

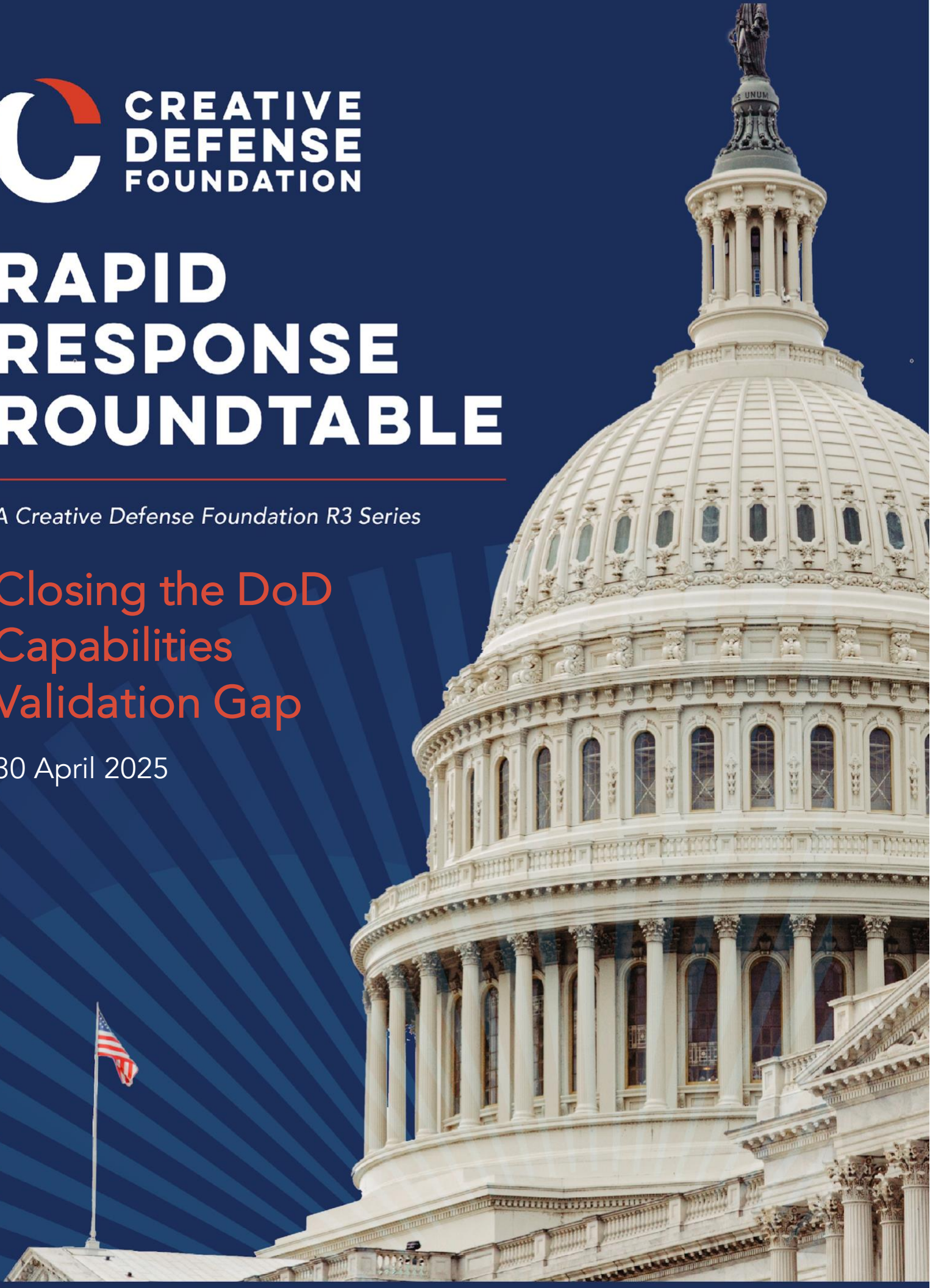


RAPID RESPONSE ROUNDTABLE

A Creative Defense Foundation R3 Series

Closing the DoD
Capabilities
Validation Gap

30 April 2025





Closing the DOD Capabilities Validation Gap

Summary of the Roundtable Discussion

(NOTE: This summary is followed by the topic description provided to attendees prior to the roundtable discussion)

This roundtable was convened on April 30, 2025, under Chatham House Rule. The following reflects the perspective of the Creative Defense Foundation and is not attributed to any individual participant or organization. By bringing together experts from across the defense ecosystem, including operational perspectives, innovation hubs, acquisition leadership, industry, and congressional staff, this Rapid Response Roundtable addressed the critical challenge of closing the Department of Defense's "Capability Validation Gap."

The capability validation gap was identified as a primary impediment to fielding innovation at the speed of relevance and represents a systemic failure. It results in promising technologies languishing in the "Valley of Death" unable to navigate the transition into operational capability. The urgency to close the gap is undeniable, driven by accelerating peer competition and an increasingly evolving battlespace demanding faster adaptation cycles.

A clear consensus emerged: the Department's traditional, linear validation processes spanning requirements generation (JCIDS), testing, certification, and fielding under the Planning, Programming, Budgeting, and Execution (PPBE) system are ill-suited for today's dynamic environment. These processes are too slow, too siloed, and often incentivize risk aversion over rapid delivery. The root causes were consistently identified as **deeply ingrained organizational, cultural, and procedural barriers** and not as technical limitations.

These include misaligned incentives that penalize prudent risk-taking; a lack of institutional mechanisms for continuous, data-driven learning that is enthusiastically shared across the national security ecosystem; and the absence of high-tech, independent integration and test environments capable of objectively evaluating and validating emerging and competing solutions. These environments are essential for ensuring interoperability, accelerating trust, and enabling rapid convergence on mission-ready capabilities

To bridge this chasm, the concept of a **Joint Integrated Validation Environment (JIVE)**, was proposed as a trial concept. Such an entity, technically proficient, mission-focused, and unencumbered by competing commercial interests, would serve as a crucial enabler. It must provide cutting-edge digital tools: high-fidelity Modeling and Simulation (M&S), validated digital twins, AI-enabled testing frameworks, and secure access to operational data streams. It should provide for rigorous, continuous validation throughout the capability lifecycle, shifting from discrete "final exams" to an ongoing, iterative process integrated with development and operations.



Achieving this requires more than just standing up a new organization; it demands **fundamental reform, robust funding, and parallel execution**. Key recommendations are:

1. Involving validation as an independent unconflicted full partner in the iterative development and fielding of warfighting capabilities.
2. Creating a business model for industry and government validation participants that is independent, unconflicted, and has incentives to reward speed, smart risk taking, and to support warfare system capability providers with access to information and data.
3. Task validation with the development and maintenance of data lakes that can be supplied to capability providers for research and development of new capabilities.
4. Task validation with the development and maintenance of automated repeatable performance analyses of standalone and integrated capabilities and kill chains.
5. Breaking down programmatic silos and integrate developmental test, operational test and user communities.
6. Tasking validation with actively exercising open architectures and interfaces to ensure interoperability and combat vendor lock.
7. Task validation with continuous modernization of integration and test technologies such as high-fidelity Modeling and Simulation (M&S), virtual environments with digital twins, AI-enabled testing frameworks, validation at the edge, and secure access to operational data streams.

It was emphasized that recently enacted flexible funding authorities, designed to catalyze change, require radical transparency and accountability from the Department. Consistent and timely reporting on both progress and obstacles is essential to building trust and sustaining momentum for further reform.

Ultimately, closing the validation gap necessitates **strong leadership and managerial courage** to implement these interconnected changes. The vision is an adaptive, data-driven validation ecosystem that treats validation not as a bureaucratic hurdle, but as a full partner in a rapidly advancing capability refinement loop. This transformation, leveraging independent validation capabilities within a reformed process structure, is not merely desirable; it is an operational imperative for maintaining U.S. military superiority.



Closing the DOD Capabilities Validation Gap

Topic Description Executive Summary

The Department of Defense must rapidly adapt its warfighting systems to effectively counter an increasingly complex and evolving threat environment. However, the ability to promptly validate and certify new capabilities as they emerge has become a critical limiting factor resulting in what is referred to here as the Capability Validation Gap. The purpose of this Rapid Response Roundtable is to bring together key stakeholders to clearly define and understand this gap, discuss its implications for operational readiness, and collaboratively identify potential technological and procedural solutions to close it.

To facilitate an informed and focused discussion, this paper provides a forward-looking vision of potential future validation capabilities, relevant technologies, and business models for closing the gap. It considers current and emerging technologies along with business models for independent unconflicted validation and continuous modernization. While recognizing that alternative approaches may exist, the concepts described here serve as a starting point to guide meaningful dialogue among participants.

The concept of a DOD enterprise-wide Joint Integrated Validation Environment (JIVE) is introduced. It presumes significant validation progress can be made in virtual environments informed with operational data and the use of processing at the edge of operational assets without disrupting primary mission objectives. Operational forces serving simultaneously as mission and validation assets is a game-changing accelerator. It enables real-time real-world validation without disrupting operations. Key technologies include artificial intelligence, virtualization, digital twins, processing at the edge, automated testing and analysis, and realistic contested environments.

This JIVE capability would improve the performance and relevance of all assets and would enable continuous integration, mission-focused training, and real-time operational assessment, making it a strategic asset in both preparing for and prevailing in future conflicts.

The Current Validation Gap

The Department of Defense experiences an unacceptable delay between the development of new capabilities and their certified deployment within the operational force. While innovators are rapidly developing new capabilities using state-of-the-art technologies, the process for integration, test, certification, and operational test and evaluation (OPEVAL) has not received the investment or innovation required to keep pace. This has resulted in a capabilities validation gap resulting in unacceptable deployment costs and delays.

The DOD typically conducts integration, test, and certification activities through a sequential process that includes system-level interface verification, cybersecurity accreditation, developmental testing (DT), operational test and evaluation (OT&E), and requirements compliance validation. During integration, systems must demonstrate interoperability with existing platforms, networks, and data architectures. Developmental testing evaluates performance under controlled conditions to confirm that technical specifications are met. Certification involves a series of formal reviews and approvals related to safety, cybersecurity, software assurance, and information assurance. Operational evaluation (OPEVAL) is

**TIME IS SHORT
AND THE
STAKES ARE HIGH.**



conducted by independent test agencies (such as AFOTEC, ATEC, or COMOPTEVFOR) to determine effectiveness, suitability, and survivability under combat-realistic conditions. When issues arise, capabilities are returned to developers often with inadequate data to understand how improvements can be made. This traditional pipeline is not optimized for rapidly evolving technologies, software-based systems, or cross domain kill chains and creates unacceptable delays in the deployment of essential capabilities.

The Rise of Adaptive Approaches

Operational commanders, especially those in forward-deployed theaters like INDOPACOM or CENTCOM, face rapidly evolving threats and shrinking decision timelines. In response, they are increasingly turning to accelerated pathways to identify, evaluate, and operationalize promising new capabilities more quickly than traditional validation cycles allow.

In practice, this has included:

1. **Direct Operator–Innovator Collaboration**

Operational units are working directly with small tech firms, DIU, AFWERX, and other innovation organizations to prototype and deploy emerging tools (e.g., AI analytics, autonomous drones, mesh communications) with appropriate oversight and within established frameworks. These efforts are often structured as minimum viable products (MVPs) or operational prototypes to enable rapid learning and iterative improvement.

2. **Operator-Led Integration**

Command-level units are sometimes integrating these tools into mission workflows locally, often before centralized interoperability testing or integration with legacy systems is complete reflecting the urgency of mission needs and the agility of modern platforms.

3. **Live Operational Testing**

In some cases, tools are evaluated in live operational environments as part of their maturation process, providing invaluable real-world data but also underscoring the need for systematic, repeatable validation practices.

4. **Use of Waivers and Alternative Authorities**

Units may pursue appropriate authorities, waivers, or acquisition pathways to enable rapid fielding of capabilities under urgent operational needs or limited-scope deployments.

5. **Innovation Pathways**

Many capabilities are developed under “innovation initiatives” that exist outside traditional acquisition channels. While this approach supports speed and flexibility, it often lacks the repeatable validation infrastructure required for broader scaling and transition to programs of record.



These adaptive approaches have created valuable operational insights and accelerated innovation, but they do not yet scale in a way that supports joint, cross-domain validation or the structured data analysis needed to inform future acquisitions. Establishing a repeatable, integrated validation ecosystem would enable the Department to preserve the speed of innovation while enhancing trust, interoperability, and operational readiness.

The Need for a Digital Validation Architecture

Today, the technology exists to dramatically modernize DOD test, integration, certification and OPEVAL making them orders of magnitude more efficient, cost effective, time effective, and most importantly makes them a full partner in a digitally connected, continuously learning warfighting ecosystem where all domains (land, sea, air, space, cyber) and services (Army, Navy, Air Force, Marine Corps, Space Force) rapidly validate new capabilities using real-world environments and provide continuously improving combat capabilities at the speed of relevance.

Digital twin environments, powered by edge computing, high-fidelity simulation engines, and AI-enabled analytics can continuously integrate live operational data to assess how new capabilities perform under realistic, contested conditions. This future digital infrastructure can host multiple competing solutions simultaneously, allowing side-by-side evaluation in joint mission scenarios and enable decision-makers to select the most effective options based on performance, resilience, and interoperability.

By capturing structured test data, outcomes, and contextual variables, a repeatable framework can be created and reused to validate future capabilities at scale. This approach transforms validation from a linear, one-time event into a continuous, high-velocity loop accelerating innovation, increasing confidence, and reducing risk.

Establishing the Joint Integrated Validation Environment (JIVE)

The totality of the digital infrastructure supporting validation activities should become the DOD's Joint Integrated Validation Ecosystem (JIVE). Moreover, just as with warfighting capabilities, it is essential that the JIVE undergo continuous modernization as an essential partner in addressing the increasingly complex and rapidly evolving technologies, threats, and missions essential to U.S. national security.

Providers of integrated validation environments must operate with business models designed to assist the defense acquisition community in accelerating capabilities, whether from current incumbents, non-traditional suppliers, government organizations or others.

Their incentives should be aligned with validating the best-performing capabilities regardless of source. These open system agents must also be responsible for capturing, curating, and analyzing data in a way that enables rapid re-certification of advanced alternatives as they emerge to ensure the DOD maintains both agility and technological superiority over time. JIVE providers should become a new component of the defense innovation industrial base designed to engage with DOD program management, program oversight, approval warrant holders, the national security investment community, and commercial technology partners to provide the integrated validation technologies needed to rapidly develop and maintain this capability.



The current defense industrial base includes large prime contractors and specialized subsystem providers, but it lacks a robust component of truly independent integrators who are unconflicted in their primary mission to rapidly integrate, test, and validate best-of-breed capabilities regardless of origin and furthermore, to keep the process, technology, and associated tests, analyses, and data available and state-of-the-art for fielding capabilities at the speed of relevance.

Additionally, the current organizational structures within the DOD and the military departments are not designed to support a joint, fully integrated, cross-domain integrated validation environment. There are no existing commands or frameworks within the services responsible for managing a dynamic, continuous digital twin ecosystem. The technology has arrived to close this gap, and this would provide a unique strategic advantage, enabling the U.S. military to validate, adapt, and deploy new capabilities faster than any potential adversary.

Creating Theater-Ready Solutions

The development and deployment of this capability can be pursued incrementally with a focus on geographic theaters where operational urgency and technological risk are highest. Rather than attempting to implement a global solution all at once, the focus should be on delivering value to combatant commanders in the regions where integrated, validated, software-defined capabilities are most critical.

Today, among all regions, the Indo-Pacific theater, under U.S. Indo-Pacific Command (INDOPACOM) represents the most urgent and strategically consequential environment. With a rapidly evolving threat from the People's Republic of China, a contested battlespace that spans thousands of miles, and the forward deployment of emerging capabilities such as autonomous systems, distributed fires, and dynamic command and control, INDOPACOM demands a real-time, digitally connected warfighting ecosystem.

Deploying this capability first in INDOPACOM would enable the joint force to rehearse, validate, and adapt kill chains at the speed of operational need while building a model that can be scaled across other combatant commands. A Theater-Ready Integrated Validation Environment (THRIVE) can also be incrementally developed based on the highest priority capabilities and kill chains.

The current characteristics for this theater are:

1. China is the pacing threat

DoD strategy and Congressional posture statements are clear: the PRC is the primary long-term challenge. A Taiwan contingency would stress joint kill chains, autonomy, unmanned systems, contested logistics, and dynamic targeting. All would benefit from a theater ready joint integrated test and validation environment (THRIVE).

2. Dispersed geography, long logistics

Thousands of miles of ocean, small island bases, forward-positioned forces — all require resilient, software-defined C2, sensor fusion, and autonomy. Real-world operational feedback from exercises like Pacific Deterrence Initiative and Valiant Shield can be directly fed into the THRIVE environment.



3. Emerging tech is already being deployed

Programs like Replicator, PACAF's Agile Combat Employment (ACE), and Navy unmanned initiatives are rapidly delivering capability but without a unified validation backbone. A THRIVE would provide the environment to test, certify, and trust these new tools at speed.

4. Service convergence is already happening

A persistent, joint validation ecosystem will unify efforts across Navy, Air Force, Army, Marine Corps, and Space Force in the region. INDOPACOM is the focal point for joint efforts like JADC2, Multi-Domain Operations (MDO), and all-domain kill webs.

Initial deployment of THRIVE should be prioritized in INDOPACOM, where the threat is most advanced, the battlespace most complex, and the demand for cross-domain integration most urgent. A digitally enabled, continuously validated joint force in this theater will not only strengthen deterrence against the pacing threat but also serve as a proving ground for scaling to other combatant commands.

Key Features would include real-time digital twins; virtual replicas of platforms and systems continuously updated from operational data; cross service multi domain integration; a joint, synthetic environment to test kill chains and operations across services; operational software testing at speed; secure, live testing of autonomy, C2, and targeting software with threat models; AI-powered decision support; advanced analytics to help commanders adapt faster than adversaries; and joint readiness and capability validation with warfighters, developers, and testers operating within a shared immersive system environment.

A robust JIVE would have use cases well beyond traditional capability validation. They would include:

- **Real-Time Scenario Simulation:** Planners can model and simulate engagements against specific adversary forces, doctrine, and tech. By altering variables (e.g., different weather, geography, or enemy tactics), you can evaluate strengths, weaknesses, and gaps in current U.S. capabilities.
- **Red vs Blue A/B Testing:** You could continuously pit U.S. forces against AI-driven adversaries that learn and adapt, testing not just equipment but doctrine, comms resilience, and interoperability.
- **Data-Driven Decision Making:** Simulations generate structured performance data for AI-assisted analysis, helping leaders make informed budgetary or strategic decisions.
- **Wargaming at Scale:** You can test deployment strategies (e.g., mass mobilization or distributed lethality scenarios) with realistic physics, logistics, and outcomes.
- **Realistic Operator Training:** Sailors and officers could train on true-to-life systems, including shipboard networks and sensor environments, in peacetime and during emerging crises.
- **Joint Force Readiness:** Assets across services can be digitally integrated into operations, helping assess true joint operational effectiveness before the real-world call.
- **Transparency with Strategic Ambiguity:** If adversaries know the U.S. has such a capability constantly simulating and adapting to emerging threats it signals unmatched preparedness and adaptability.
- **Global Influence:** Allies would likely seek to participate, creating a combined deterrent effect and better-integrated coalitions.



Challenges

Developing a Joint Integrated Validation Environment (JIVE) presents several complex challenges that span technical, organizational, cultural, and managerial domains.

- 1. Legacy Processes, Organizational Structure, Cultural and Institutional Resistance**
Current validation methods rely on traditional, sequential processes that are not optimized for rapidly evolving technology. The existing organizational structures within the DOD are not designed for a fully integrated, joint digital ecosystem, leading to fragmentation and duplication of effort. Implementing a JIVE requires significant changes in organizational culture and processes. Resistance may stem from entrenched practices, fear of obsolescence, or skepticism about new methodologies. Overcoming this resistance involves not only technological solutions but also change management strategies to foster acceptance and collaboration across different military branches and departments.
- 2. Creating Properly Aligning Interests within the Military and Industrial Base.**
A significant challenge in establishing a Joint Integrated Validation Ecosystem (JIVE) is the scarcity of truly independent, high-tech integrators capable of rapidly validating best-of-breed capabilities across domains. While some government labs assert, they should lead this function, they are often constrained by bureaucratic processes, long procurement timelines, and institutional cultures that are not optimized for agile, mission-driven integration. At the same time, many defense contractor capability providers favor proprietary systems that create lock-in and limit interoperability, which directly conflicts with the open, modular validation model JIVE requires. These dual pressures from institutional resistance and vendor self-interest complicate efforts to stand up an independent validation layer that is both fast-moving and trusted by the operational community. Overcoming this requires both new business models and leadership commitment to a neutral, unconflicted integration function.
- 3. Data Security and Sensitivity**
Handling sensitive operational data within a JIVE necessitates robust cybersecurity measures. Ensuring data confidentiality, integrity, and availability while facilitating real-time data sharing across multiple platforms and services is challenging. Moreover, balancing the need for data accessibility with stringent security protocols can impede the fluid exchange of information essential for effective validation.
- 4. Resource Allocation and Funding**
Developing and maintaining a JIVE is resource-intensive, requiring sustained investment in technology, personnel, and infrastructure. Securing consistent funding amidst competing priorities poses a significant challenge. Additionally, aligning budgetary allocations across various departments and services to support a joint initiative demands coordinated planning and commitment. Aligning incentives and creating sustainable business models that encourage independent and continuous validation remains challenging. This includes obtaining adequate funding and investment to support continuous modernization of the validation infrastructure.



Addressing these challenges necessitates a holistic approach that combines technological innovation with strategic planning, stakeholder engagement, and robust governance structures. By proactively identifying and mitigating these obstacles, the Department of Defense can enhance its capability validation processes to meet the demands of modern warfare.

Bottom Line

Despite perceptions of complexity, the technologies needed to build and sustain JIVE/THRIVE already exist and are far less challenging than those used in the development of many modern weapons systems. While initial investment is required, the cost of implementing a digitally enabled, continuously validated architecture will be significantly lower than the cumulative costs of delays, duplicative testing, and the operational risks of fielding unvalidated systems. Proven commercial models already demonstrate this approach: Tesla uses real-world driving data and digital twins to validate and improve its autonomous software in real time; SpaceX treats each launch as a live experiment, incorporating feedback into rapid design iteration; and Amazon Web Services continuously validates its global infrastructure through automated test and monitoring frameworks. These examples reinforce that JIVE/THRIVE is not only technologically feasible but strategically essential. In an era where speed and adaptability are decisive, JIVE/THRIVE represents a national security imperative.