



Real-time AI powered summary

CREATIVE DISRUPTORS BY THE LAKES

Powered by the Creative Defense Foundation



POWERED BY

COLLABORATION.AI

+

BUILT WITH



IN

MN

The opening session established a clear sense of urgency, framing the strategic imperative for the U.S. defense ecosystem to accelerate innovation in the face of rapidly advancing adversaries, particularly China. Congressional leaders and Department of War (DoW) officials underscored the need for a fundamental shift in acquisition, procurement, and collaboration. The discussion highlighted a strong bipartisan consensus on the need to reform legacy processes, empower innovators, and leverage the entire national industrial and technological base to maintain a decisive military advantage.





Opening Remarks

Key Themes

- **Accelerating Innovation to Counter Pacing Threats:** The central theme was the critical need to move faster than adversaries. It was noted that China is actively copying U.S. innovation models and scaling them at a much faster rate, creating a significant strategic challenge. The discussion stressed that the nation is "out of time" and must shift from legacy processes to a posture of rapid capability development and deployment to maintain deterrence.
- **Fundamental Acquisition and Requirements Reform:** Panelists called for a dramatic overhaul of how the DoW buys technology. This includes moving toward a problem-centric model where the DOW identifies operational challenges and industry is invited to identify promising technology and propose solutions. The goal is to unlock innovation from a broader industrial base and shorten the timeline from idea to fielded capability.

Key Themes

- **The Imperative of Bipartisan and Public-Private Collaboration:** The strong presence of bipartisan congressional leaders was highlighted as a key enabler for change. Speakers emphasized that national security transcends politics and that a united front in Congress is essential for passing budgets on time and avoiding damaging Continuing Resolutions (CRs). This partnership must extend to the private sector, creating clearer pipelines for innovators to engage with the DoW.
- **Leveraging Regional Innovation and the Industrial Base:** There was significant focus on cultivating regional ecosystems as hubs for defense innovation, citing examples in Minnesota for hypersonics, biotechnology, and unmanned underwater vehicle testing. Panelists stressed the need to engage innovators, manufacturers, and academic institutions across all 50 states, ensuring the entire national industrial base is mobilized to support national security objectives.



Opening Remarks

Actionable Recommendations

- **Establish a formal communication channel** between Congress, DoW Research and Engineering (R&E), and the private sector to prioritize technology areas and speed the evaluation and funding of promising new capabilities.
- **Reform the budgeting process** to eliminate the persistent use of Continuing Resolutions (CRs), which delay new programs and stifle innovation, and provide the DoW with predictable, stable funding.
- **Shift procurement from prescriptive requirements** to outcome-based problem statements, allowing industry to propose innovative solutions rather than bidding on rigid specifications.

Key Challenges

- **Bureaucratic Inertia:** The old procurement processes within the DoW are deeply entrenched, making it difficult to implement agile and innovative approaches despite broad agreement on the need for change.
- **Adversary Speed:** Competitors, notably China, are innovating, copying, and scaling capabilities at a pace that far exceeds the current U.S. acquisition cycle, eroding America's technological overmatch.
- **Fiscal Instability:** The persistent threat of full-year Continuing Resolutions creates significant uncertainty, stalls new program starts, and prevents the DoW from making long-term strategic investments.

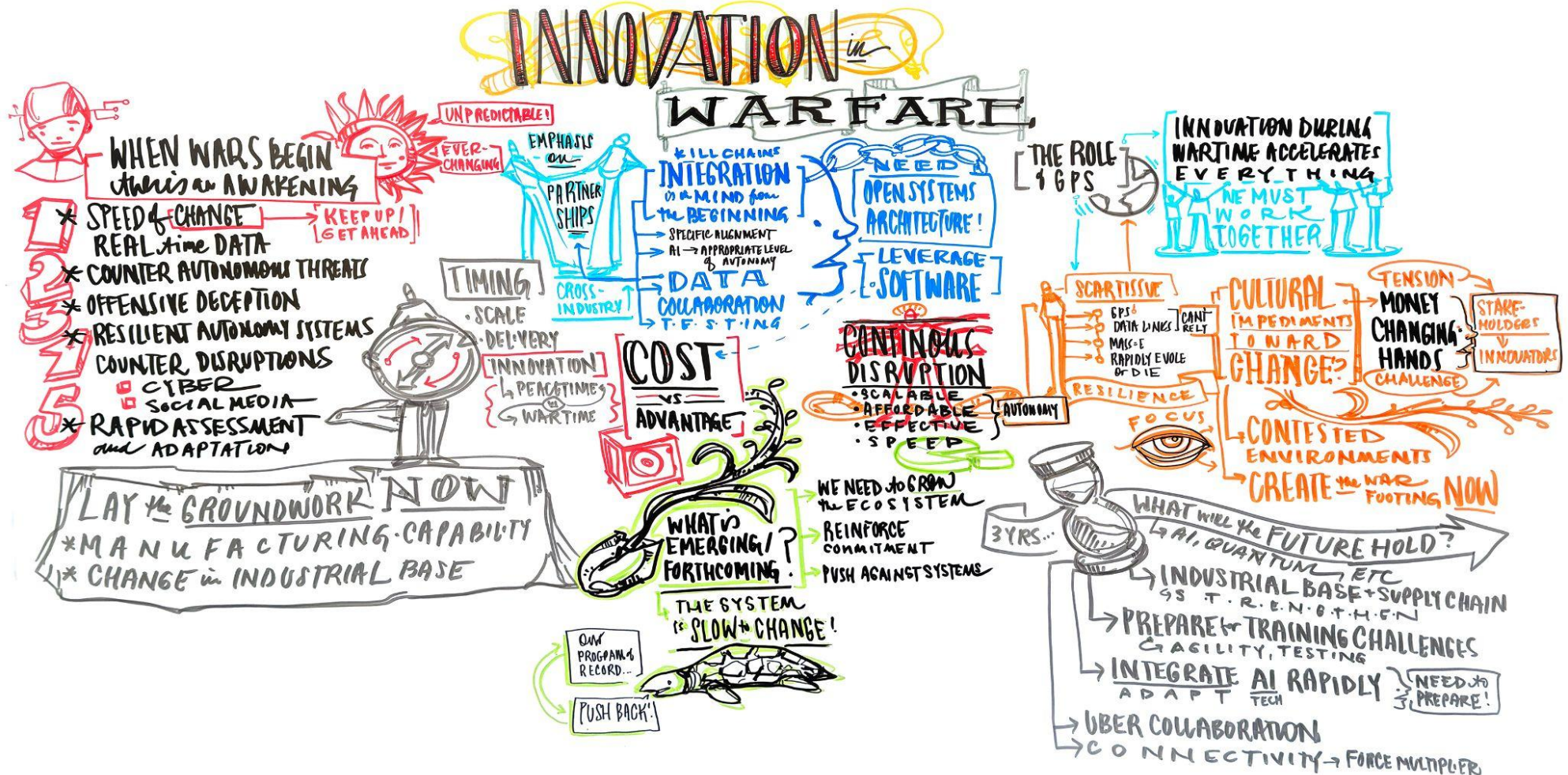
Additional Insights

- A specific, alarming example was raised of China announcing plans to build 27 bio-industrial facilities by 2027, directly copying a U.S. strategy (BioMADE) that is still working on its first few sites.
- A key cultural shift proposed for the DoW is moving from asking industry "come bid on this specific thing" to asking "here is the problem we are trying to solve, what can you bring to the table?"
- There is a recognition that Congress shares responsibility for the risk-averse culture in the DoW, as its oversight processes can often penalize failure, which in turn stifles innovation and responsible risk-taking.

Panel: Innovation in Warfare

Summary

The panel examined the paradigm shift in modern warfare, driven by the proliferation of inexpensive, autonomous systems. Discussions, framed by a speculative China-Taiwan conflict scenario, highlighted the massive gap between the rapid, chaotic nature of the contemporary battlefield (e.g., Ukraine) and the slow, risk-averse U.S. defense acquisition and industrial ecosystem. The core imperative is for the Department of War (DoW) to move from a peacetime innovation cycle to a wartime stance, emphasizing speed, adaptability, multi-vendor integration, and overcoming deep-rooted institutional inertia.





Panel: Innovation in Warfare

Key Themes

- **The New Battlefield Reality:** Warfare is now defined by the saturation of low-cost, highly capable autonomous systems. The conflict in Ukraine demonstrates a fundamental shift from traditional munitions to attritable drones at an unprecedented scale, demanding a new doctrine focused on mass production and affordability over exquisite, high-cost platforms.
- **Wartime vs. Peacetime Innovation:** A stark contrast exists between peacetime's slow, bureaucratic processes and wartime's demand for innovation in hours or days. The Israeli experience in Gaza illustrates how operational necessity forces rapid adaptation in degraded environments (e.g., no Global Positioning System, no communications) and creates true government-industry partnerships. The U.S. must adopt this mindset before a conflict begins.

Key Themes

- **Open Systems and Integration:** Victory in future conflicts will depend on seamlessly integrated, multi-vendor kill chains. This requires a mandate for open systems architecture, allowing for the rapid incorporation of best-of-breed capabilities from across the industrial base, from large primes to startups, regardless of the military branch operating the system.
- **Institutional and Cultural Inertia:** The primary barrier to innovation is not a lack of technology but a DoW culture that protects legacy programs of record. Program offices are incentivized to maintain long-term funding streams, actively resisting disruptive technologies that could deliver superior capability faster but threaten established budgets and stakeholder interests.
- **Industrial Base and Resilience:** The U.S. faces a critical vulnerability due to its diminished manufacturing capacity and reliance on foreign supply chains for key components. Sustaining a high-tempo conflict requires a robust domestic industrial base to produce systems at scale. Furthermore, technology must be designed for resilience, assuming that GPS and communications will be denied.



Panel: Innovation in Warfare

Actionable Recommendations

- **Replicate Wartime Conditions:** Establish a war stance during peacetime by creating dedicated, contested test environments to force rapid adaptation and innovation for operations in GPS-denied and communications-denied settings.
- **Reform Funding Mechanisms:** Create agile funding pools and grant authorities to move resources from underperforming legacy programs to proven, innovative solutions, bypassing the institutional resistance inherent in the current budget cycle.
- **Mandate Open Architectures:** Enforce open system standards for all new programs to break vendor lock and ensure capabilities from multiple industry partners can be integrated at speed.
- **Rebuild the Industrial Base:** Launch a national initiative to onshore the manufacturing of critical defense components (e.g., microelectronics, motors, radios) to ensure the ability to produce autonomous systems at scale.

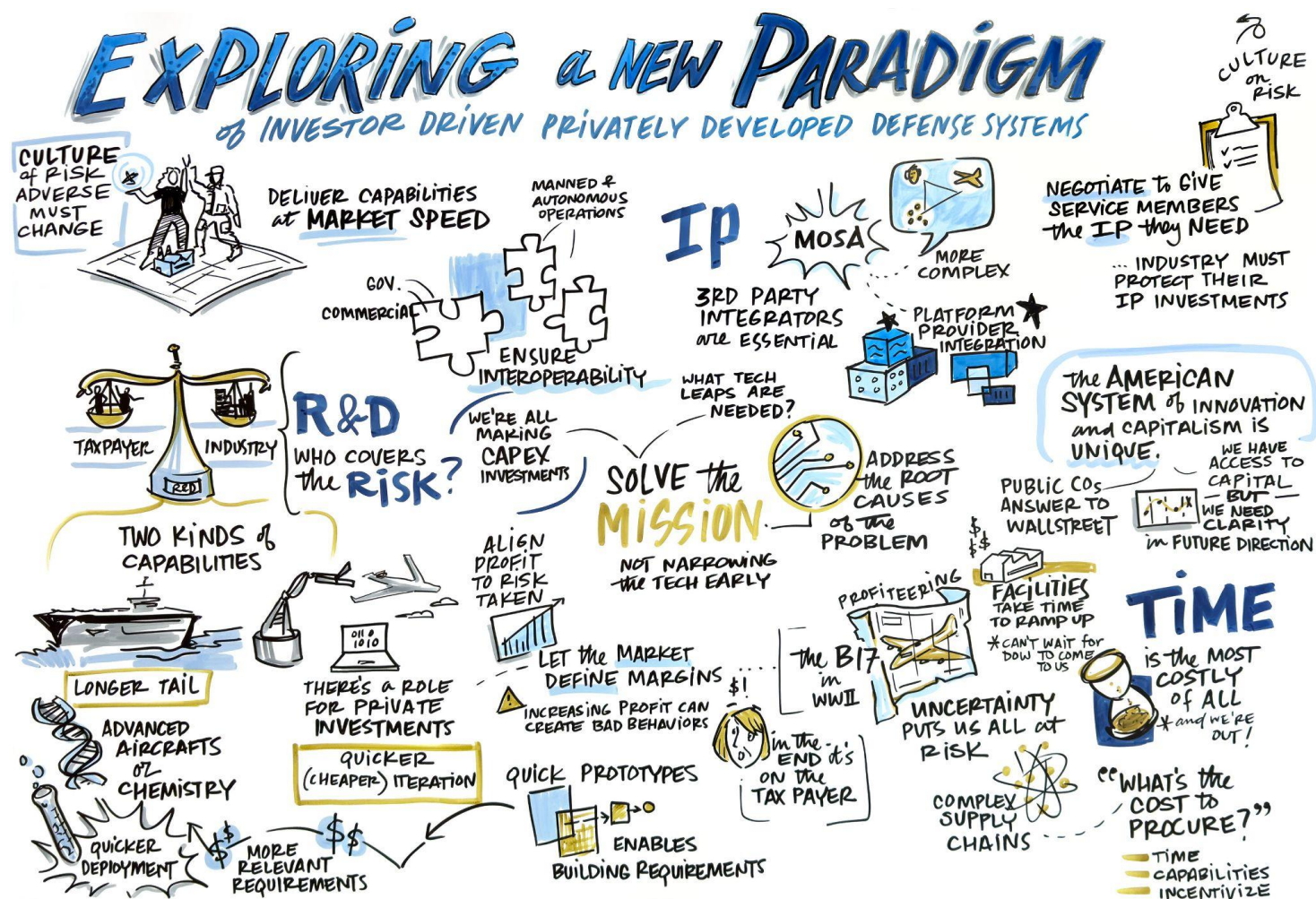
Key Challenges

- **Acquisition Culture:** The DoW's risk-averse culture and misaligned incentives reward process adherence over rapid capability delivery, stifling the adoption of disruptive technologies.
- **Manufacturing at Scale:** The domestic industrial base lacks the capacity to produce attritable drones and other autonomous systems at the speed and volume required for a peer-level conflict.
- **Contested Logistics:** Maintaining operational tempo in an environment where adversaries can deny GPS, jam communications, and create mass sensor confusion remains a primary operational challenge.
- **Training for Autonomy:** The services have not yet developed the training and doctrine required to equip warfighters to operate effectively alongside and against tens of thousands of autonomous systems.

Additional Insights

- The unsustainable cost-exchange ratio of using multi-million dollar interceptors against low-cost drones necessitates a fundamental shift toward affordable, scalable counter-autonomy solutions.
- Future conflicts will be preceded by intense legal, psychological, and cyber warfare designed to paralyze decision-making before the first shot is fired.
- The most significant challenge in acquisition reform is not creating new programs but forcing the reallocation of funds from entrenched incumbent stakeholders to disruptive innovators.

This session explored the necessity of adapting Department of War (DoW) business models to harness private capital for battlefield innovation. The core discussion focused on creating new risk/reward structures that recognize privately funded research and development, establishing methods to manage intellectual property without stifling speed, and overcoming the deep-seated cultural and bureaucratic inertia that prevents the DoW from fully leveraging the U.S. free-market system as a strategic advantage against state-controlled adversaries.



Panel: Exploring a New Paradigm of Investor Driven Privately Developed Defense Systems



Key Themes

- **Rebalancing Risk and Reward for Private Capital**
 - The current acquisition model, designed for government-funded development, is misaligned with privately-funded innovation. Procurement must differentiate between taxpayer versus private assumption of risk.
 - Profit margins should be defined by market competition and the value of the delivered capability, not by archaic guidelines. The current system fails to account for company-funded Non-Recurring Engineering (NRE) expenses when evaluating production costs.
- **Managing Inevitable Proprietary Interests**
 - Proprietary instincts are a natural outcome of government and private research models. A Modular Open Systems Approach (MOSA) is insufficient, as it can be subverted by subtle proprietary components.
 - Neutral, third-party integrators are required to validate system openness and ensure interoperability, breaking the cycle of developers self-certifying their own products.

Key Themes

- **The Operational Integration Barrier**
 - The "valley of death" for new technology is the complex, costly, and time-consuming process of certification and integration onto operational platforms (e.g., Authority to Operate (ATO), airworthiness).
 - Without a dedicated process to shepherd new systems through operational integration, private investment is wasted on capabilities that never reach the warfighter.
- **Cultural and Systemic Inertia as the Core Obstacle**
 - The DoW's risk-averse culture is the greatest impediment to reform. Personnel are reluctant to use the flexible acquisition authorities that Congress has already provided.
 - The system has become overly focused on managing existing processes, resulting in a bureaucracy that prioritizes compliance over speed and mission outcomes.

Panel: Exploring a New Paradigm of Investor Driven Privately Developed Defense Systems



Actionable Recommendations

- Establish a dedicated operational integration organization to actively shepherd non-traditional and privately developed technologies through platform certification and testing.
- Adopt business models where procurement pricing and profit are defined by the market, fairly assessing which party, either the government or the private sector, shouldered the initial development risk.
- Shift from rigid program-based budgeting to portfolio-based models that fund mission capabilities, allowing for greater flexibility and resource allocation to the most effective solutions.

Key Challenges

- The DoW's pervasive risk-averse culture prevents the effective use of existing innovative acquisition authorities and stifles rapid capability fielding.
- Unstable budgets and contract uncertainty deter the long-term private capital expenditures (CapEx) necessary for building a robust and modern industrial base.
- A fundamental disparity in costs for facilities creates an uneven playing field, where new entrants must self-fund facilities to compete against incumbents who historically benefited from government-supported infrastructure.

Additional Insights

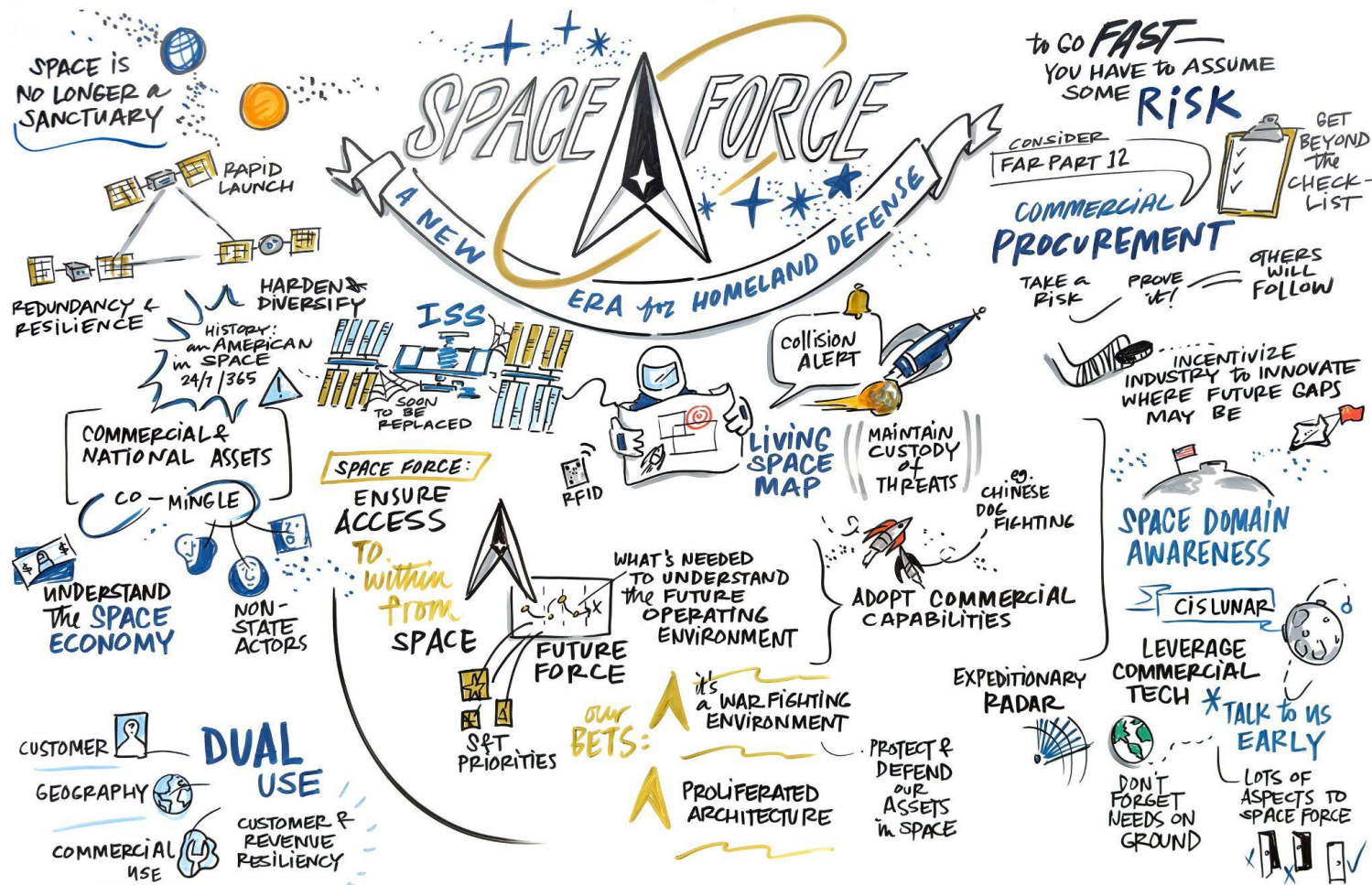
- A prevailing sentiment was that the U.S. acquisition system has "out-Sovietized the Soviet Union," creating a slow, centrally planned model that negates America's core advantage of free-market capitalism.
- A clear distinction must be made between two capability types: enduring, exquisite systems (e.g., aircraft carriers) and attributable, mass-producible systems (e.g., drones). Each requires a fundamentally different business and acquisition model.
- The time and expense of getting a capability from development to operational deployment is the most critical cost factor, far outweighing debates over profit margins.

Panel: Space Force – A New Era for Homeland Defense



Summary

This panel examined the increasingly contested space domain, highlighting the strategic imperative for resilience against adversary threats. Featuring leaders from the U.S. Space Force and dual-use technology companies, the discussion centered on the critical role of commercial innovation in providing Space Domain Awareness (SDA) and other vital capabilities. A primary focus was the urgent need for the Department of War (DoW) to reform cumbersome acquisition processes and fully leverage private capital to maintain a decisive strategic edge in space.



Panel: Space Force – A New Era for Homeland Defense



Key Themes

- **The Contested Domain and the Need for Resilience**
 - Adversaries, particularly China, are rapidly advancing counter-space capabilities, including direct-ascent anti-satellite (ASAT) weapons, co-orbital systems, and jamming technologies.
 - Resilience is a core warfighting imperative. The Space Force is prioritizing a shift toward proliferated Low Earth Orbit (LEO) architectures and rapid reconstitution capabilities to ensure mission continuity under attack.
- **Commercial Innovation as a Strategic Force Multiplier**
 - The commercial sector is outpacing the government in developing and deploying critical space technologies, especially in SDA.
 - Adopting a "buy what you can, build what you must" strategy, leveraging commercial services like SDA-as-a-service, allows the Space Force to focus finite resources on unique military requirements, such as Cislunar domain awareness.

Key Themes

- **Overhauling Acquisition for Speed and Agility**
 - Legacy acquisition processes are fundamentally misaligned with the speed of commercial space development, creating significant barriers to integration.
 - A call was made to re-invigorate the use of commercial procurement authorities, such as Federal Acquisition Regulation (FAR) Part 12, to streamline acquisitions and empower contracting officers to prioritize speed and accept managed risk.
- **Space Domain Awareness as the Foundation for Warfighting**
 - SDA was identified as a top Science and Technology (S&T) priority; simply stated, you cannot fight if you are blind.
 - Commercial ground-based radar networks are filling critical gaps in government sensor coverage, particularly in the Southern Hemisphere, enabling persistent tracking of adversary maneuvers.

Panel: Space Force – A New Era for Homeland Defense



Actionable Recommendations

- **Mandate Use of Commercial Procurement:** Enable direct acquisition authorities to utilize commercial contracting vehicles like FAR Part 12 for proven space capabilities, reducing timelines and bureaucracy.
- **Bridge the "Valley of Death":** Establish clear and predictable funding pathways for commercial technologies that successfully complete pilot programs like STRATFI, ensuring a transition to operational use.
- **Ensure U.S. LEO Presence:** Prioritize the public-private partnership to field a commercial replacement for the International Space Station (ISS) to prevent a gap in U.S. human spaceflight capability.

Key Challenges

- **Bureaucratic Inertia:** A risk-averse culture within the acquisition workforce hinders the adoption of agile, commercial-first procurement models.
- **Process Misalignment:** The slow, rigid government budgeting and requirements cycle is incompatible with the fast-paced, privately funded development of commercial space capabilities.
- **Pacing Threat:** China's rapid fielding of thousands of new satellites and development of counter-space weapons challenges the DoW's ability to deploy resilient architectures at a relevant speed.

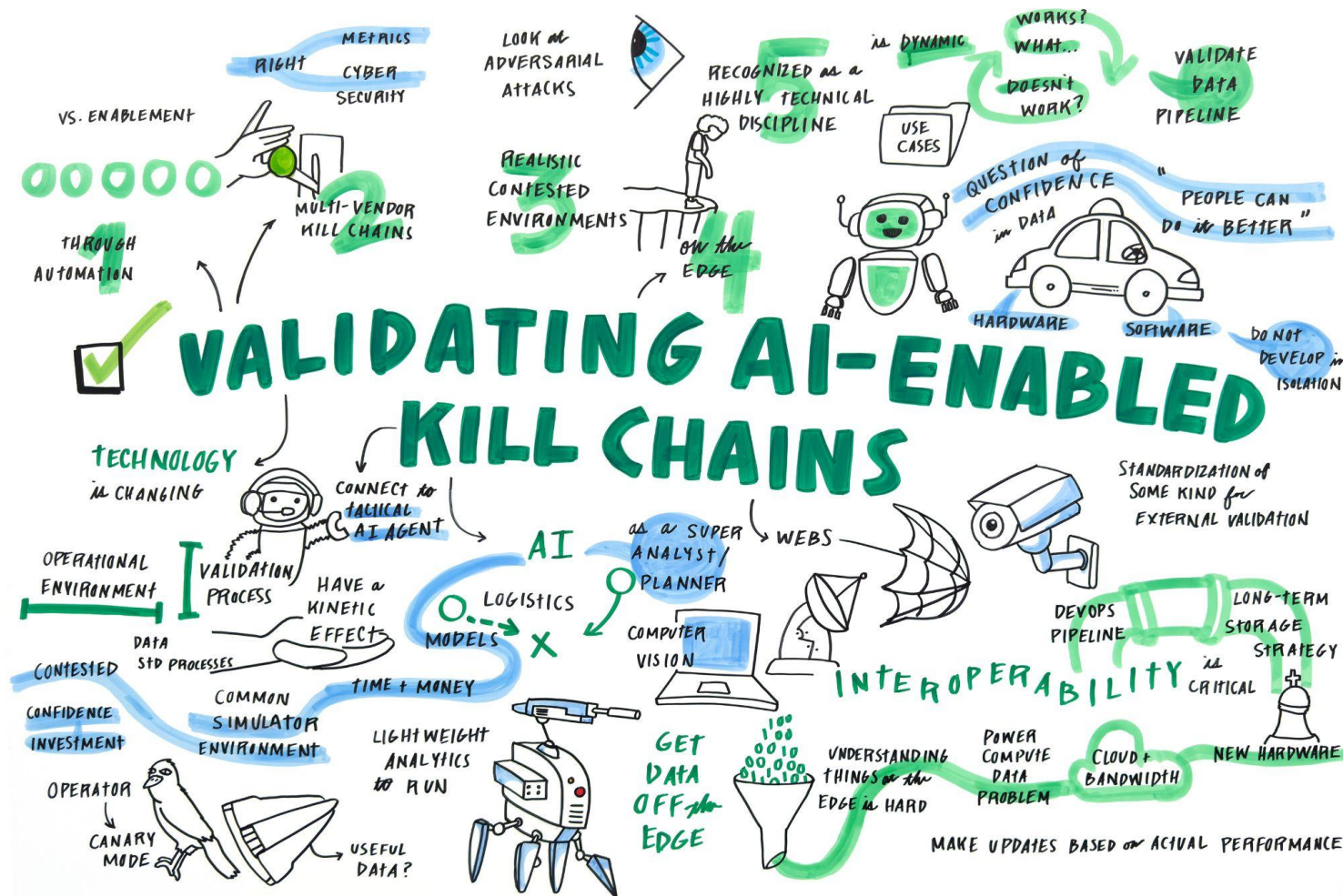
Additional Insights

- A potential shift in U.S. policy to a "part-time" human presence in space post-ISS deorbiting presents a significant strategic risk, potentially ceding persistent LEO dominance to China.
- The ground segment is a critical but often overlooked vulnerability, with many DoW operational systems lagging far behind commercial counterparts in automation, artificial intelligence, and user-interface design.
- The development of expeditionary, mobile sensor platforms offers a new layer of resilience and operational flexibility for tactical space domain awareness.

Panel: Validating AI-Enabled Kill Chains

Summary

This panel addressed the paradigm shift required to validate AI-enabled kill chains. The discussion framed the legacy model of episodic, end-of-cycle testing as obsolete for dynamic AI systems. Using the self-driving car as an analogy for the immense scale of testing now required, panelists explored the necessity of a continuous validation process that begins during development and extends through operational use. Central themes included building confidence through data, creating realistic contested test environments, and establishing robust data pipelines from the edge to enable rapid adaptation and revalidation.





Panel: Validating AI-Enabled Kill Chains

Key Themes

- **A New Paradigm for Validation:** The current approach of validating a final software instance is untenable. The focus must shift to validating the entire development pipeline, enabling continuous integration, testing, and deployment. This model treats validation not as a final gate but as an ongoing process that ensures systems are safe, effective, and adaptable. The scale of this challenge is several orders of magnitude greater than for traditional systems.
- **The Centrality of the Data Pipeline:** Trustworthy AI requires a constant feedback loop. A robust, rapid pipeline is needed to harvest operational data from assets at the edge, analyze it to understand performance against an adaptive adversary, and feed those insights back to refine algorithms. This cycle of learning, updating, and redeploying is fundamental to maintaining a decision advantage.

Key Themes

- **Integrated, Multi-Vendor "Kill Web" Testing:** AI systems cannot be validated in isolation. Testing must occur within a complex, multi-vendor "kill web" context to identify and resolve critical interoperability failures. This requires common, high-fidelity, simulated environments that accurately represent the platforms, sensors, and networks the AI will interact with during operations.
- **Confidence as the Decisive Factor:** The ultimate measure of success is a commander's confidence in the AI's recommendations and actions, especially in a complex, high-stakes environment. This confidence is built not through traditional documentation but through continuous exposure, performance characterization, shadow mode operations, and data-driven evidence of reliability under contested conditions.



Panel: Validating AI-Enabled Kill Chains

Actionable Recommendations

- Invest in and field a standardized, resilient data pipeline to ensure operational and test data can be rapidly collected from the edge, analyzed, and used to update AI models.
- Establish common, government-provided, high-fidelity, virtual environments to allow for the continuous integration and testing of multi-vendor AI systems throughout the development lifecycle.
- Deploy lightweight analytical tools to the edge to pre-process data locally, enabling the transmission of critical insights over low-bandwidth or contested communication networks.
- Prioritize the validation of the entire development and deployment factory over single software instances, ensuring the Department of War (DoW) can rapidly and safely iterate capabilities.

Key Challenges

- **Data Availability and Access:** Many currently deployed assets lack the instrumentation to collect and transmit the high-quality data needed for AI training and validation.
- **Multi-Vendor Integration:** Mismatched software interfaces and incongruent AI world models between vendors create significant integration failures and performance degradation in a kill web.
- **Replicating a Dynamic Adversary:** Creating realistic test environments that represent a thinking, adaptive adversary, rather than a static threat, remains a significant technical hurdle.
- **Cultural and Process Inertia:** The shift from a document-centric, linear validation process to a continuous, software-centric model requires a significant cultural change within the acquisition and testing communities.

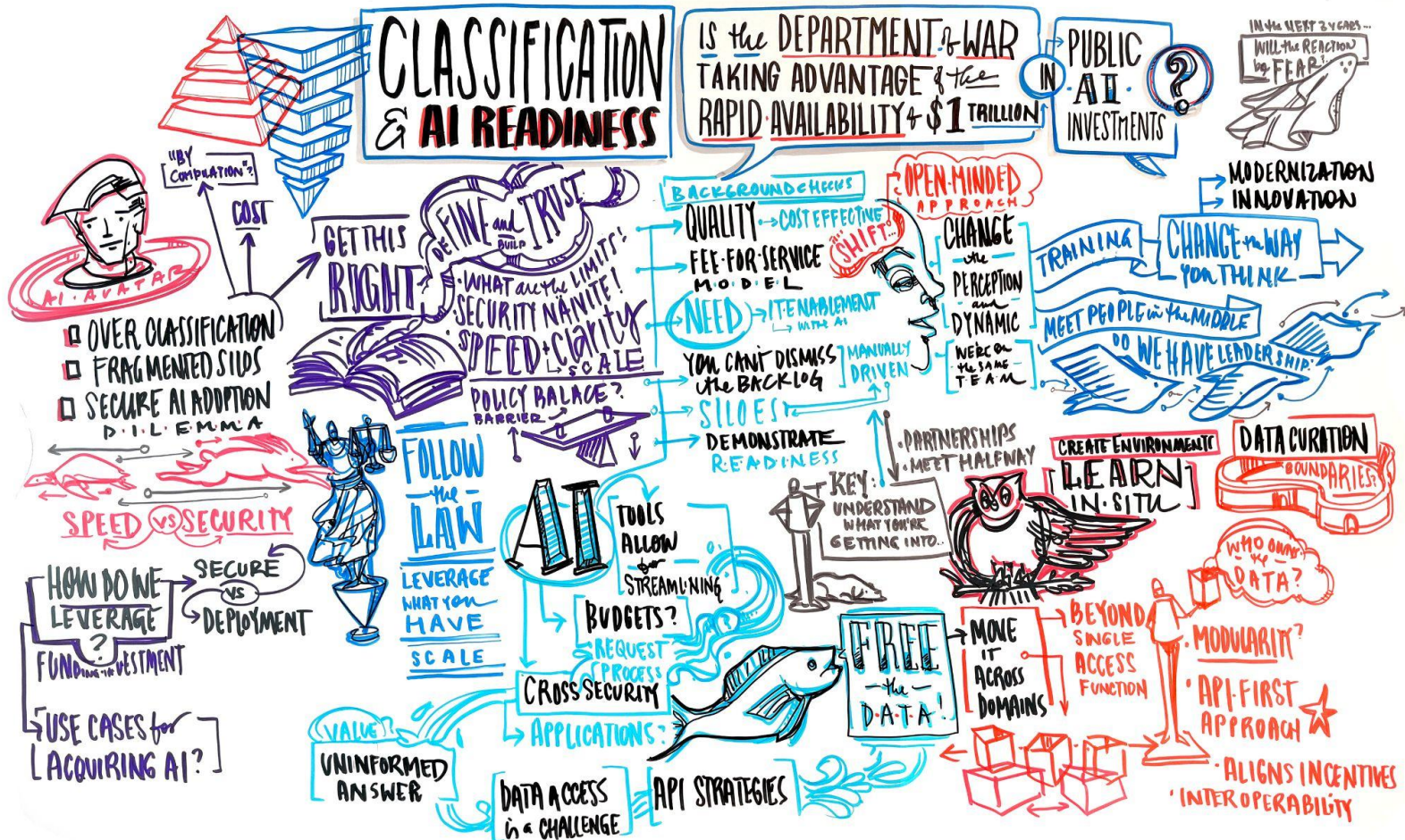
Additional Insights

- The concept of operational testing is being redefined by real-world events. A few days of modern conflict can generate more relevant performance data than decades of traditional range testing.
- Validation must address "value-laden" decisions, as an AI may be forced to make choices between undesirable outcomes, similar to the ethical dilemmas faced by self-driving cars.
- Interoperability is a primary point of failure; a lack of common interface standards for AI models creates significant friction, cost, and delays during integration events.

Panel: Classification & AI Readiness

Summary

This session examined the critical friction between the Department of War's (DoW) legacy classification and security frameworks and the urgent need to leverage commercial Artificial Intelligence (AI) innovation. The discussion centered on how over-classification, fragmented data silos, and slow accreditation processes handicap the DoW while adversaries rapidly adopt commercial AI to gain a decisive advantage. Key proposals focused on policy reform, modernizing security frameworks to match acquisition speed, and fostering a cultural shift to embrace data-driven, AI-enabled capabilities at the speed of relevance.





Panel: Classification & AI Readiness

Key Themes

- **Over-classification as a Strategic Drag:**
 - Excessive classification drives massive costs, hinders data sharing with allies and industry, and complicates the training of effective AI models.
 - A significant amount of classified material is derived from open-source information, which adversaries are already exploiting with their own AI tools. This creates a self-imposed information disadvantage for the U.S.
- **The Cross-Domain Data Dilemma:**
 - Warfighting occurs at the Secret level, but critical intelligence resides on Top Secret/Sensitive Compartmented Information (TS/SCI) networks. Current cross-domain solutions are ill-suited for tactical warfighting environments.
 - This fragmentation results in AI algorithms being trained on incomplete data, creating a risk of providing uninformed or dangerously inaccurate outputs to warfighters at the edge.

Key Themes

- **Misalignment of Speed Between Acquisition and Security:**
 - While acquisition reforms like the Software Pathway have enabled rapid capability development, they are undermined by a multi-year budgeting cycle and security policies that have not been modernized at the same pace.
 - The result is a system where technology can be acquired quickly, but the funding and security accreditation processes remain significant bottlenecks to deployment.
- **A Call for Practical Implementation and Partnership:**
 - Many legal authorities for reform already exist, but consistent execution at the implementation level is lacking. The focus must shift to enforcing existing policies, such as "buy commercial first."
 - Industry bears a co-equal responsibility to build systems designed for secure environments from inception, creating a more effective partnership with agencies like the Defense Counterintelligence and Security Agency (DCSA).



Panel: Classification & AI Readiness

Actionable Recommendations

- Mandate an "API-First" strategy for all new systems to ensure data is architected for accessibility and interoperability, preventing data stovepipes and enabling broader AI/ML applications.
- Aggressively leverage AI to streamline internal security processes, including managing the massive backlogs from continuous vetting alerts and assisting in the declassification of an ever-growing volume of information.
- Re-evaluate "classification by compilation" policies in the AI era. Information derived by AI from unclassified public sources should not be reflexively classified, as adversaries already possess this capability.

Key Challenges

- The rigid, two-year budgeting process remains a fundamental structural barrier to fielding AI capabilities at the speed of commercial innovation.
- Legacy security frameworks, some dating back to the early 1990s, are not fit for purpose in a modern technology landscape dominated by software and data.
- A risk-averse culture within the security and acquisition workforces prevents the full and intended use of agile authorities that have already been granted by Congress.

Additional Insights

- A significant cultural transformation is underway within DCSA to shift its posture from a compliance-focused auditor to a collaborative partner, offering pre-audit consultations to help industry accelerate security approvals.
- The rise of Large Language Models (LLMs) poses a novel challenge to classification. An LLM analyzing unclassified public data (e.g., budget documents) can infer and articulate strategic priorities, blurring the line between public information and classified insight.

Executive Session: Securing the Arsenal



Summary

This session focused on the proposed Civil Reserve Manufacturing Network (CRMN), examining how to rebuild the defense industrial base for surge capacity. The discussion defined the problem of fragile, multi-tier supply chains and explored solutions through advanced technology like AI-driven supply chain mapping and automated manufacturing. Panelists addressed systemic barriers, including bureaucratic qualification processes, workforce shortages, and the need for new models to incentivize commercial industry participation, framing the CRMN as a critical pilot program to test these solutions.



Executive Session: Securing the Arsenal

Key Themes

- **Supply Chain Fragility and Obscurity**
 - The defense industrial base is not a broad pyramid but a series of fragile "diamonds," with critical single points of failure several tiers down in the supply chain.
 - Examples such as specialized magnesium casters, precision ball bearings, and high-purity quartz for microelectronics illustrate how the entire ecosystem depends on a few, often vulnerable, low-volume suppliers.
- **Technological Enablers for Resilience**
 - A core theme was the application of modern technology to solve industrial base challenges. This includes using Artificial Intelligence (AI) to create multi-tier digital twins of supply chains for real-time risk analysis.
 - Leveraging software-driven autonomous factories enables flexible, high-mix, low-volume production that can pivot between commercial and defense needs, significantly increasing efficiency.

Key Themes

- **Reforming Qualification and Acquisition**
 - Bureaucratic processes were identified as significant constraints. The lengthy and costly time required to test and qualify new components or second-source suppliers is a major barrier to entry for commercial firms.
 - The conversation pointed to overly restrictive military specifications and testing requirements as self-inflicted wounds that unnecessarily limit the supplier base and stifle agility.
- **The Skilled Workforce Crisis**
 - A persistent challenge identified was the severe shortage of skilled manufacturing labor, from welders to inspectors.
 - This is compounded by the retirement of an aging workforce, the geographic isolation of key defense manufacturing hubs, and a gap between trade school education and the practical skills needed on the factory floor.



Executive Session: Securing the Arsenal

Actionable Recommendations

- Utilize AI-driven analysis to map critical weapons systems' supply chains, identifying not just component bottlenecks but also constraints caused by overly burdensome military specifications and testing protocols.
- Direct the initial \$131M CRMN funding toward qualifying existing commercial suppliers for critical needs (e.g., castings, forgings) by streamlining testing and validation processes.
- Shift from direct government funding of capital expenditures (CapEx) to using structured off-take agreements, which provide guaranteed demand signals to de-risk and attract private capital for factory construction.
- Implement programs to subsidize the first year of wages for new manufacturing apprentices to bridge the gap between training and on-the-job productivity, incentivizing small businesses to hire talent.

Key Challenges

- Extreme fragility in lower-tier supply chains, where single-source domestic suppliers for critical components like precision ball bearings or castings create system-wide risk.
- Bureaucratic inertia, particularly slow and expensive testing and qualification processes that deters new commercial entrants and delays the adoption of alternative suppliers.
- A critical shortage of skilled manufacturing labor, exacerbated by an aging workforce and the inability to attract new talent to geographically isolated defense production hubs.
- Misaligned incentives where commercial firms avoid the defense market due to complex regulations, low margins, and the difficulty of navigating DoW (Department of War) procurement.

Additional Insights

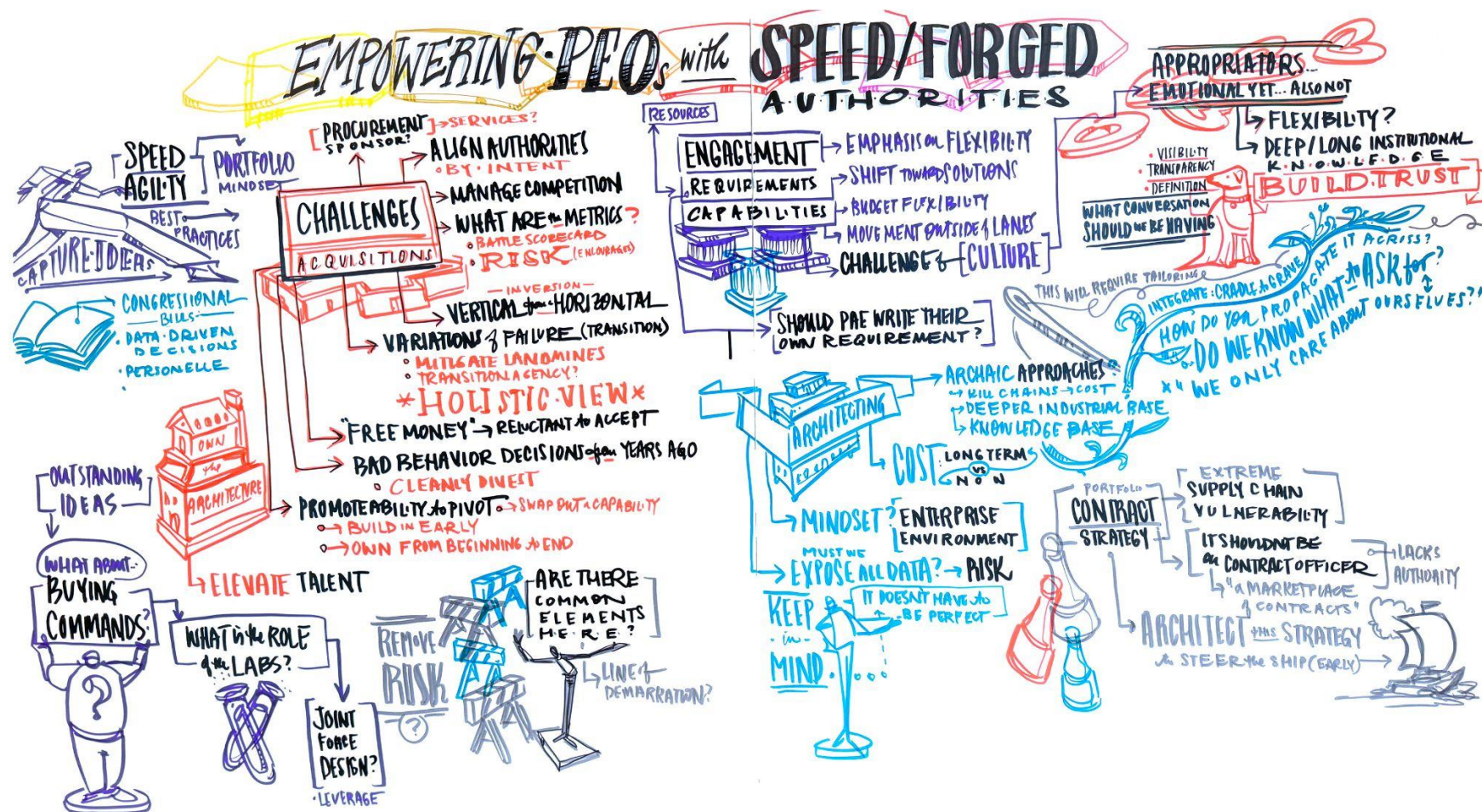
- The conceptual reframing of supply chains from broad pyramids to a series of fragile "diamonds" reveals that chokepoints are the norm, not the exception.
- A strong argument was made against direct government funding for manufacturing CapEx, proposing instead the use of commercial models like structured off-take agreements to attract private capital.
- Generative AI is a disruptive force that could reduce the demand for traditional software coders, potentially creating a new pool of tech-savvy talent for modern, automated manufacturing roles.

Workshop A: Empowering PEOs with SPEED/FORGED Authorities



Summary

This workshop explored how empowering Program Executive Officers (PEOs) through the SPEED/FORGED Acts can accelerate capability delivery. The discussion focused on shifting from rigid, program-centric management to an agile, portfolio-based model. Participants identified systemic barriers in budgeting, requirements, and contracting that hinder innovation and proposed that a portfolio structure with concentrated authority is essential to manage competition, integrate technology, and make critical trade-offs between cost, schedule, and performance to meet warfighter needs.



Workshop A: Empowering PEOs with SPEED/FORGED Authorities



Key Themes

- **Shift to Empowered Portfolio Management:**
A consensus emerged on moving from isolated programs to integrated portfolios. This requires a Portfolio Acquisition Executive (PAE) with concentrated authority over requirements, budget, and acquisition to manage competition and make trade-offs across capabilities.
- **Achieving Fiscal and Requirements Agility:**
Rigid budget line items and a locked-down requirements process were cited as primary blockers. Participants advocated for consolidating budget lines into capability areas and adopting an "acquire-to-require" model to allow for iterative development with warfighter feedback.

Key Themes

- **Enterprise Digital Engineering and Architecture:** A portfolio structure must be built on a common digital foundation. Implementing enterprise-wide digital twins and a Modular Open Systems Approach (MOSA) from the start is essential to enable integration, competition, and continuous modernization.
- **Cultural Reform Through New Incentives:**
The prevailing risk-averse culture is a major impediment. It was noted that changing the paradigm requires new metrics beyond budget execution, such as a "balanced scorecard" that incentivizes leaders to take calculated risks to accelerate capability delivery.

Workshop A: Empowering PEOs with SPEED/FORGED Authorities



Actionable Recommendations

- Develop a balanced scorecard of performance metrics for PEOs/PAEs that incentivizes speed and calculated risk-taking, moving beyond a focus on budget execution rate.
- Consolidate the Department of War's (DoW) numerous budget line items into broader capability-focused portfolios to grant PEOs/PAEs the flexibility to reallocate funds to promising technologies.
- Establish enterprise-level digital engineering standards and platforms to ensure interoperability between programs and avoid the creation of new digital stovepipes.

Key Challenges

- The ingrained risk-averse culture within the acquisition workforce, where incentives favor process compliance over rapid delivery of effective solutions.
- Overly specific and rigid budget structures, which limit the ability to pivot resources without a lengthy and burdensome reprogramming process.
- The inability to divest from costly and outdated legacy systems, which consume funds that could be redirected toward modern capabilities.
- Building trust with appropriators to allow for greater funding flexibility, given the long institutional memory of past program failures.

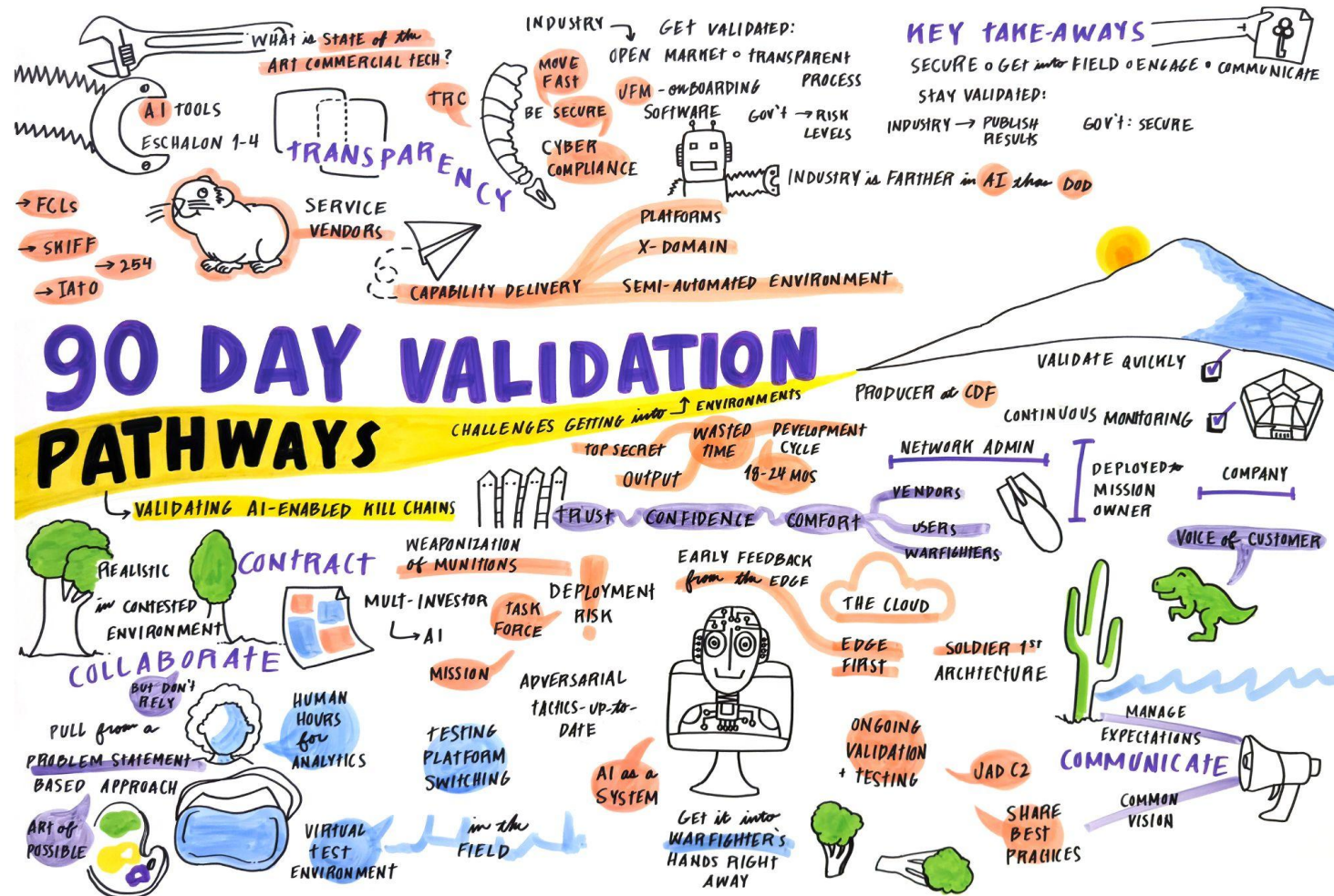
Additional Insights

The DoW often creates its own inflexibility through overly detailed budget justification materials, which it then presents as an external constraint from Congress. A fundamental disconnect exists between the urgent operational needs articulated by Combatant Commands and the services' capacity to fund and field joint solutions. There is also a critical shortage of experienced contracting officers who are both empowered and knowledgeable enough to use flexible authorities like Other Transaction Authorities (OTAs) effectively.

Workshop B: 90-Day Validation Pathways

Summary

This workshop addressed the critical challenge of accelerating the validation and fielding of Artificial Intelligence (AI) capabilities. The central problem is the tension between the need for speed and the requirement to build confidence with warfighters and government sponsors. The session explored moving from slow, static, one-time testing in isolated environments to a paradigm of continuous validation and monitoring in live, operational settings. This shift is essential to deliver multi-domain collaborative autonomy to the warfighter under urgent timelines, such as the stated goal for Indo-Pacific Command (INDOPACOM) by 2028.



Workshop B: 90-Day Validation Pathways



Key Themes

- **Shift from Static Testing to Continuous Monitoring**
 - Isolated test environments are insufficient for validating modern AI systems that learn and adapt.
 - A continuous evaluation model, mirroring commercial practices, is necessary. This involves fielding capabilities early, instrumenting them for constant data feedback in real-world conditions, and spirally improving them.
 - Live, Virtual, Constructive (LVC) environments serve as a key bridge, allowing for endless simulation runs to build initial confidence before deploying capabilities into the wild.
- **Building Trust as a Human and Cultural Challenge**
 - The primary barrier to AI adoption is not a lack of technology but a deficit of trust and confidence from end-users and risk aversion from leadership.
 - Trust cannot be achieved by "throwing software over the fence." It is earned through transparency, direct collaboration between engineers and warfighters, and managing expectations to avoid deploying immature technology that erodes confidence.

Key Themes

- **Prioritizing the Contested Tactical Edge**
 - AI systems must be developed and validated with an "edge-first" and "warfighter-first" mindset.
 - Capabilities designed for pristine, high-bandwidth cloud environments will fail in the degraded, contested, and disconnected conditions of modern warfare.
 - The entire validation architecture must be inverted to reflect the realities of the tactical edge, ensuring systems are resilient and effective where they are most needed.
- **The "Three-Body Problem" of Initial Validation**
 - The initial Authority to Operate (ATO) process is a significant bottleneck, often taking 18-24 months and creating a roadblock to fielding capabilities.
 - This delay stems from friction between three interdependent parties: the software vendor, the government mission owner, and the network administrator.
 - Overcoming this inertia requires constant communication, a shared demand signal, and strong leadership willing to assume risk to accelerate deployment.

Workshop B: 90-Day Validation Pathways



Actionable Recommendations

- Establish permanent, in-theater experimentation sites to enable continuous, real-world validation, provide direct feedback loops, and build warfighter trust through hands-on engagement.
- Adopt a risk-based validation framework that applies the most stringent checks to high-consequence systems (e.g., weaponized autonomy) while fast-tracking lower-risk enabling technologies.
- Invert the development architecture to be "edge-first," ensuring AI is designed for and tested in degraded, contested operational environments from the outset.
- Implement continuous cybersecurity monitoring as a non-negotiable requirement for all vendors, making security posture a zero-tolerance factor for participation in the ecosystem.

Key Challenges

- The lengthy process to gain an ATO on classified networks remains a primary structural barrier to rapid innovation and capability fielding.
- Overcoming deep-seated cultural risk aversion within the acquisition and testing communities to embrace iterative development and continuous monitoring.
- The significant cost and complexity of meeting cybersecurity compliance mandates like the Cybersecurity Maturity Model Certification (CMMC).
- The institutional inertia of shifting the Department of War (DoW) from a static, document-based validation culture to a dynamic, software-centric posture.

Additional Insights

- It was confirmed that the department is on a timeline to deliver multi-domain collaborative autonomy to INDOPACOM by January 2028, creating an urgent and tangible deadline.
- There is a view that intellectual property theft is inevitable; the strategic counter is to innovate so rapidly that any stolen technology is already obsolete.
- Top-down leadership is the ultimate accelerator. The INDOPACOM Commander's willingness to personally assume risk was cited as the critical factor in cutting through bureaucracy to field capabilities.

Workshop C: Strengthening Allied Industrial Base Cooperation



Summary

This workshop identified critical barriers to allied defense industrial base cooperation and formulated actionable reforms. The discussion centered on overcoming regulatory friction from export controls, streamlining bureaucratic processes, and fostering a cultural shift within the Department of War (DoW) to prioritize integration with trusted allies. The primary objective was to produce a set of near, mid, and far-term recommendations for policymakers to enhance collective security by building a more resilient and interoperable allied industrial ecosystem.



Workshop C: Strengthening Allied Industrial Base Cooperation



Key Themes

- **Overhauling Export Controls and Regulatory Frameworks:** The current export control system, particularly the International Traffic in Arms Regulations (ITAR), is a primary impediment. A move toward a single, streamlined regulatory regime aligned with the less restrictive Export Administration Regulations (EAR) is necessary. Expanding ITAR exemptions for a broader group of “trusted allies,” mirroring the AUKUS model, is a critical near-term step to reduce friction.
- **Designing for Integration from Inception:** U.S. acquisition culture defaults to developing systems solely for domestic use, making subsequent allied integration prohibitively expensive and slow. A fundamental shift is required to make “design for exportability” a mandatory early-stage consideration for all major programs, with program managers required to formally justify any decision to opt out.

Key Themes

- **Centralizing and Empowering International Cooperation:** Efforts to coordinate with allies are fragmented across the DoW, lacking a central champion. Establishing a single point of contact, potentially an Assistant Secretary of Defense for International Cooperation, would create a focal point to navigate bureaucracy, represent allied interests, and advocate for cooperative programs on Capitol Hill and within the Pentagon.
- **Improving Information Sharing and Demand Signals:** Allied industries, especially small and medium-sized enterprises, lack visibility into DoW requirements and opportunities. Inconsistent demand signals and barriers to accessing even low-level classified information prevent allies from shaping or competing for programs effectively. Secure platforms and processes are needed to facilitate earlier, more transparent communication.

Workshop C: Strengthening Allied Industrial Base Cooperation



Actionable Recommendations

- **Establish a DoW Assistant Secretary for International Cooperation:** Create a single, empowered focal point to streamline policy, advocate for cooperative programs, and serve as the primary liaison for allied governments and industry. This office would centralize oversight of disparate security cooperation processes.
- **Mandate “Design for Exportability”:** Revise acquisition policy to require program managers to design for allied export and interoperability from program inception. This shifts the onus, forcing a justification for *not* building in exportability, thereby reducing future integration costs.
- **Expand ITAR Exemptions for Trusted Allies:** Broaden the AUKUS-style legislative framework for streamlined export controls to a wider cohort of trusted allies. This would accelerate technology sharing and co-development efforts by removing significant bureaucratic delays.
- **Develop a Fast-Track Allied Innovation Pathway:** Resource and promote a dedicated pathway, possibly through the Defense Innovation Unit (DIU), for allied firms to introduce technology. This includes better resourcing for programs like Foreign Comparative Testing (FCT) to accelerate evaluation and adoption.

Key Challenges

- **Bureaucratic Inertia:** Fragmented, slow, and risk-averse processes for technology release, export licensing, and establishing cooperative agreements create significant delays and disincentivize collaboration.
- **Misaligned Acquisition Culture:** The DoW acquisition workforce is not adequately trained or incentivized to pursue international cooperation, often defaulting to restrictive “No Foreign Nationals” (NOFORN) classifications and prioritizing domestic requirements over interoperability.
- **Information and Communication Barriers:** Secure and efficient platforms for bilateral and multilateral collaboration are lacking. The inability of the U.S. to negotiate agreements in real-time severely hampers agile co-development.
- **Divergent Funding Cycles and Priorities:** Aligning disparate national budget cycles and investment priorities for long-term co-development and co-production projects remains a fundamental structural obstacle.

Additional Insights

- The concept of a formal “trusted ally” designation was proposed as a mechanism to automatically trigger streamlined regulatory treatment across export control, procurement, and information sharing domains.
- European funding initiatives, such as the European Defence Fund (EDF), are a double-edged sword; while they increase overall allied investment, their explicit goal of reducing dependency on the U.S. may create new barriers to transatlantic industrial cooperation.
- Current U.S. policy that requires international agreements to be fully finalized internally before being presented to partners was identified as a major impediment to true, collaborative negotiation.