

U.S. RESILIENT DEFENSE

DELIVERING WARFIGHTER SPEED AND AGILITY



GENERAL CATALYST INSTITUTE

FEBRUARY 2026

INDEX

1. FOREWORD
2. EXECUTIVE SUMMARY
3. FRAMEWORK
4. SHORT-TERM ACTIONS
5. LONGER-TERM ACTIONS
6. PATH FORWARD
7. GLOSSARY
8. ACKNOWLEDGEMENTS



FOREWORD

The United States military stands at a critical inflection point. For decades, our global leadership has been anchored by a model of defense acquisition designed for a more predictable era. Today, that model has become a strategic liability.

Our adversaries iterate with unprecedented speed, exploiting technological breakthroughs in months rather than years. America's reliance on static superiority, specifically the outdated assumption that a fixed technological lead or legacy advantage can be maintained indefinitely without continuous adaptation, as well as decade-long development cycles, puts our mission and people at risk.

General Catalyst believes we must fundamentally refocus how the defense enterprise interacts with the extraordinary innovation engine of the U.S. private sector. This requires a transformation built on a simple but powerful principle: **Delivering Warfighter Speed and Agility**. If our warfighters are denied the capabilities they need because we took too long to deliver them, we have failed. Speed to delivery, and the ability to adapt with agility as global challenges require, must become the organizing principle for how we acquire, integrate and sustain technology.

This report provides a roadmap for this transformation through five pillars. By establishing clear accountability for honest assessment, software quality, real-world validation, modernization and technology transition, we can build a force that is defined by its nimbleness rather than its mass alone.

These five pillars form the foundation of our transformation:

1. **Drive Operational Accountability**
2. **Advance Tactical Edge Agility**
3. **Revolutionize Real-World Validation**
4. **Expedite Strategic Resource Realignment**
5. **Accelerate Transition Pathways to the Warfighter**

The private sector is ready to partner in this mission. We must now ensure that our policies and procurement frameworks are equally ready to unleash the full potential of U.S. innovation. The moment for transformative action is now.

Sincerely,



Teresa Carlson
Founding President
General Catalyst Institute (GCI)

U.S. Resilient Defense: Delivering Warfighter Speed and Agility

GOAL: To transform the U.S. military into an adaptive, resilient force that maintains a decisive advantage by integrating private sector innovation at the speed of relevance.

Pillar 1. Drive Operational Accountability	
Short-Term Action	Longer-Term Action
Implement the Composite Readiness Index	Establish Professional Acquisition and Capital Expertise
Pillar 2. Advance Tactical Edge Agility	
Short-Term Action	Longer-Term Action
Establish Software Readiness Detachments	Institutionalize AI Decision Support with Continuous Learning
Pillar 3. Revolutionize Real-World Validation	
Short-Term Action	Longer-Term Action
Mandate Adversarial Testing	Deploy Resilient Power and Signal Distribution Infrastructure
Pillar 4. Expedite Strategic Resource Realignment	
Short-Term Action	Longer-Term Action
Activate a “Pacing Challenge” Strategic Capital Fund	Formalize the Venture-Capital-as-a-Prime Model
Pillar 5. Accelerate Transition Pathways to the Warfighter	
Short-Term Action	Longer-Term Action
Operationalize the Innovation Advantage Pathway	Invest in Industrial Base Resilience and Warfighting Capabilities

Figure 1: Delivering Warfighter Speed and Agility – Primary Goal, Five Pillars, and Actions

EXECUTIVE SUMMARY

Our current defense acquisition model is fundamentally misaligned with today's threat environment, which was built for a slower, more predictable era. The United States now faces adversaries fielding new military capabilities at a pace that compresses the window for effective deterrence. This report argues that this mismatch has turned traditional, decade-long development cycles into a strategic liability: one that risks leaving warfighters without relevant capabilities when they are needed most.

This report states that resilience through adaptation now matters more than resilience through mass production. In contested battlespaces where technology evolves in months and adversaries study our decade-long acquisition timelines, the decisive advantage now belongs to whoever can adapt faster, not whoever holds the larger inventory of exquisite legacy platforms and systems.

To restore advantage, the defense enterprise must adopt a new organizing principle: **Delivering Warfighter Speed and Agility, defined as rapid delivery and continuous adaptation of capabilities under real-world operational conditions. These advances must not just be on the battlefield, but in the processes and procedures it takes to deliver the technology.**

We propose a strategic framework anchored in five mutually reinforcing pillars:

1. Drive Operational Accountability by enabling honest, warfighter-led assessments of combat effectiveness rather than relying on legacy administrative readiness metrics.
2. Advance Tactical Edge Agility by pushing software and capability iteration closer to operational commanders, compressing decision cycles and accelerating updates in the field.
3. Revolutionize Real-World Validation by mandating adversarial testing throughout the lifecycle so systems prove resilience against electronic warfare, cyber disruption, deception and kinetic threat conditions before and after fielding.
4. Expedite Strategic Resource Realignment through incentives that reward divesting obsolete systems and reallocating resources toward high-priority, commercially driven modernization.
5. Accelerate Transition Pathways to the Warfighter by bridging the “valley of death” between prototype and production with parallel planning for sustainment, logistics, training and supply chains.

Taken together, these recommendations will shift accountability to the operational edge, create pathways for commercial technology and ensure that every dollar spent contributes directly to credible deterrence in contested environments.

Overall, the report positions speed, adaptability and rigorous operational proof as the foundations of credible deterrence and battlefield advantage. It concludes that the technology and private-sector capacity already exist; what remains is resetting incentives, continued modernization of procurement, validating capabilities under stress and ensuring successful innovations transition rapidly and repeatedly into the hands of warfighters.

These efforts require a whole-of-ecosystem approach. Cutting-edge startups and major defense partners must work together to deploy commercial innovations in operational environments. Policymakers, Congressional leaders and military commanders must create practical solutions for national security challenges and design innovative acquisition and workforce transformation pathways at the service and combatant command levels.

This approach also demands sustained investment in mutual understanding between the public and private sectors. Today, a persistent knowledge gap undermines partnership: much of the public sector lacks fluency in the realities of venture capital funding models, timelines and incentive structures as compared to traditional defense contractors and private equity. Conversely, the venture and private-company community must develop deeper empathy for the procedural, legal and political constraints that govern how fast the defense enterprise can absorb change, and for the non-negotiable imperative of delivering reliable capability to warfighters. Without deliberate, ongoing education and immersion on both sides, the trust and shared context required to sustain meaningful collaboration will remain insufficient to drive the partnerships this moment demands.

This report, while specific to U.S. defense, should serve as a playbook to implementation for our partners and allies who are also trying to build their own resilience.

By working together to continue accelerating the defense enterprise's transformation, we believe we can make our national security capabilities more adaptive, resilient and effective.

FRAMEWORK

Pillar	Description
1. Drive Operational Accountability	Restore honest assessment, by operational commanders, of the ability of systems to provide measurable advantages through a Composite Readiness Index. This approach would replace outdated administrative metrics with combat effectiveness evaluations, ensuring that readiness is defined by the ability to win against modern threats rather than the preservation of legacy hardware.
2. Advance Tactical Edge Agility	Advance the velocity of adaptation by establishing Software Readiness Detachments that report directly to operational commanders to integrate commercial capabilities in real-time. By bypassing centralized approval cycles, warfighters can iterate on autonomous systems and edge computing models, creating operational unpredictability that outpaces adversary countermeasures.
3. Revolutionize Real-World Validation	Revolutionize defense testing by mandating rigorous adversarial validation throughout the entire development lifecycle to identify vulnerabilities before systems reach the field. This approach subjects commercial and developmental technologies to sophisticated electronic warfare and cyber threats, ensuring that only the most robust and resilient capabilities reach the warfighter.
4. Expedite Strategic Resource Realignment	Expedite the shift toward capability-based budgeting through a “Pacing Challenge” Strategic Capital Fund, which allows services to retain savings from divesting legacy platforms. This market-driven incentive structure rewards leaders who move away from obsolete systems and reinvest in high-priority commercial innovations that address the most pressing pacing challenges.
5. Accelerate Transition Pathways to the Warfighter	Accelerate and strengthen the bridge between successful prototypes and fielded systems by operationalizing the Innovation Advantage Pathway to overcome the “valley of death.” By developing sustainment, logistics, and training infrastructure in parallel with technology maturation, the Department ensures that proven private sector breakthroughs reach operational units at the speed of relevance.

Figure 2: Delivering Warfighter Speed and Agility – 5 Pillars and Detailed Descriptions

SHORT-TERM ACTIONS

The following five actions constitute the immediate roadmap for transforming the U.S. military into an adaptive, resilient force. These recommendations focus on shifting accountability to the operational edge, creating high-velocity pathways for commercial technology and ensuring that every dollar spent contributes directly to credible deterrence in contested environments.

1. Implement the Composite Readiness Index

Current readiness metrics, developed in the 1980s, fail to provide accurate pictures of combat effectiveness against today's threats. In November 2025, we proposed creating a new [Composite Readiness Index](#) (CRI), to replace outdated administrative measurements with a rigorous, warfighter-centric assessment of combat effectiveness. Readiness metrics such as Defense Readiness Reporting System (DRRS) and Mission Capable (MC) rates define readiness without considering realistic adversary capabilities. This new index empowers operational commanders to provide honest evaluations of system performance across three critical dimensions: lethality and survivability in contested zones, combat mass and availability, and the ability to integrate seamlessly within the joint force. The CRI would deliver a true assessment of capability, based upon the environment in which they operate. Flying a jet off the coast of Virginia should look different than flying a jet in a near-peer contested environment; the CRI empowers operational commanders to make true, risk-based command decisions.

By prioritizing these outcomes, the military can identify which legacy systems no longer provide a strategic advantage and must be divested to make room for more capable, private sector innovations. Commanders will score systems on speed of actionable insight delivery under electronic warfare stress, platform performance with degraded data, and resilience against adversary deception attempts. This accountability mechanism ensures that operational realities drive modernization priorities, not institutional preferences for platform preservation.

The Composite Readiness Index creates a direct feedback loop where real-world operational data from contested exercises is used to continuously refine capability assessments. Systems consistently scoring below established thresholds will be designated for modernization or divestment, with savings immediately redirected to technologies that demonstrate measurable advantages in contested environments. Consider the cautionary tale from pre-World War II war games: a U.S. admiral

demonstrated that an attack on Pearl Harbor was possible, yet his conclusions were dismissed. By making commanders accountable for honest assessment, we ensure operational realities drive modernization priorities.

Future Forward #1

The holographic display in the Admiral's ready room glowed a harsh, unforgiving red. For years, the legacy sensor suites on the littoral combat ships had been rated "Mission Ready" by the program office in DC, but the new Composite Readiness Index told a different story. On the screen, the Admiral swiped past the bureaucratic fluff and looked at the raw data provided by the forward commanders: in the high-humidity, high-jamming environment of the Luzon Strait, the legacy sensors were effectively blind.

Because the CRI placed accountability in his hands, the Admiral didn't have to wait for a five-year refit cycle. He used the index to officially "fail" the legacy gear, triggering an immediate pivot to a commercial synthetic aperture radar system that had been red-teamed by his own sailors. Two weeks later, his fleet was tracking adversary "dark" vessels that had previously been invisible, turning a strategic blind spot into a position of tactical dominance.

2. Establish Software Readiness Detachments

To maintain a technological edge, the military must move at the speed of software, not the speed of traditional hardware cycles. Software Readiness Detachments are specialized teams that report directly to operational commanders, enabling commanders a full view of software and data readiness for potential combat, what gaps exist, and what actions need to be taken to improve deterrence and combat readiness. As a result of these actions, the specialized teams achieve the continuous integration of commercial software and artificial intelligence (AI) capabilities. Cumulatively, these specialized teams tied to operational commanders ensure that the warfighter is the primary driver of technological development, allowing for real-time adjustments to autonomous systems, edge computing models, and resilient communication networks.

This model transforms the tactical edge into a living laboratory where software is updated and refined based on immediate operational feedback. By bypassing centralized approval cycles, these detachments can deploy updates in days rather than months, ensuring that commercial innovations such as autonomous sensing networks and edge-based sensemaking algorithms reach warfighters at the speed of relevance. This approach differs fundamentally from past "software factories" that produced inadequate solutions without operational accountability. By working directly for

commanders, these teams overcome existing obstacles associated with ensuring private sector software is fit to fight.

Software Readiness Detachments will be staffed by uniformed personnel and civilian experts with competitive compensation to attract top talent. Each detachment will focus on high-priority mission areas identified by combatant commanders, with clear accountability for software quality tied directly to those who will depend on it in combat. This model has proven successful in special operations units, where dedicated software teams have delivered critical capabilities under operational pressure.

Future Forward #2

Chief Warrant Officer Miller didn't wear a flight suit; he wore a headset and sat behind a bank of ruggedized servers in a humid jungle bunker. Outside, a swarm of U.S. reconnaissance drones was being swatted out of the sky by a new, adaptive adversary frequency. In the old days, Miller would have filed a bug report that would take months to process through a defense contractor. But as part of the 3rd Marine Division's Software Readiness Detachment, he worked directly for the Colonel on the ground.

Miller's fingers flew across the keys, analyzing the telemetry from the downed drones in real-time. He identified the adversary's waveform logic and wrote a counter-code patch within twenty minutes. He pushed the update over the mesh network, and the remaining drones suddenly banked, their sensors recalibrating to bypass the interference. The swarm surged forward, illuminating the enemy's hidden artillery positions just in time for the strike package to scream overhead.

3. Mandate Adversarial Testing

Credible deterrence requires systems that are proven to work under the most demanding conditions. This action mandates rigorous adversarial testing throughout the entire development lifecycle, holding both legacy and emerging technologies accountable to real-world threat environments. Instead of checking boxes against theoretical specifications, systems must demonstrate resilience against sophisticated electronic warfare, cyber interference and kinetic threats. Our systems must be tested as they will fight: networked, contested, and under stress.

Adversarial testing evaluates platform performance with degraded data and adversary deception attempts, identifying vulnerabilities when they are cheaper to fix. The defense enterprise will establish a digital twin feedback loop where real-world operational data from contested exercises is used to continuously refine sensemaking algorithms and edge communication systems. These systems must undergo regular red team

evaluations where they are subjected to adversary-style misinformation and signal interference.

Developers of autonomous sensing and edge computing capabilities will be held accountable for false positive and false negative rates in high-stress scenarios, with funding tied to the system's ability to maintain a high degree of accuracy under duress. By identifying vulnerabilities during testing rather than after deployment, the military ensures that commercial innovations fail gracefully in controlled environments rather than catastrophically during conflict, guaranteeing that only the most robust capabilities reach the hands of the warfighter.

Future Forward #3

The autonomous ground vehicle (AGV) took a direct hit from a high-energy laser, but it didn't stop. It didn't even slow down. The adversary commander watched in frustration as his electronic warfare suite failed to hijack the AGV's navigation. He had expected the American machine to be a "parade ground" toy, easily confused by the chaotic signals of a contested urban environment. He didn't know that this specific model had been "red-teamed" to the point of exhaustion during its development.

Because the Department had mandated adversarial testing, the AGV had already "died" a thousand times in simulated and live-fire trials before it ever reached the mud of the front lines. The engineers had been forced to harden its logic gates and randomize its frequency hopping because the testers were paid to break it. Now, in the ruins of the city, the AGV moved with a predatory, unshakeable purpose, its hardened systems shrugging off the very disruptions that were supposed to be its undoing.

4. Activate a "Pacing Challenge" Strategic Capital Fund

Fiscal responsibility must be tied directly to modernization outcomes. A "Pacing Challenge" Strategic Capital Fund provides a mechanism for services to retain one hundred percent of the savings generated from divesting legacy systems, specifically for reinvestment in high-priority commercial innovations. This fund breaks the cycle of platform preservation by rewarding leaders who make the difficult but necessary choice to move away from obsolete hardware. Leadership could issue a policy memorandum establishing that when services divest systems scoring below established index thresholds, those savings will be protected for service modernization priorities.

By creating a direct financial incentive for capability-based budgeting, the military can rapidly scale the adoption of modular, open-system architectures and other private sector breakthroughs that address the most pressing pacing challenges. The fund will

prioritize investments in technologies that compress the decision cycle and ensure systems can adapt in real-time, including autonomous reconnaissance capabilities, resilient edge communications, secure processing infrastructure and adaptive artificial intelligence decision support.

This approach recognizes that every dollar spent on maintaining legacy systems is a dollar not invested in the adaptive capabilities required for credible deterrence. A “Pacing Challenge” Strategic Capital Fund ensures that divestment decisions are not punished through budget reductions but are instead rewarded with immediate access to modernization resources. Services will establish clear metrics for success, tracking the speed at which divested savings are converted into fielded commercial capabilities.

Future Forward #4

The Air Force had finally mothballed the last of the aging, maintenance-heavy tankers that had drained the budget for decades. In the past, those savings would have vanished into the black hole of the general treasury. But under a Pacing Challenge Strategic Capital Fund, the service kept every cent. Within months, that “dead money” was transformed into a fleet of autonomous, low-cost refueling drones launched from shipping containers.

The result was a radical shift in the Pacific power balance. Instead of a few massive, vulnerable tankers acting as magnets for enemy missiles, the sky was now filled with hundreds of small, attritable refueling nodes. U.S. fighters could now stay on station for hours longer, pushing deep into contested airspace with the confidence that fuel was always a few miles away. The legacy fleet was gone, but the capability it left behind was more lethal, more resilient and entirely paid for by the past.

5. Operationalize the Innovation Advantage Pathway

The modern warfighter requires the ability to observe and orient in contested environments where traditional intelligence, surveillance and reconnaissance systems are degraded or denied. The Innovation Advantage Pathway provides a clear and accountable mechanism for moving promising technologies from successful prototypes to fully fielded systems. When a service secretary designates a successful prototype for this pathway, it establishes a team accountable for building logistics, training and supply chain plans in parallel with production.

This pathway addresses the notorious “valley of death” where promising commercial technologies fail to transition despite successful demonstrations. By requiring that sustainment infrastructure be developed alongside technology maturation, the defense enterprise ensures that private sector partners have a predictable route to the

warfighter. Each service would ensure its transition office reports directly to the service secretary and tracks designated prototypes through the transition process with clear metrics for success.

The Innovation Advantage Pathway transforms the battlefield by ensuring that autonomous sensing capabilities, resilient edge communications, and adaptive artificial intelligence decision support systems are not just demonstrated but fully integrated into operational units. Training warfighters to operate with these systems requires developing intuition about when algorithmic analysis aligns with tactical reality and when human judgment should override machine recommendations. Warfighters need hands-on experience with systems that explain their reasoning in plain language, highlight assumptions that might be wrong and update recommendations in real-time based on emerging information.

Future Forward #5

When the startup "Sentinel Robotics" developed an autonomous ground resupply vehicle capable of navigating contested terrain without GPS, everyone expected it to languish in prototype purgatory for years. Instead, the Innovation Advantage Pathway was triggered the moment the system passed its first combat simulation. While the engineers were still refining the obstacle-avoidance algorithms, a provisional sustainment team was already embedded with forward units, building maintenance protocols, training operators on human-machine teaming interfaces and establishing supply chains for critical components.

By the time the first production run of autonomous resupply vehicles arrived at the forward operating base, the entire ecosystem was already in place. There was no "integration lag" and no confusion over spare parts or operator certification. The logistics teams simply paired with their new robotic teammates and began running continuous resupply missions through contested zones that would have been suicide runs for human drivers. The valley of death hadn't just been bridged; it had been paved over, allowing a revolutionary commercial technology to become a force-multiplying edge in record time while proving that U.S.-based robotics manufacturers could scale their innovations to save both lives and dollars.

Short-Term Actions
1. Implement the Composite Readiness Index to replace outdated administrative metrics with warfighter-centric assessments of combat effectiveness in contested zones.
2. Establish Software Readiness Detachments to enable continuous integration of commercial software at the tactical edge, bypassing centralized approval cycles.
3. Mandate Adversarial Testing to ensure systems are resilient against electronic warfare, cyber interference, and deception before full-rate production.
4. Activate a “Pacing Challenge” Strategic Capital Fund to incentivize modernization by allowing Services to retain 100% of savings from divested legacy systems for reinvestment.
5. Operationalize the Innovation Advantage Pathway to bridge the “valley of death” by building logistics, training, and supply chain plans in parallel with technology maturation.

Figure 3: Short-Term Actions

LONGER-TERM ACTIONS

While the short-term actions focus on immediate operational shifts and accountability mechanisms, the following five longer-term actions are designed to fundamentally restructure the relationship between the defense enterprise and the American innovation ecosystem. These recommendations move beyond tactical adjustments to create a permanent, scalable infrastructure for technological superiority. By institutionalizing new procurement models, professional competencies and physical infrastructure, the defense enterprise can ensure that Delivering Warfighter Speed and Agility is not a temporary advantage but a sustained strategic reality that transforms faster than adversaries can adapt.

6. Establish Professional Acquisition and Capital Expertise

The defense enterprise must professionalize its understanding of how private sector innovation is funded and scaled into real, warfighter capabilities. The current acquisition workforce possesses deep expertise in traditional defense contracting but often lacks

the capital literacy required to evaluate venture-backed companies, assess their financial runway, or structure contracts that align with commercial business models. This gap creates a fundamental mismatch between how the private sector operates and how the defense enterprise procures technology, resulting in promising innovations failing to transition despite successful demonstrations.

Ensuring that the Department advances Professional Acquisition and Capital Expertise addresses this challenge by creating a formal training and certification program. This program will be co-developed with premier business schools and private equity, venture capital and investment banking professionals to ensure it reflects real-world commercial practices. Selected contracting officers will attend week-long intensive courses that teach them to understand the differences between venture capital and private equity, the kinds of financing available to commercial companies at various stages of maturity and how the commercial market thinks about risk:reward tradeoffs. This knowledge enables professionals to better assess the different kinds of companies supporting the defense industrial base and the different kinds of funding (and hence, contracting) they are utilizing.

To ensure this competency is taken seriously, the defense enterprise will require that all programs exceeding fifty million dollars include a Capital Structure Assessment in their acquisition strategy documents. Contracting officers who complete the certification and maintain their credentials will be designated as “Gold-Tier” professionals, with this status serving as a positive promotion discriminator. This creates a clear career incentive for acquisition professionals to develop capital expertise and ensures that the most sophisticated commercial engagements are managed by personnel who understand the financial realities of the innovation ecosystem. By speaking the language of investment and growth, the defense enterprise can engage more effectively with the private sector and secure the best technologies for the warfighter.

Future Forward #6

The contracting officer stared at the term sheet from the autonomous systems startup and, for the first time in her career, understood what she was reading. The “Series B preferred equity with liquidation preference” wasn't jargon anymore. It was a clear signal that this company had eighteen months of runway and needed a contract decision now, not in two years. Because she had earned her Gold-Tier certification in capital literacy, she knew exactly how to structure a phased contract that aligned with their funding cycle while protecting the government's interests.

Three months later, the startup's autonomous reconnaissance drones were in the field, and the contracting officer was briefing a room full of skeptical program managers on why understanding venture capital wasn't just useful but mission-critical. The old guard had spent decades perfecting the art of negotiating with defense primes. She was part of a new generation that could speak fluent "Silicon Valley" and translate billion-dollar ideas into boots-on-the-ground capabilities before the competition even knew the race had started.

7. Institutionalize AI Decision Support with Continuous Learning

Artificial intelligence represents one of the most transformative capabilities available to the modern military, but only if these systems are designed to evolve continuously based on operational feedback. Static AI models that are trained once and deployed without further refinement quickly become obsolete as adversaries adapt their tactics and as the operational environment changes. The defense enterprise must transition from treating AI as a fixed product to treating it as a living capability that learns and improves in real-time based on direct input from the warfighters who depend on it in combat.

This long-term action builds directly on the Software Readiness Detachments established in the short-term phase. These detachments will serve as the primary conduit for continuous AI refinement, ensuring that decision support algorithms are constantly updated based on operational performance data. AI systems will be evaluated not on their algorithmic sophistication but on their ability to deliver actionable insights quickly and transparently under contested conditions. Commanders will assess these systems on speed of insight delivery, explainability of reasoning, and accuracy under degraded data conditions. Systems that fail to meet established thresholds will be designated for algorithm refinement or divestment, ensuring that only the most reliable capabilities remain in the field.

Training warfighters to operate effectively with AI decision support requires developing intuition about when algorithmic analysis aligns with tactical reality and when human judgment should override machine recommendations. Warfighters need hands-on experience with systems that explain their reasoning in plain language, highlight assumptions that might be wrong and update recommendations in real-time based on emerging information. By institutionalizing continuous learning as the standard for all AI systems, the defense enterprise ensures that these capabilities remain relevant and trusted, providing commanders with the decision advantage required to outpace adversaries in rapidly evolving scenarios. Furthermore, U.S. commercial software platforms have the ability to accelerate mission planning from months to hours, which

when combined with AI-powered simulation tools that enable real-time design optimization, gives military commanders decision superiority and reduces risks to U.S. forces and successful mission outcomes.

Future Forward #7

The AI decision support system had been in the field for six months, and it was already unrecognizable from its original deployment. Every time a patrol reported that the algorithm's threat assessment didn't match ground truth, the Software Readiness Detachment fed that data back into the model. The AI didn't just log the correction; it learned from it, refining its understanding of how insurgent tactics were evolving in real-time. The system had become a living extension of the unit's collective experience.

When the enemy shifted to a new pattern of ambush tactics, the AI caught it before the intelligence analysts did. It flagged an anomaly in vehicle movement patterns and explained its reasoning in plain language: "Historical data suggests this route is avoided during market days. Current traffic is inconsistent with civilian behavior." The patrol leader trusted the recommendation because the system had earned that trust through months of continuous learning. They took an alternate route, and the abandoned IEDs were discovered hours later by a follow-on sweep.

8. Deploy Resilient Power and Signal Distribution Infrastructure

Modern military operations depend on the seamless flow of power and data across distributed forces. When adversaries can disrupt these flows through jamming, cyber-attacks, or kinetic strikes, even the most advanced platforms become ineffective. Resilient power and signal distribution infrastructure addresses this vulnerability by deploying ruggedized energy management and signal transmission technologies that automatically reroute power and data through alternative pathways when primary systems are damaged or jammed. This infrastructure ensures that the digital spine of the force remains functional even under the most extreme conditions.

This long-term action focuses initial deployment on tactical units and ship-based proving grounds, where the need for resilient command, control, and communications is most acute. By hardening these critical nodes first, the defense enterprise can demonstrate the operational value of resilient infrastructure and build the case for broader deployment across the joint force. These systems will be designed to integrate seamlessly with the autonomous sensing networks and edge computing capabilities established in the short-term phase, creating a layered defense that ensures warfighters maintain situational awareness and connectivity even when adversaries attempt to isolate or deceive them. Furthermore, the U.S. private sector can aid in reshoring industrial capabilities and revolutionizing manufacturing through collaborative robotics and digitized production workflows, to help ensure a resilient domestic supply chain

here in the United States that produces critical defense hardware at the speed of relevance for the warfighter.

The deployment of resilient infrastructure is not merely a technical upgrade but a strategic investment in operational unpredictability. When adversaries cannot reliably disrupt United States command and control, they lose the ability to impose costs through electronic warfare or cyber operations. This forces them to confront a military that can adapt and respond in real-time, regardless of the contested nature of the environment. By ensuring that power and data flow continuously, the defense enterprise creates the foundation for all other adaptive capabilities to function effectively, making resilience the cornerstone of credible deterrence.

Future Forward #8

The enemy's jamming barrage hit the forward operating base like a digital tsunami, designed to sever every communication link and plunge the American forces into isolation. In previous conflicts, this would have been catastrophic. But the base's resilient signal distribution infrastructure didn't panic. It simply adapted. Within milliseconds, the system detected the disruption, rerouted data through a mesh of alternative pathways, and maintained connectivity using frequency-hopping protocols that the adversary couldn't predict.

The base commander watched the tactical display flicker once, then it stabilized. Her link to higher headquarters remained solid. Her drones continued to feed real-time intelligence. Her artillery could still receive fire missions. The enemy had just expended a sophisticated electronic warfare capability and achieved nothing. Somewhere in an adversary command post, a frustrated signals officer was realizing that the Americans had built a network that refused to die, no matter how hard you hit it.

9. Formalize the Venture-Capital-as-a-Prime Procurement Model

The traditional defense industrial base is dominated by a small number of large prime contractors who manage complex programs through extensive subcontracting networks. While this model has delivered critical capabilities in the past, it is poorly suited to the rapid integration of diverse commercial technologies from high-growth startups. The Venture-Capital-as-a-Prime model addresses this challenge by allowing a VC firm or a collection of investors to act as a primary contractor, “a prime”, responsible for obtaining the necessary certifications, clearances, and other responsibilities akin to large prime contractors for their portfolio companies. This provides a single point of accountability and shifts the burden of technical coordination and vendor management from nascent

startups with needed capabilities for the warfighter, to mature partners capable of overseeing the necessary certifications, clearances, and other responsibilities required to do work with the Department.

This model also provides the defense enterprise with access to a curated pipeline of vetted, investment-backed technologies where private sector due diligence serves as a pre-qualification mechanism. VC firms have already conducted rigorous assessments of technical feasibility, financial viability and team capability before investing, reducing the risk for the government. By leveraging this strategic oversight, the defense enterprise can rapidly scale integrated capabilities while maintaining the highest standards of performance and security. This is particularly effective for integrating multi-domain solutions that require the seamless coordination of software, hardware, and data infrastructure from multiple vendors.

The Venture-Capital-as-a-Prime model also reduces the administrative overhead for small-scale innovators, allowing them to contribute to national security without navigating the complexities of federal acquisition independently. Instead Venture Capital Firms can, if choose to do so, take on this responsibility. By reshoring industrial capabilities and revolutionizing manufacturing through collaborative robotics and digitized production workflows, the defense enterprise can ensure a resilient domestic supply chain that produces critical defense hardware at the speed of relevance for the warfighter. This creates a more diverse and competitive defense industrial base, where the best ideas can reach the warfighter regardless of the size or experience of the originating company. By formalizing this procurement approach, the defense enterprise ensures that the innovation engine of the American private sector is fully harnessed, creating a permanent pipeline of cutting-edge capabilities that can be fielded at the speed of relevance.

Future Forward #9

The program manager had grown tired of herding dozens of small startups through the bureaucratic maze of defense contracting. Each company had a brilliant piece of the puzzle, but none of them had the bandwidth to manage government compliance, security clearances, and integration testing. Then the Department decided to formalize the Venture-Capital-as-a-Prime procurement model, and this changed everything for the better. The VC firm that had invested in all these companies stepped up as the prime contractor, taking on the burden of coordination and providing a single point of accountability.

Within a year, what had been a fragmented collection of promising prototypes became a fully integrated, multi-domain sensing and

strike capability. The VC firm managed the technical integration, ensured cybersecurity standards were met and coordinated logistics across the entire portfolio. The program manager could finally focus on warfighter requirements instead of contract administration. The startups got paid on time and could focus on innovation instead of paperwork. And the warfighter got the capability that no single company could have delivered alone.

10. Invest in Industrial Base Resilience & Warfighting Capabilities

The traditional defense acquisition model treats the industrial base as a passive supplier of capabilities rather than a strategic asset requiring deliberate investment and cultivation. This approach has led to a defense industrial ecosystem dominated by a small number of large prime contractors, with limited capacity to rapidly scale production, integrate emerging technologies, or respond to surge demands during a crisis. The result is a brittle supply chain vulnerable to disruption, extended lead times for critical components, and an inability to leverage the full breadth of American industrial innovation. To restore strategic advantage, the defense enterprise must invest as much time, attention and resources in strengthening the industrial base as it does in developing individual warfighting capabilities.

Industrial base resilience is more than maintaining production capacity for existing systems, it must also include ensuring the United States possesses the domestic manufacturing infrastructure, skilled workforce and technological sophistication required to rapidly produce next-generation capabilities at scale. This requires deliberate investment in reshoring critical manufacturing capabilities, revolutionizing production through advanced automation and collaborative robotics, and deploying industrial IoT platforms that enable defense organizations to build and maintain complex hardware products more effectively. By treating the industrial base as a strategic capability in its own right, the defense enterprise ensures that technological breakthroughs can be translated into fielded systems at the speed and scale required for credible deterrence.

The current imbalance between capability investment and industrial base investment creates a strategic vulnerability. The Department can develop the most sophisticated autonomous systems, AI-powered decision support tools, or resilient communications networks, but if the industrial base cannot manufacture these systems at scale, maintain them under operational stress, or surge production during conflict, then these capabilities provide only theoretical advantage. By formalizing a requirement that industrial base investments receive equal priority with capability investments, the defense enterprise ensures that every dollar spent on technology development is matched by investment in the manufacturing infrastructure, supply chain resilience, and

workforce expertise required to sustain that technology throughout its operational lifecycle.

This approach creates opportunities for a diverse ecosystem of innovators to contribute to national security. By investing in companies that are reshoring industrial capabilities and revolutionizing manufacturing through collaborative robotics and digitized production workflows, the defense enterprise strengthens domestic supply chain resilience while reducing dependence on foreign suppliers for critical components. By deploying industrial IoT platforms and advanced operational software, the Department enables more effective building and maintenance of complex hardware products, ensuring maximum mission-critical uptime across all domains. By prioritizing software-first, AI-powered manufacturing optimization and advanced simulation tools, the defense enterprise accelerates the transition from prototype to production while maintaining the quality and reliability standards required for combat operations.

Investing equally in industrial base and capabilities also addresses the strategic challenge posed by competitors who have made industrial capacity a centerpiece of their military modernization efforts. When adversaries can produce military hardware at scale and speed that outpaces U.S. production timelines, they gain strategic advantages in both deterrence and wartime attrition scenarios. By rebuilding U.S. industrial strength through targeted investments in advanced manufacturing, automation and supply chain resilience, the defense enterprise ensures that the United States can not only develop superior technologies but can also produce them in the quantities required to maintain overmatch across all domains.

Future Forward #10

The Admiral stared at the production timeline on her screen and felt a rare moment of relief. Three years ago, when the Navy had identified a critical need for thousands of autonomous underwater vehicles to counter the adversary's submarine expansion, the answer would have been a decade-long contract with a single prime contractor and a foreign supply chain vulnerable to disruption. But the Department had finally learned its lesson: capabilities without industrial capacity were just PowerPoint slides. Now, the investment in reshoring advanced manufacturing and deploying collaborative robotics across multiple U.S.-based facilities meant that production could scale at a pace that matched the threat.

The factories hummed with a new kind of efficiency. Industrial IoT platforms monitored every stage of production in real-time, flagging potential bottlenecks before they became delays and optimizing supply chains that were now entirely domestic, with

allied partners ready to supplement capacity. The autonomous systems rolling off the line weren't just sophisticated: they were available, produced in the quantities needed to flood the contested waters and create the operational overmatch that deterred conflict in the first place. The adversary's planners had counted on American industrial atrophy and had been proven wrong. The United States had been ready. The adversary had miscalculated.

Longer-Term Actions

6. Establish Professional Acquisition and Capital Expertise to require Capital Structure Assessment training and “Gold-Tier” certification for contracting officers, aligning defense procurement with commercial financial realities.

7. Institutionalize AI Decision Support with Continuous Learning to transition artificial intelligence from static products to living capabilities that evolve in real-time based on direct operational feedback from the field.

8. Deploy Resilient Power and Signal Distribution Infrastructure to implement ruggedized energy and data management systems that automatically reroute around jamming or damage to maintain the digital spine of the force.

9. Formalize the Venture-Capital-as-a-Prime Procurement Model to shift technical coordination to companies with portfolios of needed capabilities, enabling the Department to employ multiple commercial solutions while reducing administrative barriers for innovators.

10. Invest in Industrial Base Resilience and Warfighting Capabilities to ensure the United States possesses the domestic manufacturing infrastructure, advanced automation, and supply chain resilience required to rapidly produce and sustain next-generation capabilities at the speed and scale demanded by credible deterrence.

Figure 4: Longer-Term Actions

PATH FORWARD

The transition to **U.S. Resilient Defense** is not merely a policy preference, it is a strategic necessity. The era of static superiority has been replaced by an era of continuous adaptation, where the decisive advantage belongs to the side that can iterate, integrate and field new capabilities at the speed of relevance. As this report has outlined, the path to this future requires a fundamental shift in how the defense enterprise views its relationship with the U.S. innovation ecosystem.

The moment for transformative action to advance military readiness and credible deterrence is now. Through dynamic market-driven approaches, we can and will harness innovative technology while championing operational effectiveness and ensuring warfighter safety through rigorous adversarial validation. By embracing warfighter-centric accountability, tactical edge agility and accelerated transition pathways, implementing prudent fiscal practices through protected divestment savings, and mobilizing U.S. commercial excellence, we can achieve transformation through resilient innovation.

By implementing the ten actions proposed in this report, America can move beyond the friction of legacy acquisition. We can build a defense enterprise that is as nimble as the startups it seeks to partner with and as resilient as the warfighters it serves. This bold transformation will be achieved through the **Strategic Framework: Delivering Warfighter Speed and Agility** that rallies market-driven approaches, collectively with startups, educational institutions and other partners working alongside Congress and the Executive Branch to deliver military capabilities that work for the warfighter and the nation.

The private sector is ready to lead. The technology exists to provide our forces with autonomous sensing, resilient communications and AI-driven decision support that can outpace any adversary. What remains is the institutional will to embrace accountability, reward divestment of the obsolete, and create structured pathways for commercial excellence. If we act now, we can ensure that the U.S. military remains the most adaptive and capable force in the world, secured by an innovation engine that is second to none.

GLOSSARY

Adversarial Testing: A rigorous validation mandate requiring systems to demonstrate resilience against real-world threat conditions, including electronic warfare, cyber interference and kinetic threats, throughout the development lifecycle and prior to full-rate production.

Autonomous Sensing Networks: Distributed systems of sensors that utilize artificial intelligence to observe and orient in contested environments without constant human intervention or reliance on centralized command and control infrastructure.

Capital Literacy: The professional competency of understanding private sector funding structures, including venture capital, private equity and hybrid financing models, to better align government procurement with commercial business cycles and assess company viability.

Composite Readiness Index: A warfighter-centric metric that replaces administrative readiness counts with honest assessments of a system's combat effectiveness, lethality, survivability and integration capability in contested zones against current threats.

Continuous Learning AI: Artificial intelligence decision support systems that evolve their analytical models in real-time based on direct operational feedback from warfighters, ensuring algorithms remain relevant as adversaries adapt their tactics.

Edge Computing: Data processing capabilities deployed at the tactical edge that enable analysis and decision-making without reliance on centralized cloud infrastructure, maintaining functionality in degraded or denied communications environments.

Human-Robot Teaming: The integration of autonomous systems into human units through intuitive interfaces, comprehensive training programs and logistics infrastructure that enables collaborative mission execution across all domains.

Innovation Advantage Pathway: A formalized mechanism for transitioning successful technology prototypes into fielded capabilities, including parallel planning for sustainment, training, logistics and supply chain infrastructure rather than treating transition as an afterthought.

Operational Unpredictability: A strategic state where the ability to compress decision cycles and adapt systems in real-time complicates adversary planning by preventing reliable prediction of force composition or development of effective countermeasures.

Pacing Challenge Strategic Capital Fund: A fiscal mechanism allowing military services to retain one hundred percent of savings from divested legacy systems through protected divestment savings for immediate reinvestment in high-priority commercial innovations that address pacing threats.

Resilient Edge: A strategic state where military forces maintain a decisive advantage through the rapid integration of adaptive, software-defined and autonomous capabilities that function effectively even in degraded, denied, or contested environments.

Resilient Power and Signal Distribution: Ruggedized energy management and signal transmission technologies that automatically reroute power and data through alternative pathways when primary systems are jammed, degraded, or damaged by adversary action.

Software Readiness Detachments: Specialized units reporting directly to operational commanders tasked with the continuous integration and real-time updating of commercial software capabilities at the tactical edge, bypassing centralized approval cycles.

Valley of Death: The gap between successful prototype demonstration and sustained production where promising commercial technologies fail to transition due to lack of structured sustainment planning, logistics infrastructure, or predictable revenue pathways.

Venture-Capital-as-a-Prime: A procurement model where a VC firm or a collection of investors act as a primary contractor responsible for obtaining the necessary certifications, clearances, and other responsibilities akin to large prime contractors for their portfolio companies.

ACKNOWLEDGEMENTS

This report would not have been possible without the vision and dedication of numerous leaders across the technology and national security sectors. We would like to extend special thanks to **Hemant Taneja**, **Paul Kwan** and **Lt. Gen. Scott Howell, USAF (ret.)** for their invaluable leadership and commitment to reimagining the partnership between the defense enterprise and the private sector. Thank you especially to **Jonathan Clifford** for leading our effort on this report and **Dr. David Bray** whose thought leadership ensured this report is both ambitious and achievable. Internally, special thanks to members of the GCI team including **Maryam Mujica** and **Peter Nonis** for their efforts, as well as **Jack Cohen**, **Reggie James** and **Nick Cohen** at GC. Finally, thank you to the countless founders, government leaders, and colleagues who work with the General Catalyst Institute to connect policy to outcomes.

ABOUT THE GENERAL CATALYST INSTITUTE (GCI)

General Catalyst is a global investment and transformation company that partners with the world's most ambitious entrepreneurs to drive resilience and applied AI. The General Catalyst Institute (GCI), a part of General Catalyst, bridges venture capital and government to promote national resilience through transformative technologies. GCI partners with policymakers and startups to shape policies in AI, defense and industrials, energy, fintech, and healthcare. GCI works to amplify the voices of its 900+ portfolio companies in important policy conversations around the world. Learn more at www.generalcatalyst.com/GCI.



G