power will have the edge.

A driving objective of this approach is to flip the cost curve of military competition. Simply put, we seek to impose higher costs on the enemy than on ourselves with every exchange. Today's paradigm often favors those who attack us: for example, an adversary can launch a cheap drone or missile, forcing us to fire an expensive interceptor or risk high-value assets. The autonomy-and-mass approach *reverses* this asymmetry. Using cheaper, attritable platforms in large numbers, paired with AI for intelligent tactics, including swarming, can dramatically raise the enemy's expenditures (and dilemmas) while lowering our own. It also reduces risk to our personnel—losing a drone does not cost human life or political capital the way losing a crewed jet

or ship does. In essence, autonomy at scale allows us to trade *machines for enemy missiles* or *machines for time*, preserving our human forces for when they are truly needed.

Warfare is evolving from individual human–machine teaming towards "swarm vs. swarm" engagements, where both sides will employ large autonomous formations. Human-Machine Teaming (HMT)—such as a pilot controlling wingman drones or an infantry unit supported by ground robots— is an important stepping stone and remains part of the concept. But the ultimate vision goes further: "machine–machine teaming" in which groups of unmanned systems collaborate with minimal, direct human control. In the air, this could mean dozens (or hundreds) of AI-driven drones autonomously coordinating a complex attack; at sea, unmanned submersibles might hunt in packs; on land, robotic vehicles could execute ambushes or guard flanks largely on their own. The side that better integrates and directs these swarms will enjoy tremendous advantages. A force adept at such swarming can saturate enemy defenses, exploit gaps with speed, and dynamically adapt by learning on the fly. It can also better survive attrition: if some drones are lost, the rest re-route and press on. The aggregate effect is greater than the sum of parts. Indeed, the operational system that excels in human-machine *and* machine-machine teaming will have a marked edge over one that does not. Advantages include: the ability to learn and iterate tactics rapidly, better situational awareness via distributed sensors, higher tempo (approaching machine speed) to outpace enemy reactions, and improved efficiency and precision in applying firepower. All of this translates to greater lethality on the battlefield.

To realize this lethality advantage, the U.S. military will need to embrace new manufacturing and development practices, in addition to having the best software to power autonomous systems. The Department of War is beginning to partner with industry to "hyperscale" modular defense production, adopting commercial best practices for speed and volume. The result should be a nimble production line that can rapidly surge output as demands dictate—providing a surge capacity analogous to the "arsenal of democracy" in World War II, but for smart drones, sensors, and missiles. Such capacity would give the United States a strategic depth it currently lacks: if a conflict breaks out in the Western Pacific, we would have the means to continuously replenish losses and pour additional autonomous assets into the fight, whereas an enemy exhausting its high-end missiles and platforms would struggle to do the same. This not only strengthens deterrence (by making clear to adversaries that they cannot hope to win a long fight of attrition) but also minimizes risk to the mission if war comes because our combat power will not evaporate after the first exchange. In summary, by pairing AI-enabled autonomy with mass production and adaptability, the Joint Force can achieve a lethality advantage that maximizes combat effectiveness and efficiency while driving down cost and risk to our warfighters.

In summary, the Joint Warfighting Concept proposed here articulates a vision of a U.S. Joint Force that is information-rich, decision-fast, and overwhelmingly lethal—all tailored towards prevailing against the pacing threat from China in a contested Indo-Pacific scenario. By networking proliferated and meshed sensors across all domains into a resilient "combat cloud,"

the force gains an information advantage that denies any sanctuary to the adversary and enables allied forces to see, understand, and act first. By harnessing AI to accelerate the observe-orient-decide-act cycle, the force gains a decision advantage—acting inside the enemy's tempo and dictating the terms of engagement. By fielding autonomous capabilities at hyperscale, the force gains a lethality advantage that can defeat the enemy's systems at lower cost and fewer casualties, flipping the traditional cost-exchange ratio in our favor. Connecting these pillars are the enablers of assured connectivity, which together form the digital and physical backbone of 21st-century warfare.

Dynamic Deterrence

Embracing the core pillars of this proposed JWC would enable the United States to adopt a new strategy translating its principles into operational effects. The need for this new strategy is most urgent in the Western Pacific, where American allies and partners contend with China's tactics of constant confrontation. Today, when America seeks to respond to China's coercive activities, its force design compels it to deploy scarce and expensive assets which can only be spared long enough for a brief transit through the region. These limitations inherent to our current posture prevent us from being present at the point of confrontation to reassure our friends or from staying long enough to learn how to confront, contest, and combat malicious Chinese behavior; all we can do is watch from afar.

Instead, the United States must respond to Chinese coercion with a strategy of dynamic deterrence. Dynamic deterrence flips the current cost-imposition dynamic under which the United States deploys high demand, low-density assets to counter cheaper and more plentiful adversary systems. Rather, the United States would field large numbers of cheaper but smarter autonomous vehicles sufficient to persistently deploy in the underwater, surface, air, and land domains and to flow additional capabilities as needed to scale up its response on demand. These scalable, autonomous forces would maintain sea lines of communication, reassure our allies and partners through enduring presence, and counter current and future PLA confrontation and coercion campaigns. Large quantities of autonomous equipment would offer multi-axis force presentations and create operational dilemmas for our adversaries. Equally, being present and scalable empowers the United States to seize the initiative and capture operational momentum from its adversaries when desired, as desired.

Additionally, adopting a policy of dynamic deterrence would invigorate two feedback loops. For one, conducting continuous operations to counter Chinese activity would spur military planners to adapt their tactics and procedures quickly enough to operate inside their adversary's OODA loop and adaptation cycle. In addition, operating in proximity to Chinese forces would develop more rapid feedback loops between the engineers and researchers who are developing new technological capabilities and the servicemembers utilizing them in day-to-day operations. If a conflict begins, Chinese forces will adapt to American tactics and find weaknesses in the

capabilities of American weapon systems, just as Russian forces have learned to adapt during their invasion of Ukraine. While operating in close contact does bring a higher risk of unintended actions or miscalculations, the benefits are worth the tradeoffs. The Department of War cannot wait for the shock of combat to force them to abandon the pre-planned responses. Developing and enabling a culture of adaptation now, in an era of constant confrontation, would ready credible combat power under duress.

Executing a strategy of dynamic deterrence is not limited to actions in the physical domain. In the digital realm, the United States has failed to punish Chinese provocations for far too long. Self-imposed limitations have allowed adversaries to operate with near impunity, exploiting U.S. infrastructure, stealing sensitive data, and undermining strategic interests without meaningful consequences. To restore deterrence, the United States must be willing to take calculated risks and employ more aggressive cyber, information, and cognitive warfare—to demonstrate clear and compelling consequences for malicious activity. This does not mean reckless escalation, but rather a deliberate, proportional use of offensive capabilities to impose costs on Chinese state and state-aligned actors. By leveraging its technical expertise and intelligence capabilities, the United States can disrupt hostile operations, expose malign actors, and degrade their asymmetric toolkits before they are used. Confronting China in the digital realm would provide the same real-time feedback loop to further America's cycle of adaptation. These hard-won lessons will prove invaluable in the case of any direct conflict between the United States and China.

Dynamic deterrence would put the Department of War in a more appropriate footing—challenging and disrupting confrontational actions of our adversaries. In the physical and digital realms, it would leverage the tactical triad of sensing, AI, and autonomy to deliver informational, decision, and lethal advantage. The United States cannot afford to wait—the evolution in the character of warfare is outpacing existing force designs and will continue to do so in an era requiring constant adaptation. Dynamic deterrence offers an initial foothold to that end and an operational pillar to a winning offset strategy.

Adopt a Production Mindset Instead of a Stockpiling Mindset

Since the 1990s, the Department of War has developed an acquisition process optimized for a world that no longer exists. At the time, America's dominant technological advantage combined with the lack of any plausible peer competitor implied that wars would be quick and decisive, and that military technology would improve at a relatively slow rate. Procured equipment would remain in service for decades before eventually being replaced by slightly improved versions of

the same systems.[40] Consequently, acquisitions requirements reflected a stockpiling mindset which prioritized designing these systems to maximize their ability to be sustained over an extended service lifetime.

But the world has changed. For one, the United States now faces a peer competitor whose military poses an escalating threat to the U.S. military. As a result of China's ever-growing capabilities and a robust manufacturing base, a potential future conflict against the PLA could take one of two forms—a quick and very sharp war or a protracted conflict. In either instance, Beijing would be right to conclude that the United States lacks the industrial strategic depth to wage a high-intensity or an extended war. Additionally, evolving technologies—which rapidly improve and just as rapidly make older versions of the technology become obsolete—have become increasingly important tools for warfare. As a result of these two trends, the Department of War should no longer assume that its equipment will remain in service for many years after its initial acquisition. If a conflict were to erupt, much of the purchased equipment would be destroyed in battle; or become obsolete against evolving technologies that can be rapidly iterated and adapted. Thus, the stockpiling mindset which fit the established technologies of the post-Cold War era is no longer the optimal way to acquire evolving ones.

To be clear, this is not to argue against maintaining stockpiles of critical weapons or resources—they remain essential for readiness. Rather, our concern is with the *mindset* that has guided defense acquisitions since the Cold War: one that assumes longevity, incremental updates, and the indefinite relevance of expensive platforms. That mindset no longer fits today's strategic or technological realities.

Instead, the Department of War must return to a production mindset when acquiring evolving technologies. Rather than prioritizing the ability to maintain equipment over decades, requirements should emphasize the ability to manufacture the equipment quickly, at lower costs, and with the potential to rapidly scale up the production volume. These prioritizations should predominate even if that requires making tradeoffs with maximum performance characteristics. For evolving technologies, there is no reason to pay a premium for exquisite performance today when a new generation with substantially improved performance is just a heartbeat away.

Just as importantly, emphasizing ease of production ensures that the Department of War maintains a latent manufacturing capacity to produce the equipment during a time of crisis. Because any initial stockpiles of weapons and platforms would quickly be expended during a

[40] Stephen Losey, US Air Force Warns of Aging Fighters, Poor Purchasing Efforts, Defense News (2022); Caitlin Kenney, Navy to Keep Four Aging Destroyers Beyond Their Service Lives, Defense One (2023).

protracted, high-intensity war,[41] it will be essential that the United States retain the potential to quickly scale its ability to produce critical military hardware. By engendering flexibility and resilience in production processes and techniques, the Department of War can minimize production bottlenecks and better prepare itself to tap into America's potential for creation.

Dominate Evolving Technology

For decades, technology—in addition to the exceptional skills of our warfighters—have defined America's military dominance. Over forty years ago, America's development of stealth aircraft, precision-guided munitions, space-based communications, ISR, and PNT assets, and the command-and-control networks coordinating their effects left potential American enemies in despair at the prospect of facing these powerful forces on the battlefield.[42] Even today, many American technologies face no effective parity. The strengths delivered by these established technologies remain a bedrock of U.S. strategy.

However, this very success has created a stark dilemma. Continuing to upgrade and produce established systems has become exceedingly expensive, and each new generation yields diminishing returns in capability per dollar spent.[43] These trends have reached a crisis point: the skyrocketing cost of replacing fighters, bombers, aircraft carriers, and armored vehicles is crowding out critical investment in the next generation of evolving technologies.[44] Meanwhile, America's adversaries—largely unencumbered by past capabilities—are rapidly developing and fielding new capabilities that are purposely designed to negate and even overtake the U.S. military's advantages. The United States cannot abandon its current arsenal, but it also cannot afford to neglect the transformative potential of emerging technologies. America must win the future, not just perpetuate the present.

To decisively unblock America's innovation pipeline, the Department of War should immediately redirect greater procurement funding toward *evolving technologies*. These are no longer speculative laboratory experiments—they are combat-ready capabilities already delivering decisive effects in modern conflicts. The Secretary of War must require that each service allocate

[41] Seth Jones, Empty Bins in a Wartime Environment: the Challenge to the U.S. Defense Industrial Base, Center for Strategic and International Studies (2023); Stacie Pettyjohn, et al., Dangerous Straits: Wargaming a Future Conflict over Taiwan, Center for a New American Security (2022).

[42] Shawn Brimley, Offset Strategies & Warfighting Regimes, War on the Rocks (2014).

[43] Gregory Allen & Isaac Goldston, Updating Augustine's Law: Fighter Aircraft Cost Growth in the Age of AI and Autonomy, Center for Strategic and International Studies (2024).

[44] Michael Brown, The Empty Arsenal of Democracy, Foreign Affairs (2025).

at least 20% of its procurement budget to these evolving technologies. This shift will drive two essential outcomes:

- First, it will rescue breakthrough capabilities from the so-called "Valley of Death." Right now, too many promising technologies wither after initial success because established technologies absorb the available procurement funds. When their temporary R&D contracts run out, they tend to disappear.

- Second, devoting meaningful levels of procurement funding to evolving technologies sends a clear demand signal for private sector investment. Historically, the U.S. government has often played this role: for example, government purchases of aircraft for the Postal Service in the 1920s helped accelerate the growth of the domestic aviation industry,[45] while government purchases of semiconductors in the 1950s for the Department of War and NASA had a similar impact.[46] However, private sector companies and venture capital firms will not invest without a clear and stable demand signal from the government. R&D funding pipelines are too limited and too fragile to play this role; only a sustained investment of procurement funds will generate the necessary impact.[47]

Drive Credible Allied Capability

American allies and partners must significantly increase their investments in sensing, artificial intelligence, autonomy, and the supporting infrastructure necessary to deploy them at scale. As geopolitical threats intensify, allies and partners cannot risk lagging behind adversaries or America in capabilities that will determine informational, decisional, and lethality advantage. Investing in these capabilities is not merely about keeping pace with adversaries—it is about ensuring interoperability with U.S. forces, accelerating operational rhythms, and maintaining the strategic edge necessary to preserve regional stability in the face of rising authoritarian aggression.

But increasing spending alone is not enough. Allies and partners should spend their newly dedicated resources towards creating an integrated system of sensing, AI, and autonomy that can also operate at the pace and level of sophistication that America's will. When it comes to AI, in particular, this should happen at all levels of the AI stack. At the lowest level, each ally or partner

[45] Eunhee Sohn, et al., Technology Adoption and Innovation: The Establishment of Airmail and Aviation Innovation in the United States, 1918–1935, Strategic Management Journal at 3-35 (2024).

[46] Kira Fabrizio & David Mowery, The Federal Role in Financing Major Innovations: Information Technology During the Postwar Period in Financing Innovation in the United States, 1870 to the Present, MIT Press (2007).

[47] Aaron Mehta, Exclusive: Outgoing DIU Head 'Frustrated ... We're Not Supported' More by Big Pentagon, Breaking Defense (2022).

should specialize in the types of data they are collecting and curating to feed into the training of AI algorithms. Coordinating to assign distinct "data missions" would ensure each ally or partner brings unique value to the partnership and would accelerate the training of robust AI models capable of handling even the most obscure corner-cases. Additionally, American allies and partners could collaborate in shared data centers. Shared hardware and data sets accelerates the development of advanced models. Finally, the allies and partners will need to develop the simulation and training capacity to test that any AI models they develop will be interoperable with the AI algorithms being developed by the United States. By becoming centers of AI excellence rather than passive technology importers, U.S. allies and partners can transform themselves into vital contributors to the alliance's strategic edge.

Institutional Reforms

Joint Warfare and Innovation Command (JWIC)

At present, the Department of War is not fully organized to prepare for wars looming on the horizon. Responsibilities for future-force design and development are fragmented and scattered across the Department, diluting accountability and blunting progress. No single entity, below the Secretary of War, can be held responsible for forging a force that is as lethal and ready as it must be. While each military service branch continues to pursue its own modernization path, no unified body exists with the mandate, authority, and strategic focus to design and drive joint warfighting concepts for the all-domain conflicts of tomorrow. This must change—immediately.

One way to address this shortcoming would be for the United States to establish a Joint Warfare and Innovation Command (JWIC) as the dedicated entity within the Department of War responsible for preparing the U.S. military to fight and win future wars. The JWIC would fill the present gap by developing integrated operational concepts that reflect how wars will actually be fought—across domains, with human-machine teaming, in contested information environments, and at machine speed. Crucially, this command would not just be a think tank—like the Office of Net Assessments—or a reincarnation of the disestablished Joint Forces Command, whose mission remains unclear even in hindsight. Instead, JWIC would have the institutional weight to advocate for the resources needed to realize its vision and the authority to shepherd the development and acquisition of the technologies and capabilities required to bring that vision to life. Without such a command, the United States risks modernizing in fragments and incrementally—over-optimizing for yesterday's fights while underpreparing for those that lie ahead. To ensure a coherent, competitive, and future-ready force, the Department of War must unify concept development, resourcing, and innovation under one roof, with a singular focus on winning the next war.

Digital Warfare Corps and U.S. Digital Command (USDIGICOM)

Finally, the United States has persistently been unable to cope with sustained attacks by its adversaries in the digital domain. These attacks will only escalate as ever-more powerful AI systems come online. To combat this challenge, the United States should establish a Digital Warfare Corps within a newly formed U.S. Digital Command to defend its interests and maintain strategic superiority in the digital domain. As adversaries increasingly wage cyber operations, deploy advanced AI-enabled systems, and exploit data as a weapon, the United States must organize for this new battlespace with the same seriousness it applies to land, sea, air, and space operations. Just as important, it would serve as a powerful mechanism for recruiting, training, and retaining top-tier technical talent—individuals who might otherwise be lost to the private sector. By consolidating digital capabilities under a single command, the United States can shift from reactive defense to proactive dominance, shaping the digital terrain rather than merely surviving in it. Digital superiority will be decisive in future conflicts, and the time to build the institutions required to win in that domain is now.

Dedicated Innovation Budget

Despite the widespread recognition of the transformative potential that sensing, AI, and automation hold for the future of warfare, the Department of War has been slow to invest in their scaled implementation, particularly of AI and autonomy. Efforts remain fragmented, under-resourced, and often bogged down in bureaucratic red tape, leaving the United States vulnerable to more technologically agile adversaries. Reserving at least 1% of the Department of War's overall budget for a dedicated innovation budget would signal a serious commitment to overcoming these structural hurdles and institutionalizing technological adaptation. In an era where technological advantage is increasingly defined by speed, adaptability, and iteration, the rigid annual budgetary process is too slow and cumbersome to keep pace with commercial innovation or the tactics of agile adversaries. Granting the Secretary of War— in close coordination with the Chairman of the Joint Chiefs of Staff—discretionary authority over this innovation fund would enable the rapid launch of high-impact pilot programs, the scaling of promising prototypes, the strategic pursuit of evolving technologies, and the agility needed to operate within the reality of Congressional continuing resolutions. This modest but targeted investment would create an essential fast lane for defense innovation—allowing the Pentagon to act more like a 21st-century technology enterprise and less like a Cold War-era bureaucracy. If the United States is to maintain military-technological superiority, it must empower its leadership with the tools and flexibility to act at the speed of relevance.

Annex A: Offset-X Revisited

This annex revisits three core themes from the original Offset-X—**Distributed Operations**, **Human-Machine Teaming**, and **Software-centric Warfare**. We assess whether these concepts remain militarily decisive, evaluate the progress the Department of War has made toward realizing them, and survey the opportunities offered by emerging and evolving technology.

Distributed Ops

Key to Offset-X was the critical need to design the Joint Force as a distributed, networked force to deter near-peer adversaries, especially the People's Republic of China (PRC). The Services have made some significant progress toward this vision, but this progress is still far too slow and uneven given the existential threat posed by a formidable, lethal, and increasingly global People's Liberation Army (PLA).

Conceptual Foundation and Strategic Relevance

Offset-X prioritized building a force around software-defined systems, modular open architectures, AI-enabled command and control, and deeper integration with allies and partners. This approach directly counters the PLA's theory of "system destruction warfare,[48] which aims to cripple U.S. battle networks. Rapid experimentation was identified as critical to quickly fielding this new kind of force.

At the Service level, pragmatic applications of a distributed, network-based force design are taking shape in each Service's capstone operating concepts:

- **Army – Multi-Domain Operations (MDO):**[49] Emphasizes calibrated force posture, the Project Convergence experimentation series, and multi-domain formations to penetrate and defeat anti-access/area-denial (A2/AD) threats and enable joint all-domain warfare.

[48] Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare, RAND (2018).

[49] The U.S. Army in Multi-Domain Operations 2028, TRADOC (2018).

- **Navy/Marine Corps – Distributed Maritime Operations (DMO)[50] & Expeditionary Advanced Base Operations (EABO):[51]** Promote decentralization and autonomous action to generate operational unpredictability and resilience.

- **Air Force – Agile Combat Employment (ACE):[52]** Focuses on dispersal, mission command, and rapid maneuver by multi-capable Airmen to complicate adversary targeting and sustain combat operations from austere locations.

- **Space Force – Space Doctrine Publication (SDP) 3-0 (Operations):[53]** Defines spacepower as inherently network-based, highlighting the necessity of resilience, distributed sensors, and rapid command and control in a congested, contested domain.

The United States' theory of victory now hinges on credible deterrence, campaigning, and building enduring advantage to counter strategic threats from China and Russia—at range. The emerging Combined Joint All-Domain Command and Control (CJADC2)[54] approach and the new Joint Warfighting Concept (JWC) are critical to executing this strategic imperative.

CJADC2

The Combined Joint All-Domain Command and Control (CJADC2) initiative has been the most prominent and well-funded example of the Department of War acting to embrace distributed operations. CJADC2 serves as the connective tissue of the modern Joint Force—a data-centric, interoperable framework linking sensors, shooters, and decision-makers across space, air, land, sea, and cyber domains.

Initiated in 2019, CJADC2 has been a top Pentagon priority, envisioned as a system-of-systems combining software applications, integrated data, AI, and cross-domain concepts to give warfighters a decisional advantage. It will serve as the Joint Force's neural "backbone," enabling true integration of a distributed force. However, CJADC2 progress has been hampered[55] by the absence of a central organizing framework that can guide, track, and assess Service CJADC2-related investments to measurable goals and milestones.

---

[50] Defense Primer: Navy Distributed Maritime Operations (DMO) Concept, Congress.gov (2025).

[51] Expeditionary Advanced Base Operations (EABO), U.S. Marine Corps (2021).

[52] Agile Combat Deployment, U.S. Air Force (2022).

[53] Space Doctrine Publication (SDP) 3-0, Operations, U.S. Space Force (2023).

[54] CJADC2, U.S. Chief Digital and Artificial Intelligence Office (last accessed 2025).

[55] Defense Command and Control, U.S. Government Accountability Office (2025).

Service resource alignment has begun, though unevenly. The Marine Corps' Force Design 2030[56] invests in long-range precision fires, unmanned systems (including long-range unmanned vessels), and distributed logistics. Its 2024 update aggressively shifts away from legacy heavy formations toward smaller, faster, more lethal units. The Army is funding long-range fires, network modernization, and synthetic training environments as part of Project Convergence,[57] but many of its modernization programs won't fully field effects until the 2030s—leaving dangerous near-term gaps. The Air Force's new force generation model and a major funding infusion for ACE in FY25 (over $500 million)[58] signal a commitment to dispersed operations and readiness. The Space Force is integrating commercial capabilities and small satellites to build a resilient space architecture, though its doctrinal development is lagging relative to the threat.

The distributed, network-based force envisioned in Offset-X remains indispensable to deterring and defeating China in a high-end conflict. While each Service is making strides, the Joint Force as a whole must firmly entrench decentralization, resilience, and software-defined warfare as standard practice. Only by doing so can we close the deterrence gap and sustain our edge into the 2030s.

Human-Machine Teaming

Since the release of the Offset X report, the concept of human-machine teaming has only grown more relevant to military operations. Leaders in each of the military services have emphasized that developing effective human-machine teams will be critical to fighting and winning the wars of the future.[59] As a result, each of the military services has developed plans to field units combining humans and autonomous machines within the next ten years. These plans include the Air Force's intent to fly the Collaborative Combat Aircraft alongside manned fighters,[60] Army Futures Command's templates for Human-Machine Integrated formations,[61] and the Navy's

[56] 2024 Force Design Booklet, U.S. Marine Corps (2024).

[57] Project Convergence, U.S. Department of Defense (last accessed 2025).

[58] Michael Marrow, Air Force Wants to Retire 250 Aircraft as Part of $188B FY25 Budget Request, Breaking Defense (2024).

[59] Allyson Park, Mastering Human-Machine Learning Crucial for Air Force, Official Says, National Defense Magazine (2024); George Seffers, Gen. James Rainey: Man-Machine Integration May Revolutionize Combat Arms, Signal (2023).

[60] Jennifer DiMascio, U.S. Air Force Collaborative Combat Aircraft, Congressional Research Service (2025).

[61] Ashley Roque, Army Eyeing First Human Machine Integrated Formations in 2027, Common Controller for Robotics, Breaking Defense (2025).

preparation to integrate manned-unmanned teaming into its operations by 2030.[62] Lessons learned from the ongoing war in Ukraine should heighten the sense of urgency within the Department of War to adopt and integrate human-machine teams for the U.S. military.

Most current initiatives have focused on using autonomous equipment to perform the most dangerous tasks, avoiding trading "blood for first contact."[63] In practice, this means unmanned systems taking on high-risk missions such as reconnaissance, explosive ordnance disposal, logistics resupply under fire, or serving as decoys alongside crewed platforms. Programs like the Army's Robotic Combat Vehicle (RCV),[64] the Navy's Ghost Fleet Overlord,[65] and the Air Force's Loyal Wingman[66] exemplify this approach. These systems aren't meant to replace human warfighters but to complement them with new capabilities.

However, this cautious approach only scratches the surface of AI's battlefield potential. Recent experiments hint at far more transformative possibilities. In one example, the Army's XVIII Airborne Corps leveraged AI to dramatically speed up its kill chain, enabling the formation to dramatically scale up its ability to identify, prioritize, and engage targets with roughly 1% of the usual number of personnel required.[67] Similarly, AI tools have been instrumental in Ukraine's defense against Russia, accelerating targeting and decision cycles.[68] Yet despite these successes, such advanced applications of AI remain largely confined to isolated units. The vast majority of U.S. forces have yet to integrate these game-changing capabilities.

More importantly, the Services have yet to truly exploit the complementary strengths of humans and machines. Humans and AI excel at very different things, yet current concepts often treat machines as either mindless underlings or mere replacements for humans in undesirable roles. This mindset wastes the potential of artificial intelligence. To unlock the full power of human-machine teams, the Department of War must radically rethink force design. Machines should be

[62] Navy CNO Positive on MUM-T Operations by 2030s, Potomac Officers Club (2024).

[63] Strategic Landpower Dialogue: a Conversation with GEN James Rainey, Center for Strategic & International Studies (2024).

[64] Andrew Feickert, The Army's Robotic Combat Vehicle Program, Congressional Research Service (2025).

[65] Ghost Fleet Overlord Unmanned Surface Vessel Program Completes Second Autonomous Transit to the Pacific, U.S. Department of Defense (2021).

[66] Stephen Losey, How Autonomous Wingmen Will Help Fighter Pilots in the Next War, Defense News (2022).

[67] Emelia Probasco, Building the Tech Coalition: How Project Maven and the U.S. 18th Airborne Corps Operationalized Software and Artificial Intelligence for the Department of Defense, Center for Security and Emerging Technology (2024).

[68] David Sanger, In Ukraine, New American Technology Won the Day. Until it was Overwhelmed, New York Times (2024).

used not just to mimic human actions, but to do what humans cannot—whether it's processing data at machine speed, operating at extreme scale or persistence, or compensating for human cognitive blind spots.[69] Embracing AI's strengths to offset human limitations, and vice versa, is essential if we hope to dominate the future battlespace.

Software-centric Warfare

The original Offset-X report highlighted two pillars of software-centric warfare. First, the United States must attain and maintain a **software advantage** so that our military can execute critical tasks faster and more effectively than any adversary. Software can be updated or reconfigured in hours, whereas hardware changes take years. A force built around software-defined capabilities can tighten its OODA[70] loop, iterate tactics faster than an adversary can react, and deploy new effects at the speed of relevance. Second, the Department of War must ensure that all future weapon systems are inherently software-defined, modular, interoperable, and continuously upgradable—ideally at low cost. Just as software-centric vehicles improve with each update, the Pentagon must design every new platform with software at its core so it can evolve rapidly over its lifecycle.[71]

Since 2023, the Pentagon has made some moves in this direction, though progress remains halting. The wider use of "software factories" and DevSecOps pipelines has improved the speed, efficiency, and security of military software development. Rather than rebuilding common components over and over, programs can now reuse libraries and toolkits, allowing teams to focus on delivering the mission capability. These modern practices are slowly pulling the Department of War away from slow, waterfall-style acquisitions toward agile, iterative methods more in tune with today's tech environment. In March 2025, Secretary of Defense Pete Hegseth reinforced this shift by formally endorsing the Software Acquisition Pathway, further empowering the Department to acquire and deploy software at the speed and scale required.

However, achieving parity with commercial best practices remains a distant goal. Prior to the release of Secretary Hegseth's memo,[72] only 82 Pentagon programs had adopted the Software

[69] Sidharth Kaushal, et al., Leveraging Human-Machine Teaming, Royal United Services Institute and the Special Competitive Studies Project (2024); James Ryseff, Mastering Human-Machine Warfighting Teams, War on the Rocks (2024).

[70] Brian R. Price, Colonel John Boyd's Thoughts on Disruption: A Useful Effects Spiral from Uncertainty to Chaos (2023).

[71] Whitney McNamara, et al., Final Report of the Commission on Software Defined Warfare, Atlantic Council (2025)

[72] Pete Hegseth, Directing Modern Software Acquisition to Maximize Lethality, U.S. Department of Defense (2025).

Acquisition Pathway since its introduction in 2020.[73] With this new mandate, the challenge will be to ensure that programs truly adopt the spirit of modern software best practices as opposed to repackaging a traditionalist approach and mindset within the processes and procedures newly required by the Software Pathway. The United States' unmatched commercial software talent and venture ecosystem are eager to help, but the Pentagon must clear remaining barriers—a lethargic cybersecurity approval process, a widespread lack of mastery for cloud and DevOps infrastructure, and, above all, a lack of a digitally fluent acquisition workforce capable of adopting software-centric approaches instead of beginning from a hardware-centric mindset. Closing those gaps would let the military scale continuous integration across sensors, weapons and AI-enabled decision aids—turning software from a niche enabler into a decisive strategic advantage.

These three critical enablers cannot be considered in isolation. For the warfighter's benefit, they must be pursued together as a coherent and complementary package by design. Only by orchestrating a Joint Force that is distributed, teamed with machines, and software-centric can we leap ahead of the legacy force we deploy around the world today. With the military services currently unable to meet the full spectrum of Combatant Commander requirements, ongoing conflicts heralding a changing character of war, and the likelihood of constant confrontation across an all-domain global operating environment, the United States must seize the opportunity at hand and commit fully to the one approach that can maintain our edge: **Offset-X**

[73] DoD Software Cadre Accelerates Innovation in Acquisition, Defense Acquisition University (2025).