CIPHERBRIEF

NatSecEDGE

Special Report

Insights from the frontlines of
National Security and Innovation

2025

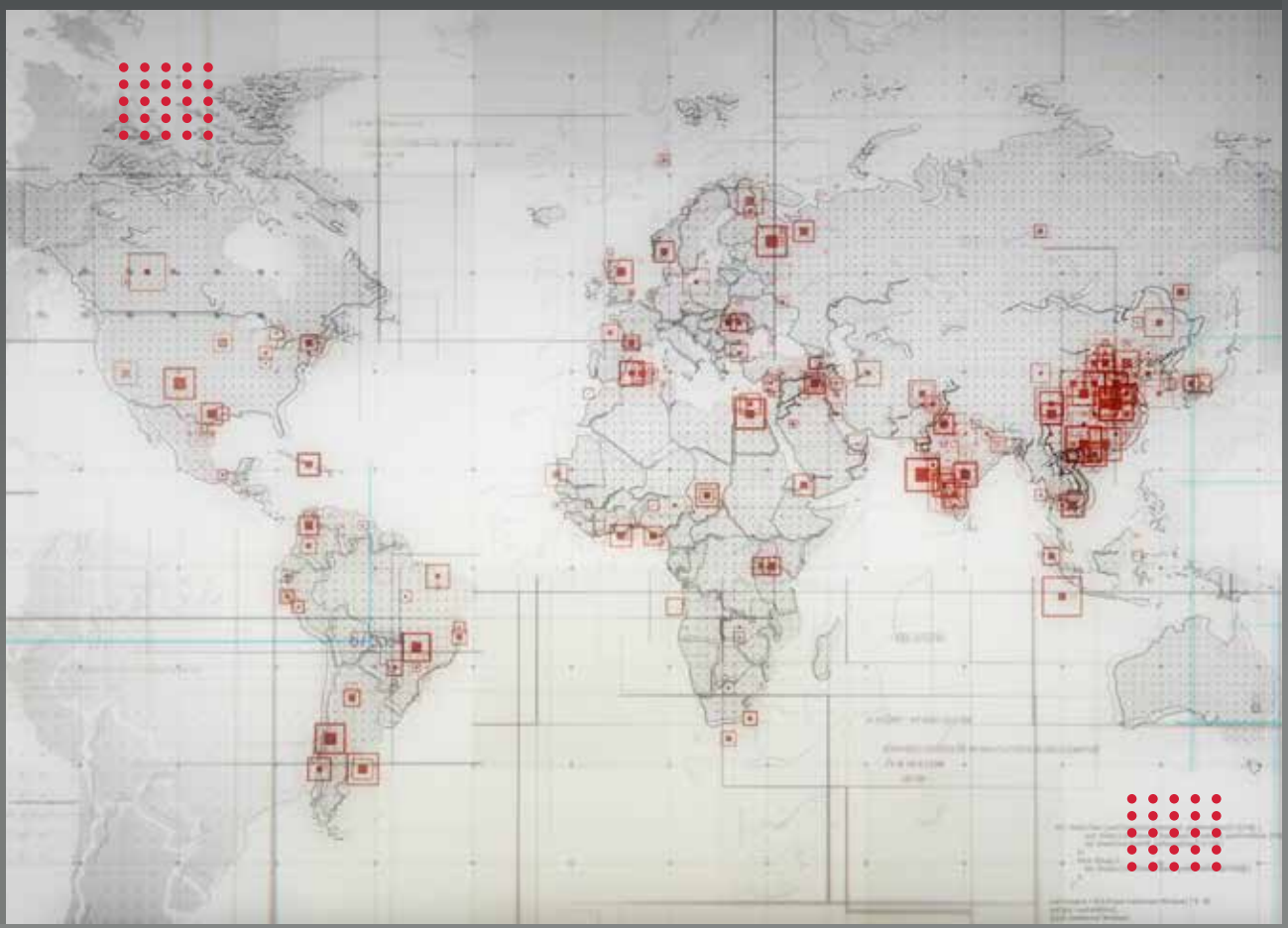

TABLE OF CONTENTS

TABLE OF CONTENTS

FOREWORD

The 2025 Nat Sec EDGE Forum brought together a diverse coalition of leaders from government, industry, investment, and innovation to confront a shared reality: America's national security advantage is eroding-and our ability to adapt at speed will determine the outcome of future conflicts.

Across two days of discussions, senior officials, technologists, operators, and investors delivered a clear message: the U.S. is engaged in an unprecedented strategic competition with near-peer adversaries who are moving faster, with fewer constraints, to dominate in emerging domains. While the U.S. still holds an innovation edge, our traditional systems for acquisition, classification, and risk management are too slow, too fragmented, and too siloed to respond to the velocity of today's threats.

What emerged from this gathering was not just urgency-but clarity. We need a new model for national security innovation-one built around speed, trust, integration, and mission-first execution. This means enabling "new primes" that can move at the pace of technology, equipping the defense industrial base with secure pathways to scale, and empowering operators and decision-makers with the tools to bridge policy, procurement, and operational need.

It also means recognizing that the problem is no longer technological-it's sociological. The innovation exists. The capital exists. The threat is clear. What's missing are the connective tissues: the incentives, partnerships, and trust frameworks that can accelerate solutions from concept to deployment.

This report captures the most critical messages and moments from Nat Sec EDGE. It is intended as both a record and a roadmap-for those shaping the future of American security.

Suzanne Kelly
CEO & Publisher, The Cipher Brief

Session Recap

KEYNOTE I- STRATEGIC TECHNOLOGY COMPETITION IN THE NEW COLD WAR

Dr. Michael Vickers
Former Under Secretary of Defense for Intelligence

> "America's technological competition with China is the central competition of the new Cold War." - **Dr. Michael Vickers**

Executive Summary

Dr. Michael Vickers delivered a sweeping strategic overview of how technology is reshaping global power dynamics, arguing that the U.S.-China technological competition is not merely a feature of current geopolitics but the central axis of a new Cold War. He framed artificial intelligence (AI), autonomy, quantum computing, and synthetic biology as core pillars of a historically unprecedented revolution-one that will define economic, military, and political supremacy in the 21st century.

Drawing on four decades of national security leadership and his background in military and intelligence operations and policy, Vickers warned that the U.S. risks losing its edge if it does not make significant structural and strategic reforms. He emphasized that national security "begins at home," calling for investments in R&D, revitalized civic education, fiscal responsibility, and a more robust industrial and technological base.

His remarks underscored that deterrence alone is not victory-the U.S. must achieve sustained technological and economic escalation dominance to prevail. He concluded by warning that the pace of change is accelerating and that many key domains-space, cyber, undersea warfare-will be decisively shaped by AI in the next decade.

Strategic Takeaways:

- AI is not just a capability-it is a platform for power projection and national wealth.
- China is gaining in AI, open-source, and state-backed development. The U.S. must press its advantage in innovation and originality.
- Restoring American competitiveness requires more than military investment; it demands societal and economic renewal.
- Defense priorities must focus on autonomy, global strike, cyber superiority, and resilient supply chains.
- Technological dominance must be coupled with democratic strength and strategic clarity-this is a whole-of-nation competition.

Session Recap

KEYNOTE II- THE FUTURE IS ALREADY HERE

> “Do you understand your data better than the adversary does? That’s the new cyber battlefield.” - **Steve Faehl**

Steve Faehl
Federal Security CTO, Microsoft

Executive Summary

Steve Faehl of Microsoft says that the future of artificial intelligence-particularly generative AI-is not speculative, but active and reshaping the cybersecurity and national security landscape today. His central message: while the technology is evolving rapidly, most challenges come not from the models themselves, but from how we misunderstand, misapply, or fail to secure them.

Faehl broke down the discussion into a critical framework: the security of AI, security with AI, and security from AI, urging clarity and nuance in national dialogue. He emphasized that generative AI is best understood as a map of human knowledge, and its effectiveness depends entirely on asking the right questions and solving the right problems.

He addressed common misconceptions-such as fears of ongoing “learning” by Large Language Models (LLMs) in deployment-and highlighted major risks like misaligned use cases, poor system security, and an underprepared workforce. The explosion of software and applications created via generative tools will bring new security challenges, particularly in identity, lineage, and API abuse.

Faehl ended with a powerful reminder that all AI successes-and failures-are human in origin. He called for deeper collaboration across sectors and a rethinking of how we fund, govern, and apply AI, suggesting a shift from viewing AI as an IT project to a strategic HR and intelligence function.

Strategic Takeaways:

- Misapplied AI is a larger problem than malicious AI.
- Privacy fears often stem from misunderstanding static vs. training models.
- An explosion in generative software development will increase exposure unless identity, provenance, and API control are prioritized.
- National strategy must shift AI investment from “tech” to “talent”-governing it like HR or intelligence.
- Agility in cyber will be defined by how fast capabilities can be built, not just bought-generative AI allows real-time defense and offense creation.
- Understanding and context-rather than raw data-will define cyber advantage in conflicts with near-peer adversaries.

Session Recap

KEYNOTE III- UNLOCKING THE IMAGINATION TO ACTION ERA: THE AI-DRIVEN FUTURE

Gilman Louie

CEO of America's Frontier Fund and former CEO of In-Q-Tel

> "The future is being driven not by nations-but by individuals unlocking imagination to action through AI." - **Gilman Louie**

Executive Summary

Gilman Louie offered a strategic overview of how generative AI and large language models (LLMs) are fundamentally altering the global landscape-politically, economically, and militarily. He framed AI not only as a national security challenge but as a civilization-wide transformation, driven by exponential changes in computation, innovation, and human-machine interaction.

Drawing on his experience as a commissioner on the National Security Commission on Artificial Intelligence and as a long-time venture investor, Louie recounted how even in 2021, the U.S. government failed to anticipate the rapid evolution of generative AI. He warned that America's lead over China in AI has narrowed to mere months, not years-despite attempts to "strangle" Chinese progress through chip sanctions. Scarcity, he said, has only accelerated Chinese innovation.

He introduced four core capabilities needed to approach Artificial General Intelligence (AGI): graduate-level math, machine-written code, sensor-based real-world understanding (physical AI), and the ability to generate original questions. Louie emphasized that the arrival of "almost-AGI" is likely within the 2030–2035 horizon-a timeline well within the venture investment cycle-and urged immediate U.S. focus on AI integration, infrastructure, and digital twin ecosystems.

Strategic Takeaways:

- Move faster: The U.S. is at risk of being out-integrated by China in physical AI and system-level capabilities.
- Prioritize scale and manufacturing: Innovation without production capacity is meaningless in sustained conflict.
- Invest in enabling technologies: Digital twins, SMRs, and quantum will define the next phase of competitive advantage.
- Embrace "almost AGI" as near-term: Planning for 2035 is already late.
- Redefine talent and organizational posture: The U.S. government must become "tech-native" to retain the next generation.
- Recognize the true power of AI is decentralization: Empowered individuals with access to AI will disrupt traditional hierarchies and reshape geopolitics.

Session Recap

SPECIAL OPERATIONS COMMAND AND THE FUTURE OF ACQUISITION

> “Everybody’s talking past each other. We have to invest the time to get everyone rowing in the same direction.” - **Melissa Johnson**

Melissa Johnson
Acquisition Executive, U.S. Special Operations Command (USSOCOM)

Executive Summary

Melissa Johnson provided a clear-eyed and practical view of how USSOCOM is addressing one of the most persistent defense innovation challenges: the Valley of Death. Speaking live from Tampa, she emphasized that co-locating key acquisition personnel under one roof-and integrating the full lifecycle of S&T, development, production, and sustainment-has enabled USSOCOM to move faster, more efficiently, and with greater accountability.

A recurring theme throughout the session was SOCOM’s growing engagement with private capital. Johnson emphasized the increasing importance of venture capital and private equity partners in helping to identify, fund, and scale emerging technologies. She noted that SOCOM has been holding quarterly roundtables with private investors and urged companies to engage through USSOCOM’s “Vulcan” system-its primary intake and collaboration platform.

While USSOCOM is a small-volume buyer, Johnson highlighted its role as a pathfinder for the Department of Defense. SOCOM often leads early experimentation and prototyping, with larger military services subsequently adopting and scaling those technologies. She acknowledged the need to do more to facilitate that transition from SOF to Big A (Army, Air Force, etc.), and pointed to Vulcan as a tool already being used across the services to identify promising technologies submitted to SOCOM.

Strategic Takeaways:

- Unified teams reduce transition friction: Co-locating S&T, PEOs, and acquisition leaders enables tighter integration from experimentation to fielding.
- SOCOM is a proving ground: While not a high-volume buyer, SOCOM plays a critical role in risk reduction and accelerating early-stage technologies.
- The Vulcan system is a force multiplier: Companies that enter the SOCOM ecosystem may find traction beyond SOF as DOD programs monitor and pull promising capabilities.
- Private capital is essential to scouting: The venture community is increasingly viewed as a strategic partner, not just a funding source.
- Horizontal integration is the new edge: Tying together multi-domain effects-from cyber to space to maritime-is SOCOM’s strategic vision for the future.

Session Recap

NATIONAL SECURITY, AI & FUTURE WARFARE

Will Hurd
Former U.S. Congressman, and former CIA Officer

> “China has mandated an AI-literate population by 2030. We’re still arguing whether AI belongs in school.” - **Will Hurd**

Executive Summary

Congressman Will Hurd outlined the key challenges and opportunities facing U.S. national security as it navigates a fast-evolving technological and geopolitical landscape. Drawing on his experience as a CIA officer, member of Congress, OpenAI board member, and now defense tech executive, Hurd framed the future of warfare around what he calls “War 4.0”-a conflict environment defined by speed, scale, and savagery, driven by autonomy, AI, and ubiquitous sensors.

Hurd expressed cautious optimism about America’s ability to outpace China in AI development, but warned that ***bureaucratic inertia, budget dysfunction, and public apath***y are slowing critical innovation. He called for urgent reform of congressional budgeting cycles, stronger alignment between warfighters and procurement authorities, and a shift in mindset across industry and government to match the tempo of modern conflict.

He emphasized the importance of autonomy on the battlefield, the urgency of preparing the American public for geopolitical stakes (especially regarding Taiwan), and the critical need for better storytelling to galvanize action. Hurd also stressed the role of investors, startups, and defense tech firms like Chaos Industries in building tools that give the warfighter the advantage-especially in communication-denied and drone-saturated environments.

Strategic Takeaways:

- Congress must adopt two-year budgets to enable meaningful innovation and tech transition.
- Procurement must be tethered directly to the warfighter, not bureaucratic intermediaries.
- The AI battlefield advantage will depend on software-defined, resilient, and autonomous systems-not exquisite, high-cost gear.
- U.S. education and public engagement are critical to sustaining national resolve in future conflicts.
- Defense innovators must speak plainly, deliver real results, and design for the field, not the lab.

Session Recap

PRIVATE CAPITAL AND THE FUTURE OF NATIONAL SECURITY

Ambassador Henry Crumpton

Chairman & CEO, Crumpton Global LLC

> “We’ve crossed the threshold into the third world war. It’s just a very deep, complex gray zone that we don’t fully understand.” - **Amb. Henry Crumpton**

> “The tools for AI are in everyone’s hands- friends and adversaries alike. Decision advantage now depends on how fast and how boldly we move.” - **Teresa Smetzer**

Teresa Smetzer

Fmr. Director of Digital Futures, CIA; National Security Executive

Executive Summary

This conversation between national security leaders Teresa Smetzer and Hank Crumpton explored how revolutionary technologies, blended battle domains, and global instability are driving a shift in national security investments from traditional government-led models to innovation ecosystems increasingly shaped by private capital and commercial solutions.

Crumpton underscored the new nature of warfare as a “unified global battlefield” where success is predicated on dominance across six interdependent domains: land, sea, air, space, cyber, and the human terrain. He called for greater private sector alignment with end-user needs and emphasized the criticality of digital risk management, networked leadership, and counterintelligence in this new conflict paradigm.

Smetzer stressed that space, cyber, and AI are no longer areas of government exclusivity, as private sector firms are now leading innovation and deploying critical infrastructure. Both called for proactive approaches to adversarial AI, synthetic biology, and materials science while reinforcing the importance of trusted public-private partnerships and international alliances.

The conversation concluded with an emphasis on the unique advantages Texas offers as a hub for defense innovation.

Strategic Takeaways:

- Modern conflict spans six domains-land, sea, air, space, cyber, and human terrain-and that investors must evaluate technologies in terms of their utility within and across this interconnected battlefield.
- The traditional divide between government and private industry is collapsing. Companies like SpaceX, Palantir, and Anduril exemplify how commercial firms now define strategic capabilities-often more rapidly and effectively than government.
- We have entered a new world war-"a deep, complex gray zone war" with China, Russia, Iran, and North Korea-where private infrastructure (like seabed cables, LEO satellites, and AI data centers) is increasingly targeted.
- Investors and company leaders must treat digital risk as enterprise risk. Complacency around cybersecurity, insider threats, and third-party vulnerabilities is a critical liability.
- Need for urgent innovation in adversarial AI defense and provenance tracking.
- Beyond AI and quantum, Smetzer highlighted material science, logistics, and synthetic biology-particularly drug production decoupled from foreign supply chains-as strategic investment areas.
- Crumpton advocated for decentralized, adaptive models of leadership rooted in trust networks rather than rigid hierarchies, citing early CIA operations in Afghanistan as a prototype for future engagements.

Session Recap

U.S.–CHINA COMPETITION: TECHNOLOGY, TRUST, AND THE BATTLEFIELD OF THE FUTURE

Gilman Louie
CEO, America's Frontier Fund

Chip Usher
Former NSC Senior Director for Intelligence Programs

Rick Ledgett
Former Deputy Director, NSA

John Sherman Moderator
Dean, Bush School of Government and Public Service, Texas A&M

> "We need to build a national public-private partnership for AI defense. It doesn't exist yet, but it must." - **Chip Usher**

Executive Summary

This session tackled the evolving technological and cultural dimensions of U.S.–China strategic competition, emphasizing the critical role of artificial intelligence, cyber threats, and national infrastructure. Gilman Louie argued that the AI race is not only about hardware and algorithms but about societal values and adoption-highlighting that the Chinese population overwhelmingly trusts AI, whereas Americans remain deeply skeptical. Chip Usher expanded on China's methodical state-driven AI buildout, revealing a vast and sophisticated infrastructure tied to the People's Liberation Army and powered by state subsidies, foreign partnerships, and aggressive policy planning. Rick Ledgett issued a stern warning that Chinese actors are already embedded within U.S. critical infrastructure, preparing for scenarios like a Taiwan conflict by developing the capability to degrade American systems at will. The panel concluded by underscoring the urgency of public-private partnerships, cultural resilience, and long-term investment in the next generation of national security leaders.

Strategic Takeaways:

- Cultural Trust in AI Is a Competitive Advantage:

  China's collectivist values and societal trust in AI technology enable rapid integration and deployment, giving Beijing an edge in adoption and scaling.

- U.S. Domestic Skepticism Is a Vulnerability:

  Widespread public mistrust in AI in the U.S. may slow adoption and erode competitiveness, despite American leadership in foundational technologies like large language models.

- China's AI Buildout Is Massive and Military-Integrated:

  China has established over 100 AI-focused data centers with hundreds of exaflops of compute power, many linked to the PLA and state-controlled infrastructure.

- Export Controls Are Leaky and Insufficient:

  Despite expanding sanctions, Chinese AI projects continue to receive support from foreign suppliers, including some from Five Eyes countries and Japan.

- Cyber Penetration by China Is Advanced and Strategic:

  Chinese state actors (e.g., Volt Typhoon and Salt Typhoon) have deeply infiltrated U.S. telecommunications and energy systems to pre-position for future conflict scenarios.

- Public–Private Partnerships for AI Defense Are Urgently Needed:

  The U.S. lacks a coordinated structure for AI resilience, which must be addressed to secure AI systems and infrastructure from state-sponsored threats.

Session Recap

LESSONS FROM THE BATTLEFIELD: INNOVATION IN UKRAINE AND IMPLICATIONS FOR FUTURE

> “Ukraine has a procurement system that is producing tomorrow’s technology for today’s wars. Our system produces yesterday’s technology for tomorrow’s wars.” - **David Petraeus**

David Petraeus
Former Director, CIA
Moderator: Suzanne Kelly

Executive Summary

General David Petraeus provided a sweeping assessment of the ongoing war in Ukraine with a particular focus on how AI-driven unmanned systems, commercial innovation, and adaptive tactics are reshaping modern warfare. Drawing on a recent trip to Ukraine, Petraeus characterized the battlefield as a live laboratory of emergent technologies, where Ukrainian ingenuity, necessity, and improvisation are driving tactical advantages despite being outmanned and outgunned.

He emphasized that drones are now the new artillery, with Ukraine launching as many as 7,000 drones in a single day-an unprecedented figure that reflects how AI and remote capabilities are replacing traditional platforms. The most stunning recent example: a strategic drone strike deep into Russian territory, reportedly planned over 18 months and possibly executed by algorithmically piloted drones. The operation caused an estimated $7 billion in damage, including the destruction of Russian AWACS aircraft and strategic bombers-with an attack cost of under $1 million.

Petraeus praised Ukraine’s battlefield innovation model, noting that its procurement and development pipeline fuses operators, developers, and manufacturers in real time-a stark contrast to the U.S. system, which he described as “an industrial-age process” building yesterday’s technology for tomorrow’s wars.

Looking ahead, Petraeus sees AI expanding across every aspect of the conflict-from mission planning and EW countermeasures to command-and-control systems, where Ukrainians are already integrating AI and open-source tools to unprecedented effect. He cited Ukraine’s creation of a fully functional C2 system for $3 million-surpassing the utility of U.S. systems costing billions.

Petraeus concluded with a call for closer partnerships between government and industry, warning that the U.S. must radically reform its procurement approach, harness private-sector innovation faster, and learn from Ukraine’s rapid fielding model if it hopes to retain its military edge in future conflicts-including a potential fight with China over Taiwan.

Strategic Takeaways:

- Ukraine's battlefield offers a live template for how distributed, AI-enabled systems will dominate future conflicts.
- The cost-performance asymmetry of drones makes large, expensive platforms increasingly vulnerable and obsolete.
- The U.S. must reimagine procurement as a real-time co-development process between operators and industry, not a multiyear bureaucratic treadmill.
- Algorithmic autonomy, not just remote control, will define the next evolution of unmanned combat systems.
- Private-sector partnerships must be institutionalized and scaled, particularly in AI, EW, maritime autonomy, and agile C2 systems.

Session Recap

DEFEATING THE NEW INSURGENCY: A NATIONAL SECURITY APPROACH TO MEXICAN CARTELS

> “We’re trying to fix the private sector–government relationship. There’s a lot of finger pointing. But if we get commercial GeoINT right, we could have real-time awareness of everything from the oceans to cartel movements.” - **Dan Crenshaw**

Dan Crenshaw
Congressman (R-TX)
Moderator: Suzanne Kelly

Executive Summary

Congressman Crenshaw emphasized the need to redefine the U.S. approach to Mexican drug cartels, describing the threat not as a “war on drugs” but as a counterinsurgency campaign against well-armed, strategically minded, and increasingly violent transnational organizations. He discussed the bipartisan urgency around countering fentanyl, the importance of Mexico’s new political leadership, the necessity for unified interagency coordination, and the pivotal role of advanced technologies-including commercial geospatial intelligence-in counter-cartel and broader national security missions.

Key Takeaways:

- Reframing the Threat: Cartels as Insurgents- He frames the fight against cartels as a counterinsurgency in a neighboring country, comparing it to Plan Colombia but noting differences in sovereignty and sensitivity in Mexico.
- Momentum with Mexico’s New Government- Crenshaw cited new openness from Mexico’s incoming President Claudia Sheinbaum and security lead Omar García Harfuch to joint U.S.-Mexico cooperation against cartels.
- Technology and Counter-Cartel Operations- Crenshaw stressed the need for the U.S. to outpace cartel innovation by ramping up analytical capacity, intelligence authorities, and interagency coordination.
- Overcoming Bureaucracy to Embrace Commercial GeoINT- A major focus of Crenshaw’s current work is streamlining the pipeline between commercial geospatial firms (especially in Texas) and the defense/intel community.
- 5. Counterintelligence, Drone Threats & Force Protection- Crenshaw warned of serious counterintelligence and drone-based threats to government facilities.
- 6. Broader National Security Priorities Crenshaw is also focused on:
- Autonomous systems, especially drawing on Ukraine’s lessons to prepare for future conflicts (e.g., Taiwan).
- Enhancing the U.S. capability for offensive cyber operations.
- Rethinking how the government applies existing authorities more aggressively in defense and intelligence settings.

Session Recap

ACCELERATING INNOVATION AT THE TACTICAL EDGE

Lt. Col. Nick Rinaldi
Human Performance Portfolio Lead,
Army Applications Lab

> “Right now the scoreboard is driving how we train. If we don’t change the scoreboard, we’ll keep training to the past.” - **Lt. Col. Nick Rinaldi**

Moderator: Brad Christian

Executive Summary

This fireside chat between Brad Christian and Lt. Col. Nick Rinaldi explored how the U.S. Army is leveraging non-traditional commercial partnerships to rapidly integrate technology into field formations through the Army Applications Laboratory (AAL).

Rinaldi shared how the lab focuses on solving real operational problems-not admiring them-by engaging directly with soldiers in the field and pairing them with technologists. The conversation emphasized how new technologies-especially in autonomy, robotics, and expendable systems-can reshape ground combat capabilities, but only if accompanied by cultural and procedural change. Central to that change is a shift in procurement timelines, training approaches, and redefining how the Army measures success.

Strategic Takeaways:

- AAL Operates at the Intersection of Soldiers and Solutions: AAL’s mission is to connect dual-use commercial technologies directly with warfighters in the field to address high-priority operational problems through iterative, real-world testing.
- The Process Begins with the Problem, Not the Product: Success depends on building the entire kill chain of stakeholders-from technologists to end users-and addressing real operational challenges, not starting with available technologies.
- Field Integration Is the Key to Innovation: The most successful companies embed with units early in the training cycle, iterating alongside soldiers rather than waiting until product completion to deliver a solution.
- Disposable Systems Are Changing the Battlefield: Inspired by lessons from Ukraine, AAL embraces throwaway technologies (e.g., drones, unmanned ground vehicles) that are fast, scalable, and tailored for rapid obsolescence-not long-term sustainment.
- Cultural Change Is the Greatest Barrier to Progress: A shift in mindset is required across the Army to adopt and field fast-moving technologies. Leaders must change the “scoreboard” used in training and procurement to incentivize innovation over compliance.

Session Recap

STRATEGIC RISKS AND OPPORTUNITIES IN THE MIDDLE EAST: AI, ENERGY, AND IRAN

> There's not enough energy in the world right now to support global AI requirements. - **Norman Roule**

Norman Roule
Former National Intelligence Manager for Iran

Moderator: Suzanne Kelly

Executive Summary

In a wide-ranging briefing, Middle East expert Norman Roule offered a high-level assessment of strategic developments across the Gulf region, AI infrastructure expansion, energy markets, and the Iran nuclear issue, framing key opportunities for the United States and its allies-as well as significant emerging risks. Roule emphasized that AI development in the Gulf is inevitable, and that U.S. leadership in this space hinges on constructive partnerships with countries like the UAE and Saudi Arabia, which are actively inviting U.S. collaboration over Chinese alternatives.

Roule highlighted the sheer scale and ambition of Gulf states' investments in AI infrastructure, including multi-billion-dollar NVIDIA-powered data centers that could surpass the largest AI clusters in the world. He warned, however, that long-term success depends on locking in secure frameworks now to prevent future adversarial exploitation-particularly investment spillover to China.

On energy, Roule broke down OPEC's shift in production strategy and forecast a period of stable-to-lower oil prices, with Saudi Arabia expected to reclaim market share and U.S. shale investments likely to decline.

Finally, on Iran, Roule emphasized that Tehran's nuclear red lines remain unchanged, and that no diplomatic formula currently exists to halt Iran's enrichment. He concluded with a stark warning about the potential for Iran to field ICBM capabilities by 2035, based on U.S. defense estimates.

Strategic Takeaways:

- The AI race in the Middle East is already underway-U.S. influence depends on early engagement, not resistance.
- The window to define secure norms is now, while Gulf states are still shaping their AI governance and infrastructure.
- The energy-AI nexus is reshaping OPEC thinking and global investment flows.
- Watch summer 2025: Diplomatic agreements around AI, tech transfer, and security protocols will be finalized. Stakeholders must weigh in now.

Session Recap

CYBER, INNOVATION AND THE FUTURE OF AI

Kelly Bissell

Corporate Vice President, Microsoft

> “We have to build seatbelts and airbags into technology now.” - **Kelly Bissell**

> “We’re not investing in innovation for innovation’s sake-we’re investing for strategic advantage.” - **Katie Gray**

Katie Gray

Senior Investing Partner, In-Q-Tel

Executive Summary

This conversation between Microsoft’s Kelly Bissell and In-Q-Tel’s Katie Gray explored the escalating cyber threats posed by malicious AI, the pace of global innovation, and the growing need for strategic investment to ensure U.S. technological advantage.

Bissell emphasized the real-time challenges Microsoft faces in combating fraud and abuse across its platforms, while Gray provided a venture capital perspective on how emerging technologies-especially AI-are transforming both defense and commercial landscapes.

The conversation touched on AI-fueled cyberattacks, the importance of digital literacy, the future of software development (including “vibe coding”), and the need for resilient public-private collaboration to mitigate evolving threats. Both agreed that sustained innovation and a strong U.S. tech ecosystem will be decisive in maintaining national security.

Strategic Takeaways:

- Malicious AI Adoption Is Rapid and Sophisticated: Bad actors are already using AI to mimic human behavior for fraud and misinformation, creating a new level of threat sophistication that requires anticipatory innovation.
- Security Must Be Built-In, Not Bolted-On: Companies must embed safety mechanisms-akin to “airbags”-into technology itself to keep up with evolving risks like deepfakes and AI-generated malware.
- Public-Private Collaboration Is Essential: Large companies cannot innovate alone. Partnering with startups and investors is critical to stay ahead of adversaries and fill capability gaps quickly.
- Culture of Innovation Must Be Maintained: U.S. innovation success hinges on fostering a dynamic venture ecosystem, supportive immigration policies, strong universities, and government-funded R&D.
- AI Will Reshape the Workforce and Software Paradigms: With tools like GitHub Copilot and “vibe coding,” individual users can build applications at unprecedented speed, shifting the boundary between consumers and creators-and redefining entry-level jobs.

Session Recap

AI & TECH'S BIGGEST IMPACT

Former Senator Bob Kerry
Managing Director, Allen & Co

Moderator: Ambassador Henry Crumpton

> "We didn't invent the shipwreck until we invented the ship. AI will bring good and bad-we must be ready for both." - **Bob Kerry**

Executive Summary

On the anniversary of D-Day, Medal of Honor recipient, former U.S. Senator, and veteran statesman Bob Kerrey offered a wide-ranging and deeply personal conversation about national service, leadership, democracy, AI, and the challenges of civic life in a technology-driven world. Speaking with humility and wit, Senator Kerrey reflected on the promise and peril of artificial intelligence-particularly in healthcare and public trust-while emphasizing the enduring need for democratic values and personal courage.

Kerrey urged caution about fear-driven narratives around AI, emphasizing instead its potential to improve diagnostic precision, expand educational access, and deepen civic understanding-if guided by human values and supported by democratic systems. He pushed back on fatalistic views from figures like Henry Kissinger, arguing that AI must be shaped by who we are, not feared for what it might become.

Drawing on his own experiences-from losing a leg in Vietnam to serving in Congress and running healthcare companies-Kerrey made the case for national service, character-building leadership, and fostering personal responsibility among young Americans. His call for mandatory post-high school military service was grounded in a desire to rebuild unity, purpose, and resilience among citizens.

Above all, he warned against conspiratorial thinking and division, emphasizing the foundational ideas of the American experiment. "Democracy is hard," he said. "But it's worth it."

Strategic Takeaways:

- AI can drive massive improvement in health, education, and national security-but only if shaped by democratic values and public trust.
- National service-particularly military-is a powerful tool to rebuild shared responsibility and national cohesion.
- Conspiracies, social fragmentation, and misinformation are the true existential threats-not AI.
- Democracy must be defended actively, especially by young Americans who are increasingly disillusioned.
- Technology is a tool-leadership and values determine whether it's used to unite or divide.

Session Recap

IMAGINING THE GOLDEN DOME

RADM Mark Montgomery (Ret.)

Former Executive Director Cyberspace Solarium Commis-

Steve Faehl

CTO, Microsoft

> “Our military is clinically insane. We build 99% weapons when we could win with two 80% ones.” - **Mark Montgomery**

Executive Summary

In a wide-ranging and characteristically candid session, retired Rear Admiral Mark Montgomery offered a bold blueprint-and a scathing critique-of America’s preparedness for emerging missile threats, especially from China and Russia. His central thesis: the only viable path to defending the U.S. homeland from long-range cruise and hypersonic missile attacks is a space-based missile defense architecture, powered by low-cost satellite launches, proliferated sensor constellations, and kinetic or directed-energy interceptors.

Dubbed “Golden Dome,” this next-generation system would look radically different from traditional terrestrial defenses like THAAD or Patriot batteries, which Montgomery derided as inadequate, unaffordable, and operationally obsolete. With Chinese and Russian missile capabilities rapidly evolving, Montgomery argued that legacy procurement models-designed for static platforms and exquisite weaponry-must be replaced with low-cost, mass-deployable effectors and real-time C2 (command and control) architectures.

He praised the selection of Gen. Mike Guetlein to lead the effort, calling him a rare operator who understands space, missiles, and bureaucratic warfare. But Montgomery warned that political ego, congressional pork-barreling, and legacy defense industry inertia could sabotage the vision unless bold leadership and commercial partnerships (especially with SpaceX) are prioritized.

Montgomery also made a strong case for cost-per-shot asymmetry, pointing to Ukraine’s drone war as a model for the U.S. to emulate. He advocated for using “good enough” 80% solutions fired in salvos rather than designing single, gold-plated interceptors with 99% accuracy. He emphasized the need to move away from exquisite and expensive weapon systems and toward software-defined, refreshable space technologies launched on a 3–5 year cycle.

His final call to action: match America’s technological edge with political will, bureaucratic humility, and urgency-before adversaries hold the homeland at risk.

Strategic Takeaways:

- Golden Dome's architecture must be distributed, refreshable, and space-based-not an extension of current missile defense paradigms.
- SpaceX is indispensable for launch cadence, cost, and payload innovation.
- A hybrid force design with software-defined payloads, modular buses, and low-cost effectors is key to scale.
- The effort needs ruthless C2 discipline, rapid-fire modeling & sim, and lean tech procurement-especially from defense-tech startups.
- Political unity and strategic humility will be the deciding factors in avoiding another two decades of underinvestment.

Session Recap

SECURING THE ARSENAL OF DEMOCRACY: HOW DCSA PROTECTS INNOVATION AND INDUSTRIAL TRUST

> “There’s not enough energy in the world right now to support global AI requirements.” - **Matthew D. Redding**

Matthew D. Redding

Assistant Director, Industrial Security, Defense Counterintelligence and Security Agency

Executive Summary

Matthew Redding delivered an in-depth overview of the Defense Counterintelligence and Security Agency’s (DCSA) role in protecting America’s defense industrial base.

Framing security as the core enabler of innovation and trust, Redding emphasized that industrial and personnel security are foundational to national defense.

He warned of growing adversary activity-particularly from China-infiltrating unclassified networks, research institutions, and startup ecosystems, and advocated for a public-private security partnership based on shared responsibility.

Redding outlined DCSA’s expansive oversight across classified contracts, personnel vetting, and facility security, and urged companies-especially non-traditional startups-to bake in security early as a competitive differentiator and national duty.

Strategic Takeaways:

- Security is a Value Stream and a Trust Enabler: Trust, not just compliance, is the currency of working with the government. Companies must build and demonstrate trustworthiness in people, facilities, technology, and funding sources.
- Adversaries Target the Unclassified Domain: China and others are increasingly focused on acquiring knowledge through legal and illegal means in unclassified R&D, academia, and supply chains, making security in those areas vital.
- DCSA is the Industrial Security Backbone of National Defense: Overseeing 90–95% of classified U.S. contracts, DCSA vets personnel, facilities, and IT systems, and enables trusted access to sensitive programs through proactive engagement and training.
- Early Investment in Security Mitigates Risk and Builds Brand: Redding urged startups to integrate security from inception-embracing secure-by-design practices-and emphasized that doing so will accelerate government collaboration and protect IP.
- Continuous Vetting & Insider Threat Detection Are Working: DCSA’s continuous monitoring identifies thousands of at-risk individuals in near real-time, preventing potential breaches and enabling responsive, risk-based mitigation.

Session Recap

THE DIGITAL LIFECYCLE OF A NATION-STATE THREAT

Kelly Bissell
CVP, Microsoft

Cynthia Kaiser
Former Asst. Dep. Director of FBI for Cyber

Matt Olsen
Partner, WilmerHale & Fmr. Attorney General for National Security

Rick Ledgett
Former Deputy Director, NSA
Moderator

> “The only difference between a nation-state and a ransomware gang is encryption at the end.” - **Cynthia Kaiser**

Executive Summary

This panel explored the evolving digital threat landscape, with a specific focus on how nation-state adversaries and cybercriminals are exploiting the fragmented global cyber ecosystem. The discussion highlighted the blurring line between nation-state and cybercriminal operations, the growing need for private-public operational collaboration, and the urgent demand for innovation in both technology and policy frameworks.

The conversation traced the evolution from counterterrorism-era data challenges (e.g., pre-9/11 intelligence silos) to today’s persistent and sophisticated nation-state threats-notably China. Matt Olsen framed this shift as a legal and policy challenge, underscoring the importance of ensuring U.S. laws and authorities are modernized to allow for effective digital threat tracking.

The panel highlighted the success of recent disruptive operations-particularly the FBI's botnet takedowns-as models for proactive digital defense. But speakers warned that disruption alone is not enough: the ecosystem must be fortified through better technology, scalable defensive tools, and greater venture-investor engagement to commercialize breakthrough ideas.

The session also included sharp warnings against offensive "hack back" strategies by private entities. Panelists called these proposals legally problematic and strategically dangerous, advocating instead for improved intelligence sharing and coordination between industry and government.

Strategic Takeaways:

- Disruptive cyber operations, when integrated with private-sector intel, offer an effective model for defending at scale-but require trust and coordination.
- Offensive strategies must be led by the government; no viable path exists for legal private hackback.
- Emerging cyber technology is promising, but must be democratized beyond large enterprises.
- Policy updates (e.g., 702) and public service revitalization are essential to keep pace with digital adversaries.
- Investors and industry leaders should accelerate commercialization paths for defensive innovations that enable detection and resilience at scale.

> "Attackers are leveraging every fracture in the digital ecosystem. We must stop operating in silos." - **Kelly Bissell**

> "Disruptions don't end a campaign-but they sure slow it down." - **Rick Ledgett**

> "Public service is not the vibe right now. That's a risk to national security." - **Matt Olsen**

Session Recap

THE ROLE OF CIA'S T2MC IN SECURING U.S. TECHNOLOGICAL ADVANTAGE

Sheetal Patel

Former Assistant Director, CIA Transnational & Tech

> "Security doesn't have to be all or nothing. Sometimes it's about protecting what matters most, not everything." - **Sheetal Patel**

> "AI requires compute, compute requires data centers, and those require power. It's all connected-we can't look at these in silos." - **Susan Hennessey**

Susan Hennessey

Former Chief of Staff, National Security Division, DOJ and Counsel, WilmerHale

---

Executive Summary

In this focused fireside session, Sheetal Patel reflected on her recent leadership of the CIA's Transnational and Technology Mission Center (T2MC), created under Director William Burns to bridge the gap between national security imperatives and rapid advancements in emerging technologies.

The center was designed to drive collaboration between the U.S. Intelligence Community, private sector, and international allies in monitoring, understanding, and competing with the People's Republic of China in key tech domains.

Patel discussed the importance of breaking down government stovepipes, identifying priority technology sectors, building better partnerships with industry, and addressing the critical need for integrated risk management-especially in supply chains and insider threat detection.

She emphasized that while China remains a top focus, broader structural urgency and alignment are still lacking across sectors.

Strategic Takeaways:

- Urgency Still Lags Despite Strategic Threats: Despite years of warning, there remains a disconnect between rhetoric and action in U.S. efforts to compete with China technologically. True urgency and cross-sector cohesion are still missing.
- T2MC Aims to Break Government Silos: The center was structured to dismantle stovepipes between CIA's operational, analytical, technical, and digital directorates, and foster integrated approaches to tech competition.
- Top Technology Focus Areas Identified: T2MC concentrated on six technology categories: next-gen communications (like 6G), microelectronics, high-performance computing, next-gen power and batteries, financial tech (crypto/CBDC), and synthetic biology. AI was treated as a cross-cutting enabler across all domains.
- Supply Chain and IP Risk Are Paramount: Companies must know who their vendors are, where the code resides, and what intellectual property must be protected. A tiered, risk-based approach-rather than all-or-nothing-is encouraged.
- AI Will Accelerate Both Progress and Threats: AI acts as a "great equalizer," with the potential to enable rapid global development and also amplify misinformation, IP theft, and offensive capabilities. Its infrastructure dependencies-data centers, power, chips-must be assessed holistically.

Session Recap

THE FUTURE BATTLEFIELD OF UNMANNED SYSTEMS

Shawn Driver
Chief of Staff, HavocAI

Jim Blom
Head of Corporate Development and Portfolio Strategy, Fairlead

Philip Carson
Investor, Cubit Capital

Jeremy Hitchcock
General Partner and Co-Founder, New North Ventures

Moderator

> “If we flood the Pacific with a thousand USVs and change the adversary’s decision-making-maybe we’ve deterred conflict.” - **Shawn Driver**

Executive Summary

This session explored the critical and rapidly evolving maritime domain, emphasizing the role of autonomy, industrial base revitalization, and scalable production to deter conflict in the Indo-Pacific region.

The panel brought together operators, technologists, investors, and legacy defense manufacturers to examine how maritime innovation must match the urgency of the geopolitical threat posed by China.

With the U.S. Navy under-capacity and traditional shipbuilding slow and costly, panelists emphasized leveraging commercial industrial bases, scalable autonomy stacks, and public-private partnerships to produce thousands of non-exquisite unmanned surface and subsurface vessels (USVs/UUVs) within a short time horizon.

Participants highlighted how breakthroughs in collaborative autonomy, AI, and modular ship production-paired with flexible policy and capital alignment-could flood the Pacific with deterrent capabilities by 2030.

Strategic Takeaways:

- The Tyranny of Distance Demands a New Maritime Strategy: The Indo-Pacific region's vast geography (e.g., 8,000 miles from San Diego to Manila) requires autonomous systems capable of long-range operation with minimal support. Traditional logistics nodes will not be survivable in a peer conflict.
- Rapid Production Through Commercial Maritime Base: Companies like Havoc AI are integrating autonomy into existing commercial vessels instead of building new hulls, drastically shortening timelines. Havoc has already outfitted 47+ vessels with plans to scale from 14-foot USVs to larger platforms.
- Collaborative Autonomy Is Operational Today: Havoc demonstrated control of 30 vessels from Rhode Island, San Diego, and Portugal, passing commands across a mesh network and Starlink, enabling team-level autonomy regardless of whether it's 1 or 1,000 vessels.
- Industrial Base Needs Distributed Activation: Drawing lessons from WWII's Higgins boats (built in New Orleans), panelists stressed tapping regional industrial capacity-especially in the Philippines and Pacific islands-and using modular, non-exquisite, scalable systems.
- Manufacturing and Software Integration Are Key: Robotic shipbuilding is gaining momentum. Companies are investing in CAD-to-build efficiencies and behavioral libraries for autonomy stacks, seeking to cascade thousands of platforms in 24–36 months.
- Need for Infrastructure and Policy Alignment: Building out shipyards and production at scale will require rezoning, redevelopment of legacy terminals, federal incentives, and alignment of IC, Navy, and private equity efforts.

> "The U.S. is activated now. We just need policy, incentives, and capital to follow." - **Jim Blom**

> "Controlling multiple vessels from one console with text-based AI instructions-it's not the future, it's now." - **Philip Carson**

Session Recap

NAVIGATING A MINERALS CRISIS

John Watters

Executive Chairman, Apollo Information Systems

> “Capitalism is being played like a fiddle. Communism is winning this economic war-and it’s irrational to expect market forces to solve a national security crisis.” - **John Watters**

> “We are one of the few countries at scale that doesn’t have an office of industrial warfare. And it’s coming back to bite us.” - **Gilman Louie**

Gilman Louie

Managing Partner, America’s Frontier Fund

Executive Summary

John Watters delivered a forceful warning about what he described as the greatest near-term strategic vulnerability facing the United States: China’s near-total dominance over the global supply chain for critical minerals and metals. These materials are indispensable to every layer of U.S. national security-from microelectronics and F-35s to fiber optics and electric vehicles. Watters argued the threat is not hypothetical or long-term-but imminent, already manifesting in China’s export bans on gallium and germanium, two metals essential to semiconductor production.

Watters, a seasoned cybersecurity executive turned industrial strategist, revealed that China holds a 99% share of global gallium refinement capacity, a material required for integrated circuits. Even if the U.S. invests billions in new chip foundries under the CHIPS Act, it won’t matter if it can’t source the input materials. In a striking comparison, Watters described this as “having burgers and fries, but forgetting the cows and potatoes.”

He explained that China has weaponized global capitalism by subsidizing refining and undercutting prices to such an extent that Western companies cannot economically compete. The refining choke point-not mining-is the bottleneck, and Watters made clear that no new refineries will be built without government-backed guaranteed offtakes due to below-OPEX returns.

In Watters’ view, this is a true existential risk to U.S. national power projection, one that requires wartime-like

mobilization, government-led solutions, and Quad-level (U.S.-Japan-India-Australia) coordination. Among his recommendations were strategic stockpiles, refinery subsidies, permit reforms, and a new federal office dedicated to industrial warfare strategy.

His final message was blunt: "It's time to panic early and avoid the rush."

Strategic Takeaways:

- The U.S. must treat critical mineral supply as a national security imperative, not a market function.
- This requires the mobilization of federal investment, potentially through legislation or a presidential executive order.
- The Quad alliance offers a realistic multilateral path-if coordinated rapidly and decisively.
- Every element of the defense and technology sector is vulnerable unless refinery choke points are addressed now.
- The first step must be the creation of a unified, strategic Office of Industrial Deterrence-to both track and outmaneuver adversaries who already understand how to wage economic warfare.

Session Recap

PUBLIC-PRIVATE CYBER DEFENSE: NSA'S COLLABORATION STRATEGY WITH INDUSTRY

Kristina Walter

Director, Cybersecurity Collaboration Center, National Security

> "The development and capabilities that were once only possible inside the government are now happening faster in industry-and if we don't partner, we can't put all the puzzle pieces together." - **Kristina Walter**

Executive Summary

Kristin Walter offered a behind-the-scenes look at how the NSA's Cybersecurity Collaboration Center (CCC) has transformed government-industry engagement over the past five years. Speaking remotely from Fort Meade, she outlined the NSA's evolving posture-shifting from a culture of secrecy to one of operational transparency, proactive outreach, and real-time threat sharing with the private sector.

Walter emphasized that industry-not government-is best positioned to action intelligence against cyber threats due to its control over infrastructure, speed of development, and situational awareness. NSA's new model flips the old script: rather than offering companies classified briefings without follow-up, the agency now prioritizes actionable intelligence at the "unclassified but non-public" level-pushing dozens of threat reports weekly to over 1,500 industry partners.

The CCC's operational focus has been to protect the Defense Industrial Base (DIB) and its critical vendors, including large defense contractors and small businesses with little or no cybersecurity maturity. Through government-funded programs, NSA now provides a "menu of defensive services," including attack surface mapping, DNS filtering, autonomous penetration testing, and direct threat collaboration via Slack channels.

Walter cited a turning point during the Russia–Ukraine war, when major tech companies rapidly took sides and began actively defending U.S. allies-proving that values-driven corporate behavior can directly reinforce national security. NSA is now seeing a new wave of proactive engagement from commercial entities asking how to prepare for future conflicts, including a potential crisis over Taiwan.

In closing, Walter said her top strategic goal is to enable industry to take defensive action based on NSA intelligence-without having to wait for individualized government direction. That will require close coordination with the next administration to remove remaining policy roadblocks.

Key Takeaways:

- NSA Embraces Openness and Industry Collaboration: The NSA's Cybersecurity Collaboration Center (CCC) represents a major shift from secrecy to active industry partnership.
- Private Sector Is Central to Cyber Defense: Industry builds the infrastructure and is best positioned to act on intelligence in real time.
- Speed and Volume of Intel Delivery Has Scaled: The CCC pushes out dozens of threat reports weekly to help partners respond rapidly.
- Ukraine War Galvanized Industry Engagement: For the first time, major companies proactively sought roles in potential geopolitical conflict.
- Cyber Support Reaches Deep Into the Supply Chain: NSA provides free cyber services to small DIB vendors, acknowledging their limited resources.
- Four-Part Cyber Defense Package for Small Vendors
- Real-time intel sharing via Slack
- Attack surface mapping & patch guidance
- Automated internal pen-testing (Horizon3)
- DNS blocking using NSA + commercial threat data

Session Recap

INNOVATION CASE STUDY- FROM A BIOMETRIC FASTLANE TO AFFORDABLE COUNTER-AIR WARHEADS

> “We are already at war. We just haven’t mobilized like it.” - **Brian Miller**

Brian Miller
SVP, BMNT

Executive Summary

Brian Miller offered a compelling argument that U.S. national security innovation is not constrained by a lack of technology but by bureaucratic and sociological barriers.

Through three rapid innovation case studies facilitated by BMNT and NavalX, Miller demonstrated how a networked, operator-led approach-dubbed “innovation operations”-can accelerate the delivery of capabilities to the fleet within 12 months or less.

These initiatives succeeded by bypassing traditional procurement bottlenecks and leveraging flexible funding pathways, unconventional partnerships (such as with In-Q-Tel), and stakeholder alignment. His core message: solving innovation problems in government is about people, incentives, and negotiation-not technology.

Key Takeaways:

- Innovation is a Sociological, Not Technological Problem: BMNT’s core thesis: the barriers to innovation are not about access to cutting-edge technology, but about navigating bureaucracy, aligning stakeholders, and creating urgency.
- Case Study 1: Biometric Fast Lanes at Naval Air Station North Island: To solve daily traffic and base security issues, BMNT redirected an unused Marine Corps earmark and partnered with ID.me to install biometric access lanes-doubling throughput in under a year, at no added cost to the Navy.
- Case Study 2: Alternative Navigation for USVs in GPS-Denied Environments: In partnership with In-Q-Tel and Intel, BMNT helped deploy Anello’s low-cost silicon photonics gyro for Task Force 59 in the Red Sea-delivering alternative navigation for < $10K/unit within six months.
- Case Study 3: Real-Time Ocean Telemetry for Naval Special Warfare: NSW Group 4, lacking real-time sea-state data, worked with BMNT to deploy 16 upgraded buoys in under a year, improving risk reduction in austere maritime insertions.
- The “Innovation Operator” Model: A single skilled individual-empowered but embedded-can drive rapid results by forming networks, brokering resources, and cutting across stovepipes.
- Call to Action: Mobilize Like We’re at War: Miller urged a wartime mentality to accelerate innovation-emphasizing that the U.S. is already engaged in great power competition with near-peer adversaries.

Session Recap

RETHINKING THE PRIME MODEL: A NEW INDUSTRIAL STRATEGY FOR NATIONAL SECURITY

Mary Beth Long
Independent Board Director, Aero-vironment

> “What’s being called for is not just a new acquisition model-but a new generation of primes.” - **Mary Beth Long**

Executive Summary

Mary Beth Long called for a shift away from the traditional defense industrial base model, arguing that modern warfare demands a new class of defense primes focused on modularity, speed, integration, and innovation driven by real battlefield needs. Drawing on her board role at AeroVironment and extensive industry experience, she positioned her company’s recent merger with BlueHalo as a blueprint for what the next generation of “new primes” could look like.

Key Takeaways:

- The Traditional Prime Model Is Outdated for Today’s Fight: Defense innovation is shifting from large-scale, domain-specific, exquisite platforms to rapidly adaptable, disposable, and field-tested systems.
- AeroVironment’s Battlefield-Driven Innovation Cycle: Lessons from Ukraine and other modern conflicts show the need for rugged, rapidly deployable tech that can be assembled in the field by tired, overstretched warfighters.
- Toward an Integrated, Modular System-of-Systems Approach: AeroVironment sees the future in flexible architectures that allow rapid hardware swaps, software updates, and international variants.
- New Primes Must Stand Alone: Unlike legacy primes reliant on international sales to sustain programs, AeroVironment’s model is designed to function independently-though exports remain a plus.

Microsoft Security

Defend Against Advanced Threats with AI-Powered, End-to-End Security

Federal mission leaders face immense challenges in combating cyber threats that evolve faster than defenses can adapt. State-sponsored attacks and advanced technologies are targeting critical systems, intensifying the threat landscape.

We've designed our security offering from the ground up to enable Zero Trust-delivering built-in integrations with unified policies, controls, and automation to accelerate your implementation and strengthen your security posture. Instead of using individual tools across each Zero Trust pillar, a truly comprehensive strategy connects them together through a centralized access policy engine and integrated threat protection, delivering in-depth cybersecurity across your on-premises, hybrid, and multi cloud environments.

Building this foundation is critical in today's cyber threat landscape and enables you to integrate AI solutions into your organization's cybersecurity strategy, augmenting the capabilities of your tools and your team. No matter where your organization is on the Zero Trust journey, Microsoft can help you utilize existing solutions and incorporate best practices to help accelerate your agency's success.

Get started today! Reach out to MSFedSecurity@Microsoft.com to learn more.

THANK YOU TO OUR SPONSORS

Microsoft

CRUMPTON VENTURES

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP

GORDON VENTURES

smetzer ASSOCIATES LLC

DEFENSE INTELLIGENCE MEMORIAL FOUNDATION

CIPHERBRIEF

NatSecEDGE

Follow NatSecEDGE for updates on how to attend in 2026