2023

Tuck National Security and Innovation Conference

Prepared by Allison Coukos T'24

SPONSORS

NEW NORTH VENTURES

The John Sloan Dickey Center for International Understanding at Dartmouth

Tuck CENTER FOR PRIVATE EQUITY AND VENTURE CAPITAL

Tuck CENTER FOR BUSINESS, GOVERNMENT & SOCIETY

Tuck REVERS CENTER FOR ENERGY, SUSTAINABILITY & INNOVATION

Executive Summary

The Tuck National Security and Innovation Conference at the Tuck School of Business at Dartmouth College, sponsored by New North Ventures, centered on the importance of collaboration between the private sector, government, and academia to drive innovation and support the national security mission. The conference brought together about 70 attendees across industry, government, and academia, as well as undergraduate and graduate students.

Keynotes from Ron Corsetti, the Civilian Aide to the Secretary of the Army, and Mike Pyle, the Deputy National Security Advisor for International Economics, respectively highlighted the growing relevance for partnerships across the public and private sectors to bolster the United States' national security posture. The absence of a cohesive system and complex acquisition procedures have made it difficult for the government to keep pace with integration of emerging technology to support the national security mission.

Breakout sessions explored topics, including government-driven innovation, the relationship between academia, government, and the private sector, emerging opportunities within the public sector, and the integration of emerging technologies by intelligence and defense sectors. Discussions emphasized the need for streamlined acquisitions, innovation networks, and the integration of strategic industries like energy, AI, and cybersecurity.

Afternoon small group sessions explored key themes like non-dilutive capital opportunities, policy innovation, and strategic engagement for driving innovation. Throughout discussions, the need for long-term, strategic investments in technology, infrastructure, and energy security was highlighted.

There was an emphasis on understanding and navigating the complexities of selling to the government, the role of venture capital in aligning with security measures, and the significance of international collaboration. These discussions articulated a vision emphasizing the integration of innovation and policy, the identification of strategic industries, and the imperative to prioritize secure-by-design products, underscoring the intricate interplay between policy, innovation, and a robust ecosystem for sustainable growth and global security.

The Tuck National Security and Innovation Conference was the inaugural conference for the Tuck School of Business at Dartmouth College, and it created a solid foundation for future conversations, especially at a time when the government is navigating how to best fund innovation and support collaboration with the private sector.

While the public and private sectors have made strides to support collaboration, there is still work to be done. Agencies and departments can support more cross-agency and department collaboration to identify best practices, as each agency and department supports innovation initiatives differently. As barriers are removed to drive innovation forward, the government needs to continue to increase funding, whether it be through grants or alternative funding mechanisms, to support both external partners, like startups, and internal partners, such as the Defense Innovation Unit. If the government chooses to not invest heavily in these areas, it still has the ability to influence investment while not controlling it, such as through the development of centers that are outside of the scope of the United States government but that work hand-in-hand with government players. Overall, conference attendees were optimistic about future collaboration across these different players as those closest to these issues see the progress that is occurring now, and that will continue to occur in the months and years ahead.

Morning and Afternoon Keynotes: Ron Corsetti and Mike Pyle

Both the morning and afternoon keynote speakers underscored the need for a robust collaboration framework involving the government, private sector, and academia to bolster innovation. Ron Corsetti, the Civilian Aide to the Secretary of the Army, and Mike Pyle, the Deputy National Security Advisor for International Economics, were the respective speakers.

The speakers both noted that while those across government, the private sector, and academia understand the urgency in establishing this framework, there is much work to be done. In recent years, there has been a decline in U.S. federal government spending on research and development relative to GDP, which can lead to less investment in innovation initiatives. The difficulty in investing in innovation has been compounded by a complex acquisition process. While there are pockets of government that have established successful processes to accelerate innovation, including international initiatives such as NATO's Defence Innovation Accelerator for the North Atlantic, there is still an overall absence of a cohesive system.

Ron Corsetti highlighted the need for an innovation ecosystem stakeholder model, advocating for interconnectedness among entrepreneurs, risk capital, universities, government entities, and corporate stakeholders. Additionally, the keynotes highlighted how the United States must invest in both domestic and international relationships to drive innovation and fortify national security. Overall, the speakers envision more collaborative synergy between public and private sectors, emphasizing a streamlined process for driving innovation and technological advancement that creates a stronger national security posture.

Mike Pyle commented on the role that international partnership plays in supporting our national security mission. Two key issue areas that he discussed were defense and climate, which, while they can be closely intertwined, pose different priorities. Overall, he noted the importance of the United States leveling the playing field and utilizing international tools to promote stability abroad.

Breakout Sessions 1

Government as an incubator: Exploring the ways in which government can drive innovation internally

In "Government as an incubator: Exploring the ways in which government can drive innovation internally", Nick Reese, Co-Founder and Managing Partner at Frontier Foundry and Former Director for Emerging Technology Policy at the Department of Homeland Security, and Matt Hayden, Former Assistant Secretary of Homeland Security for Cyber, Infrastructure, Risk, and Resilience discussed the ways in which the government, using the Department of Homeland Security (DHS) as a model, can drive innovation internally. During their conversation, the panelists highlighted how there are directorates within government Departments, such as the Science & Technology directorate within DHS, that can serve as hubs or catalysts for internal innovation. However, both noted that the biggest barrier to government innovation internally is internal bureaucracy and processes as well as a lack of funding. The current process to drive innovation is complex and disparate, making it difficult for private sector players, such as startups, to engage with DHS.

The panelists also highlighted the importance of providing funding to drive innovation. The speakers noted how DHS could enable innovation by making it easier for startups to access grants and additional funding streams.

Why the public sector is emerging as an attractive end market

In "Why the public sector is emerging as an attractive end market," moderator Nate Ashton, a Member of the Board of Directors and former Executive Director of The Alliance for Commercial Technology in Government, led a conversation with Tyler Sweatt, CEO at Second Front Systems, and David Kovar, the Founder and CEO at URSA (Unmanned & Robotics Systems Analysis). The panel covered key themes of non-dilutive capital and regulatory challenges, finding opportunity amidst chaos, emerging models from global scenarios, removing barriers and policy innovation, capital dynamics and new entrants, defense innovation and long-term commitment, strategic engagement and partnership ecosystems, execution strategy and value proposition, networking, grant understanding, and time management, and mission focus and balancing speed with thought.

Key Themes

1. **Non-dilutive capital and regulatory challenges:** The public sector offers avenues for non-dilutive capital, yet navigating regulatory hurdles and different investment timelines necessitates a patient and strategic approach from startups and businesses.
2. **Opportunity amidst chaos:** Amid chaotic situations, there lies immense opportunity. However, seizing these opportunities requires thoughtful action, considering the second and third-order effects, especially in a landscape where action impacts larger societal or geopolitical frameworks.
3. **Emerging models from global scenarios:** Recent events, like Ukraine's post-war reconstruction and initiatives like the Warsaw Conference and Drone Summits, showcase emerging models for leveraging public sector involvement in rebuilding and innovation, emphasizing the potential for partnerships and investment.
4. **Removing barriers and policy innovation:** The journey from concept to reality involves challenges. Innovators must focus on removing barriers, including writing policies that facilitate the transition from ideas to actionable projects, particularly in applying commercial tech to public sector needs.
5. **Capital dynamics and new entrants:** The evolving landscape in the public sector demonstrates an inversion in the cost of capital and the emergence of uninformed capital sources. This dynamic creates opportunities for new market entrants but demands informed decision-making.
6. **Defense innovation and long-term commitment:** Leveraging non-dilutive federal funding and navigating the existing contractor base underscore the need for sustained effort and commitment, especially for startups aiming for long-term success in the defense space.
7. **Strategic engagement and partnership ecosystems:** Understanding the ecosystem and "hacking the system" involve strategic engagement strategies, recognizing that the government comprises numerous powerful entities, each acting as significant potential customers or collaborators.
8. **Execution strategy and value proposition:** Success in this space demands a combination of value creation and value protection. Companies need to execute horizontally, emphasizing the importance of a comprehensive strategy.
9. **Networking, grant understanding, and time management:** Navigating the prime and subcontracting dynamics involves understanding SBIR phases, proposal assessments, and stakeholder engagement. Networking and face-to-

face interactions remain pivotal, ensuring thoughtful engagements and pitching aligned business solutions.

10. **Mission focus and balancing speed with thought:** In defense innovation, the focus revolves around missions, considering recent conflicts, like Ukraine and Israel/Gaza, for technological applications. Balancing speed with thoughtfulness remains crucial, accounting for potential second and third-order effects.

Through the wormhole: How the IC/DoD have tried to scout, integrate, and deploy emerging tech over the past 25 years…and what they're doing differently today

In "Through the wormhole: How the IC/DoD have tried to scout, integrate, and deploy emerging tech over the past 25 years…and what they're doing differently today," moderator Adam Caruso, a Tech Scout from Special Operations Command (SOCOM), led a conversation with Jeremy Hitchcock, Co-Founder at New North Ventures, Trevor Hough, Principal Owner at The ADK Group, and Keeley MacAfee, a Senior Associate at Decisive Point. The panel highlighted the evolution of technology collaboration between the intelligence community, Department of Defense (DoD), and the private sector. Panelists emphasized the need for more streamlined acquisitions, deeper collaboration, and the integration of innovative tech solutions, especially in the realms of AI and data analytics, to address the challenges of modern warfare and national security.

Key Themes

1. **Complexities of Tech Integration in Defense:** The discussion highlighted the challenges faced by government agencies, especially at the combatant command level, in integrating emerging technologies. Various protocols exist within different departments, leading to a need for streamlining frameworks for effective tech discovery and acquisitions. The Special Operations Command (SOCOM), for instance, emphasized its learning curve in navigating acquisitions and integrating tech discoveries into their pipeline.
2. **The Role of Innovation Networks:** Initiatives, such as the Propel Accelerator and the National Security Innovation Network (NSIN), serve as pivotal platforms for collaboration between government entities and private sector innovators. The involvement of organizations, like the Defense Innovation Unit (DIU), illustrates the effort to bridge the gap between defense requirements and private-sector innovations.
3. **Navigating Security and Foreign Investment Concerns:** The conversation highlighted the need for stringent due diligence regarding foreign investments and affiliations in technology companies. Concerns about foreign involvement and the challenge of discerning potential risks were discussed extensively, particularly in ensuring the security of supply chains and mitigating potential threats from adversarial entities.
4. **Evolving Approaches to Security and Trust:** Evaluating technology companies requires multifaceted assessments beyond just capabilities. The panel emphasized the importance of scrutinizing not only technology but also a company's founding team, supply chain, and its ability to align with US-based operations and values. This holistic approach aims to ensure reliability and trustworthiness in tech partnerships.
5. **Securing Critical Infrastructure and Supply Chains:** The conversation emphasized the criticality of securing supply chains, acknowledging that it's challenging to entirely disentangle components made by potential

adversaries. Understanding the nuances between jurisdictions and the security of components within software and hardware was discussed, highlighting the need for certified and secure designs.

6. **Regional Innovation and Collaborative Initiatives:** Attention was drawn to regional efforts, such as those in New England with MIT and other universities, aimed at fostering local tech incubation, manufacturing, and innovation. These initiatives aim to reduce reliance on foreign technology by investing in local tech ecosystems.
7. **The Business Case for Trusted Partnerships:** The significance of forging partnerships with trusted sources was underlined as a fundamental part of the defense strategy. Building a robust business case, leveraging innovation networks, and investing in secure infrastructure were highlighted as critical steps for the successful integration of emerging technology in defense operations.

Breakout Session 2

Cybersecurity Tabletop Exercise

In "Cybersecurity Tabletop Exercise," Mike Tetreault, the Cybersecurity Advisor for Rhode Island, Cybersecurity & Infrastructure Security Agency (CISA) of the Department of Homeland Security, Richard F. Rossi, the Cybersecurity Advisor for New Hampshire, CISA, and Woody Groton, Cyber Operations Officer at the New Hampshire Army National Guard explored the vulnerabilities arising from third-party vendors and the multifaceted challenges in the contemporary cybersecurity landscape.

Key Themes

1. **Third-Party Vendor Risk and Cybersecurity Focus:** The conversation highlighted the risks associated with third-party vendors lacking stringent cybersecurity practices, which can create potential vulnerabilities in supply chains and partnerships. One specific example referenced during the tabletop was the 2013 Target breach, where, through a third-party HVAS vendor, over 70 million customers lost credit card and/or personal information. This incident underscored the real-world impact of third-party vendor vulnerabilities and the need for heightened vigilance.
2. **Certifications and Cybersecurity Measures:** The tabletop participants covered the legitimacy and importance of SOC I and SOC II certifications. The participants noted that when businesses pursue and get these certifications it indicates that a business has undergone certain measures to ensure cybersecurity and indicates their commitment to security practices.
3. **Budget Constraints and Training Deficiencies:** A core concern raised during the tabletop was the lack of budget allocation for cybersecurity training and the adoption of best practices to shed light on prevalent vulnerabilities, especially within government entities. When government entities are not adhering to best practices or providing training, it can have significant consequences more broadly. One specific example that participants highlighted was the impact on critical infrastructure, where, if individuals are not trained property or there are not best practices, systems, such as our water supply, can be compromised.
4. **AI's Role and Confounding Cybersecurity:** The participants closed the tabletop by discussing the impact the artificial intelligence (AI) can have on

cybersecurity. AI introduces a new level of complexity to cybersecurity as hackers can use natural language processing and other tools to create even more convincing phishing attempts and amplify the challenge of identifying fraudulent communications.

From the lab to market: the relationship between academia, government, and venture

In "From the lab to market: the relationship between academia, government, and venture," Eugene Santos, Sydney E. Junkins 1887 Professor of Engineering, Dartmouth College, led a discussion with Justin Fanelli, Acting Chief Technology Officer at the Department of the Navy, Major Joe Swain, United States Army Reserves, Karen Presley, Deputy Director of the Technology Transfer Program, National Security Agency, and Lee Krause, Principal, Securboration and Co-Founder, Rampart AI. The panel discussed key themes around a collaborative ecosystem that brings together academia, government, and industry, the role of tech transfer and innovation support mechanisms, encouraging innovation and overcoming challenges, research pipelines, recruitment, and training, and driving and scaling innovation.

Key Themes

1. **Collaborative Ecosystem Bridging Academia, Government, and Industry:**
    - *Addressing the Valley of Death*: The "Valley of Death," the gap between research and implementation, was a reoccurring theme throughout the panel. Participants discussed how academia generates promising ideas that often fail to transition into real-world applications. Collaboration among academia, government, and venture capital is seen as key to addressing this gap.
    - *Mission-Driven Collaboration*: The discussion highlighted the importance of aligning innovation with mission requirements. The urgency to deliver solutions, especially in defense contexts, pushes for tighter collaboration. There's recognition that urgent mission needs demand agile and collaborative approaches. One example highlighted was how universities can align their research pipelines to more focused research areas.
    - *Overcoming Barriers*: Barriers, such as risk aversion in the military and reluctance from established players to embrace innovative newcomers, hinder progress. Participants stress the need to address these barriers to facilitate smoother collaboration.
2. **The Role of Tech Transfer and Innovation Support Mechanisms**
    - *Tech Transfer Legislation and Collaborative Agreements*: Leveraging tech transfer legislation and cooperative agreements, like CRADAs (Cooperative Research and Development Agreements) help to reduce research costs, mitigate risks, and facilitate collaborations with startups and academia.
    - *Hacking for Defense/AI*: Initiatives like "Hacking for Defense" or "Hacking for Intelligence" engage students to solve real-world government problems. These programs provide students with hands-on experience, foster innovation, and potentially lead to viable commercial solutions.
    - *Building a Diverse Ecosystem*: The panel stressed the importance of collaboration across various departments and services within the DoD to converge the disparate initiatives into scalable solutions. Efforts to enable cross-departmental collaboration and create an environment are critical to fostering product-centric thinking rather than being fragmented across different programs. The panelists also highlighted the role of diversifying

collaboration, tapping into minority-serving institutions and diverse thought to enhance problem-solving.

3. **Encouraging Innovation and Overcoming Challenges**
   - *Overcoming Risk Aversion*: The panel discussed the need to balance risk aversion in the military with the necessity for innovation. There's recognition that innovation often involves risks, and the challenge lies in creating a culture that embraces calculated risks.
   - *IP Ownership and Commercialization*: Discussions revolved around managing intellectual property, licensing technologies, and the expectations regarding licensing fees. There's a need to navigate the balance between government-owned IP and incentivizing commercial entities.
   - *Adapting Organizational Structures*: The challenge of integrating technological advancements, particularly AI and machine learning, into organizations structured around human-based processes is acknowledged. There's a need to evolve these organizations towards being more tool-based to fully utilize technological innovations.
4. **Research Pipeline, Recruitment, and Training**
   - *Research Pipeline and Mission-Driven Education:* The panelists discussed challenges in exposing students to mission-driven projects and integrating real-world applications with academia curriculum. One way to potentially bridge the gap between government problems and academia was to shift the traditional research pipeline, where universities focus on basic research and subsequent stages, to focus on research around emerging, real-time government challenges.
   - *Connecting Academia with Government Mission:* The panel highlighted programs, such as "Hacking for Defense," which aim to integrate lean startup methodologies into defense and intelligence at universities, enhancing hands-on learning experiences. Initiatives like "NobleReach" seek to recruit individuals into a life of service and connect them with mentors, fostering a deeper understanding of how their work aligns with larger missions.
   - *Challenges in Recruitment and Training:* Recruiting students for government jobs faces hurdles due to issues, like pay disparities and challenges in exposing them to the nature of government work. Programs focusing on adventure training and real-world problem-solving help retain interest among students, particularly those leaning toward government-related careers.
   - *Educational and Generational Divide in Government Roles*: The panel highlighted the need to train and equip military personnel, particularly non-commissioned officers (NCOs) with technological skills relevant to their missions. Challenges exist in educating higher-ranking officers and officials about the advantages and applications of emerging technologies, like AI and unmanned systems, requiring a shift in thinking and a focus on outcome-driven metrics.

5. **Driving and Scaling Innovation**
   - *Addressing Skill Shortages and Encouraging Technology Adoption:* The panel discussed the need to address the current skill shortages, especially in emerging technologies, like AI, and the importance of quicker adaption within government structures. They emphasized automation and simplified tools to ease tasks for lower-ranking personnel without replacing jobs is essential in driving technology adoption.

- *Fragmented Innovation Initiatives:* The DoD has multiple innovative initiatives across different services, such as contracting initiatives, like OTAs, policy adjustments, and hubs, like NavalX, AFWERX, and innovation units. Each service is tackling innovation individually but could benefit from collaborating and learning from each other's successes and failures.
- *Scalability Challenges*: The primary concern is not just access to innovative solutions but ensuring that these solutions can scale effectively to cater to thousands of users, a concern raised by clients and venture capitalists alike. The challenge lies in transitioning from lab capability to products usable by end-users within a reasonable timeframe, which often takes too long due to bureaucratic procedures.
- *Data Access and Ownership*: The discussion highlighted challenges related to access to realistic data sets for testing innovative solutions. There's a need to ensure data availability and access, especially in conflict zones, without compromising ownership rights.
- *Challenges Faced by Small Businesses*: Small businesses face obstacles in obtaining FCL (Facility Clearance) and PCRs (Personnel Clearance) to participate in innovative programs and initiatives like OTAs. Access to these clearances is often challenging, hindering their ability to contribute to government projects.
- *Need for Speed and Innovation*: There's a call for faster adoption of innovative technologies and processes within the DoD. Panelists discussed the need for a change in attitude and more innovative approaches to streamline bureaucratic processes, especially in awarding contracts and clearances to smaller businesses.
- *Engagement and Relationship Building*: The consensus is that relationships and engagements play a pivotal role in overcoming barriers. Building strong connections between commercial entities and government partners can facilitate smoother interactions and more effective collaboration.

Fueling our future: Exploring innovation and challenges in energy security and resiliency

In "Fueling our future: Exploring innovation and challenges in energy security and resiliency," moderator Allie Coukos, the conference organizer, led a conversation with Pete Mathias, a Partner at Alumni Ventures, and Michael Baskin, PhD, Strategic Partnerships Manager, Defense at National Renewable Energy Laboratory. The panel discussed the need for sustained, strategic investment in both technological innovation and infrastructure development to ensure energy security and resilience, emphasizing a multifaceted approach involving collaboration, long-term vision, and addressing critical bottlenecks in capacity and deployment.

Key Themes

1. **Defining Energy Security**: Energy security encompasses global petroleum flow, energy access, and the significance of energy in military operations. Energy security is not solely a technological issue; it involves strategic, operational, and tactical aspects.
2. **Energy Investment Opportunity**: Energy is an essential yet untapped area for venture capital and investment. While software and tech have seen significant investment, energy remains underinvested.
3. **Vulnerability of Infrastructure**: The US energy infrastructure is physically and technically vulnerable, impacting global petroleum flow and electrical

grids. The recent Texas grid outage exemplified the economic and human costs of a grid failure.

4. **Long-Term and Generational Perspective**: Addressing energy security is a generational problem that requires long-term investments and strategic thinking. This type of long-term investment requires venture capitalists to rethink investments in the space as traditional VC timelines (high growth in short timeframes) are diametrically opposed to the timelines required for energy investments. Hardware and deep tech innovations present substantial opportunities but require sustained, patient investment.
5. **Capacity and Bottlenecks**: Capacity, rather than solely technological innovation, is a crucial bottleneck. This capacity constraint involves people, processes, and the need for infrastructure expansion. The bottleneck extends to the queue of projects waiting to connect to the grid, indicating a need for a focus on building solutions, such as transmission lines, that expand the grid and its capabilities.
6. **Innovation and Deployment**: Innovation is at the margins in hardware and deep tech. Deployment and demonstration are critical stages that require de-risking through financial backing and loan programs. Government teams, particularly those at the Department of Energy, are identifying ways to foster and drive this innovation and collaboration between public and private sector partners.
7. **Collaborative Solutions**: Energy security involves everyone. Initiatives, like those in the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response, aim to level up utilities, emphasizing the need for collective efforts to tackle vulnerabilities.

Small Group Discussions

Go-To-Market with the Government: The ins and outs of selling to government buyers

In "Go-To-Market with the Government: The ins and outs of selling to government buyers," moderator Kevin Liu Huang, CEO at Dextral, led a conversation with Bill Cameron, Managing Director at 3Comply, and Aneel Alvares, Director, Defense Engagement at Defense Innovation Unit. The panel aimed to equip small businesses and startups with the essential knowledge and strategies needed to navigate the complexities of selling to the government, while emphasizing the importance of innovation, compliance, and cybersecurity readiness.

Key Themes

1. **Navigating the RFP Process**: It is crucial for small businesses and startups selling to the government to understand the Request for Proposal (RFP) process. Different agencies and departments have different procurement requirements, submission guidelines, and evaluation criteria.
2. **Program Delivery and Governance:** Efficient program delivery and robust governance structures are key when supplying to government entities.
3. **Prime versus Subcontracting:** When selling to the government, companies can either pursue being a prime contractor or a subcontractor, each having different implications when it comes to conducting business with the government. But a startup or small business doesn't need to win a prime contract via RFP to earn revenue selling to the government. There are other

avenues, such as subcontracting or reselling that exist for those knowledgeable enough to use them.

4. **Available Support for Businesses**: There are significant resources and support systems available to small businesses, such as state-sponsored APEX Accelerators and DoD incubators that offer guidance and mentorships. When working with the government, it's crucial to have a uniformed leader advocating for your technology – programs such as these help create those connections.
5. **Unique Aspects of Selling to Government**: Selling to the government has a unique regulatory environment, including the Federal Acquisition Regulation Supplement (FARS) and Defense Federal Acquisition Regulation Supplement (DFARS) that emphasize American-made product requirements. Additionally, sellers need to understand and articulate the differences between commercial off-the-shelf (COTS) products and meeting specific government specifications when offering products/services. Because of this complex environment, companies with parallel commercial businesses will have less existential pressure to make unfriendly government sales process work – dual revenue streams can be incredibly beneficial.
6. **Data Handling and Cybersecurity Requirements**: When working with the government, suppliers can handle different types of data, such as Classified Information, Covered Defense Information, and Non-Public Federal Contract Information, and there are associated cybersecurity requirements depending on the data classification.

A Path Forward: How venture capital and government can work together TODAY to further the national security mission

In "A Path Forward: How venture capital and government can work together TODAY to further the national security mission," Lauren Zabierek, Senior Advisor at CISA, Jeremy Hitchcock, Co-Founder at New North Ventures, and David Skinner, Northeast Regional Director at the National Security Innovation Network (NSIN) discussed the intricate interplay between venture capital, government policy, and innovation ecosystems and how these players can align to address evolving security needs, navigate diverse funding avenues, and explore strategic sectors for growth and collaboration.

Key Themes

1. **Security-Centric Product Development:** The evolving landscape underscores the significance of prioritizing secure-by-design products, aligning with Presidential Executive Orders on cybersecurity. Startups aiming to engage with the government need to embed robust cybersecurity features into their offerings from inception.
2. **Diverse Funding Avenues for Startups:** Exploring various funding streams available to startups, including non-dilutive options like SBIR/STTRs, venture capital, and grant funding, is critical for startups' growth and innovation trajectory.
3. **VC Focus on Security Measures:** There's been a shift in venture capitalists' thinking, particularly concerning startups targeting government contracts. VCs are increasingly prioritizing strong security protocols over first-to-market advantages, recognizing the imperative for startups to align with robust security standards when eyeing government contracts.
4. **DIU Onramp Hubs for Accelerating Innovation**: The Defense Innovation Unit and NSIN's establishment of defense innovation onramp hubs across

strategic regions in the country accelerates innovation, fostering growth and collaboration in defense technology.

5. **Global Perspective on National Security:** National security considerations are transcending domestic borders, with a growing emphasis on international lenses, notably exemplified by initiatives, such as the NATO Defense Innovation Accelerator for the North Atlantic (DIANA) program.
6. **International Collaboration**: Both government entities and private sector players advocate for enhanced international cooperation, recognizing the significance of collaborative efforts in advancing innovation and security solutions globally.
7. **Policy and Innovation Nexus**: Acknowledging the interplay between policy, innovation, and a robust ecosystem, the focus extends beyond technological innovation to encompass policy innovation. Creating supportive policies and systems that cater to the heart of the ecosystem – its people – is pivotal for sustainable growth.
8. **Strategic Industries for Innovation**: Highlighting areas of strategic importance, including advanced batteries, 5G, AI, semiconductors, and more, underscores opportunities for startups and individuals interested in the innovation space.