WAR ON THE ROCKS

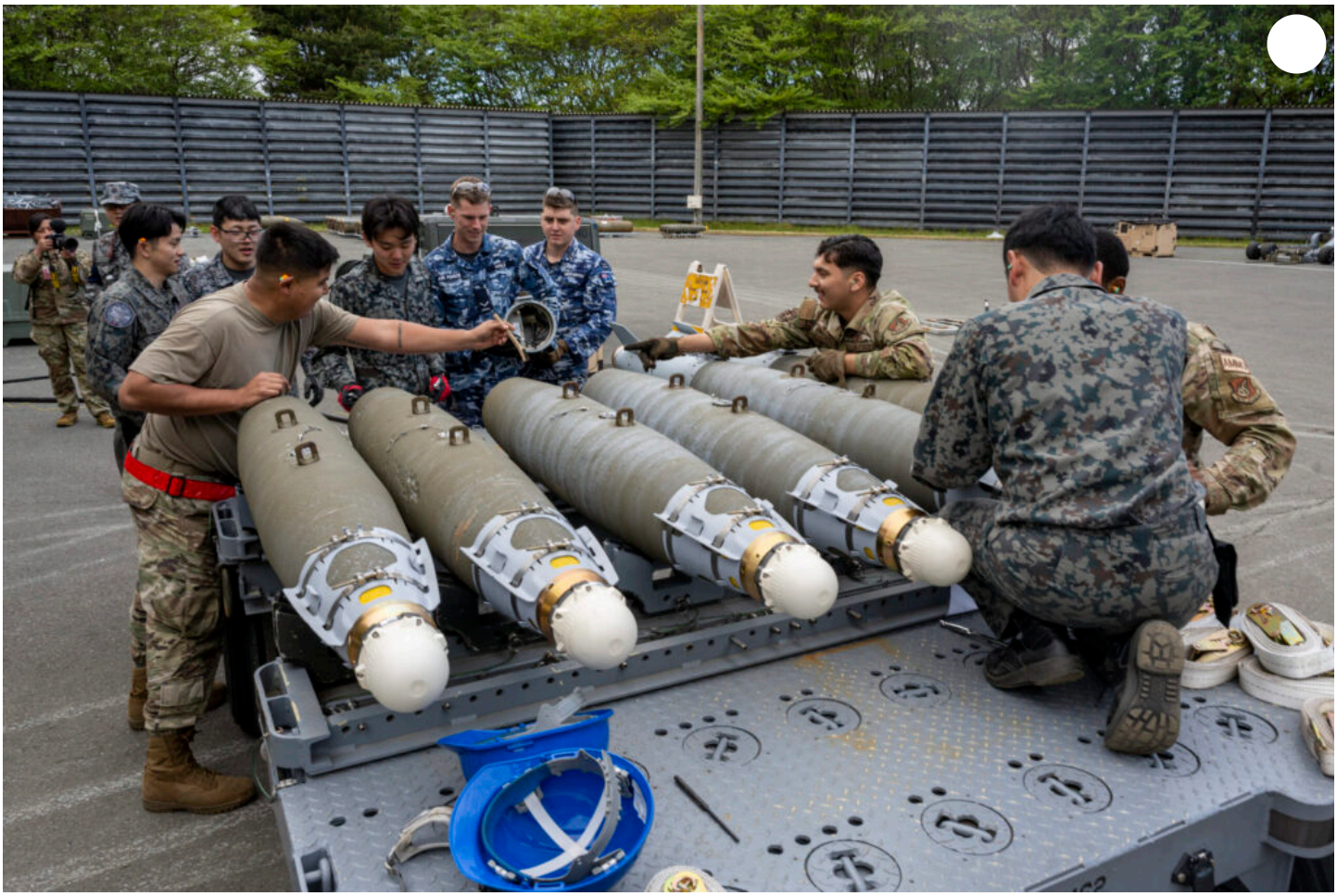
TEXAS NATIONAL SECURITY REVIEW

OVERCOMING GOLIATH: HOW THE DEFENSE ESTABLISHMENT CAN MAXIMIZE ALLIED INNOVATION

NICK IORIO AND SCOTT DEWITT

OCTOBER 7, 2024

COMMENTARY



The Department of Defense has a building alliance capability problem. Through the 2018 and 2022 National Defense Strategies, the Department of Defense has trumpeted its alliance system as a primary pillar of national security. Yet as of late 2024, the collective benefits of coproduction and co-development of the critical technologies that will decide or deter the next conflict have remained woefully untapped.

The nature of this challenge is twofold. It involves a deeply entrenched and networked defense-industrial complex, and an over-engineered security

cooperation bureaucracy that is impressively resistant to change. These combined forces are confounding the Department of Defense in systemically identifying and resourcing the pivotal emerging technology solutions to build alliance capabilities. Any way you slice it, external industry forces and defiant legacy approaches are actively undermining the Department of Defense's ability to shape alliance defense outcomes. To overcome these forces, the Department of Defense needs to transition from a primarily "*sell legacy American defense platforms*" security cooperation approach to a "*build with, and sometimes exclusively for*" allies and partners capability mindset to address this problem.

The Department of Defense security cooperation enterprise is well placed to lead this transition through an allies and partners cooperative innovation (co-innovation) development model. A development model that starts with a convergence of national security interests and evolves into a confluence of defense innovation activities. This starts with a mutual understanding of existing and emergent capabilities, moves into cooperative research and collective planning, and then migrates through the development process to joint production. A fully inclusive process, by incorporating proven defense partners in the Department of Defense alliance capabilities community, will unlock the intangible benefits of the multilateral pillar of the National Defense Strategy. To enable this co-innovation model, the Department of Defense should confront the dual challenge of its own highly federated stakeholder system and the consolidation of the complex that President Dwight D. Eisenhower cautioned against in his farewell address. Otherwise, we may find the complex being the Goliath that defeats David.

This approach won't be easy, especially for a highly federated community like security cooperation. It requires a concept and capability development focused on allies and partners, more effective workforce training, and greater acceptance of technology transfer risk. In tackling these challenges, the Department of Defense's investments in scaling innovation for the Joint Force can help, as well as the secretary of defense's recent foreign military sales guidance. There are also valuable lessons to be drawn from current conflicts

such as Ukraine, while the 2017 congressional security cooperation reforms can provide a solid foundation to effect change.

What the Future Could Look Like

Effective co-innovation is particularly important as we enter a future where software is crucial to battlefield success. The role of software in enabling and challenging actions on the battlefield will likely have a profound impact on the warfighter, specifically the small unit (company and below). These formations will need to operate more independently from larger units and headquarters located in the battlefield's rear. These units will need to apply their own locally sourced solutions to operate in communications, logistics, and mobility denied environments. Small units' success will depend on their ability to collaborate with their friends in immediate proximity, which will include allies and partners. Rearward battlefield technological support from higher headquarters and the broader defense enterprise will be the exception, not the rule.

Let's explore a fictional scenario to give an example of how this might look.

A platoon-sized force, dispersed over an operating area, is using robotic, autonomous, and unmanned vehicles. These assets, including small tactical vehicles and one-to-two legacy platforms retrofitted with autonomous enabling software, can launch and command small ground and aerial drone swarms. The pairing of these manned and unmanned capabilities enables the platoon to independently integrate its reconnaissance and targeting strengths, conduct local parts production, and employ software fixes. Importantly, these systems took a *build with* approach, enabling the U.S. platoon to collaborate more efficiently with local allied units rather than depending on such collaboration taking place in the rear.

Concerted efforts through production diplomacy enabled this platoon's survival. Efforts such as the Partnership for Indo-Pacific Industrial Resilience and lessons from the Ukraine Contact Group resulted in a diverse set of industrial and innovation partnerships providing for commonality and modularity across old and new capabilities. The NATO and Ukrainian engagement on DELTA informed approaches to battle systems integration. A combination of government open-source collaborations applied lessons from AUKUS Pillar II and partnerships across countries' defense innovation centers of excellence to proliferate joint prize challenge outcomes that received validation through unit- and task force-level operational applications.

How can this scenario become reality? While the primes continue to deliver big ticket technologies, smaller companies would increasingly avoided insolvency through early entry to the international defense market. The resulting international commercial collaborations will foster the scaling of novel battlefield solutions, expanding American, allied, and partner defense-industrial base resiliency.

Freeing Security Cooperation Innovation from Legacy Limitations

The above scenario does not discount the need for enterprise-level solutions. Indeed, even Eisenhower was not calling for the disestablishment of the military-industrial complex. Instead, he was warning that such establishments could foreclose wider and diverse opportunities for innovation coming from a diverse pool of innovators. America did not heed Eisenhower's warning. The Department of Defense and Congress, in partnership with industry and an insular bureaucracy, have only further entrenched a broken complex through perhaps well-intentioned but poorly considered defense-industrial retrenchment policies in the early 1990s.

Even in today's more innovation-friendly regime, there is a question in terms of how many defense tech or dual-use start-ups are becoming programs of record with the ability to disrupt the complex. Instead, many become unwilling partners to primes. While there is a lot of potential for the development of a more robust, diverse, and hence resilient enterprise, there is an institutional tendency to still build toward brittle solutions and supplier bases.

The security cooperation community has a golden opportunity to contribute toward building a more robust defense-industrial base and enabling the types of collaborations for the warfighter outlined in the above scenario. The value of this effort is clear — more resilient forces capable of operating and adapting in chaotic, complex, and degraded operational environments. The trick is going to be in the art of piecing together existing approaches, authorities, and insights to create the outputs that affect change.

Freeing Security Cooperation from the Constraints of Bureaucracy

In establishing the Defense Innovation Community of Entities and placing the Defense Innovation Unit as the head of the innovation ecosystem, the Department of Defense is taking a strong step toward enabling more coherent innovation identification from non-traditional defense commercial sources. For these efforts to strengthen the combined American, allied, and partner industrial bases, organizations across the Office of the Secretary of Defense and the Defense Innovation Unit will need to identify ways for the Defense

Innovation Community of Entities to deeply engage with the security cooperation community. Processes will need development that create repeatable methods to understand partner nation operational problems, associated requirements, and the landscape that could be addressed by the non-traditional defense innovation industry.

Getting creative on funding approaches is the next challenge. Many security cooperation funding cycles are bureaucratic, arduous, and planned over a five-year timeframe. They frequently rely on delivering previous generations of technology. The security cooperation community will need to dust off not regularly used authorities to create security cooperation research and development opportunities with allies and partners. This approach may require cross-government support.

Efforts such as AUKUS and the India-U.S. Defense Acceleration Ecosystem provide proof of concept for how to bring more capable international partners along on America's innovation journey. For grant recipients, it is necessary to find creative ways to employ grant assistance funds to enable non-traditional partnerships in the commercial, academic, and non-profit spheres. These types of partnerships, if they are viable, would have the added benefit of helping non-traditional American defense companies expand their portfolios and off-set risk as they seek a sustained customer base among the services.

Recommendations for Future Exploration

Fostering Security Cooperation Innovation Connections

It is vital for the security cooperation community to become more fluent in the non-traditional commercial sector. Many companies in this category don't have the business development bandwidth or knowledge on how to engage the international defense market. The core issue stems from translation, as both sides don't know how to communicate with one another. One idea to get after this shortfall is establishing a Critical Defense Technology Fellowship program for security cooperation and special operations experts to have dedicated space to engage with non-traditional technology companies. The Defense Innovation

Unit On-Ramp Hubs and defense tech accelerators are well placed to serve as this conduit. A creative broadening assignment of this nature will help advance two-directional communication and education needs on the government and industry side, while also acting as a career capstone event for disruptive defense technology professionals. An innovation-focused fellowship would thrive within a well-aligned partnership between the Defense Innovation Unit, the Defense Security Cooperation University, and the new Defense Security Cooperation Service. Outside of the need for funding for such a fellowship, concerted thought would need to be given to making this assignment a strong pathway for civilian and military career advancement rather than an off-ramp to a commercial career.

Security Cooperation Workforce Reform

Security cooperation workforce reformation has been the "*soupe du jour*" over the last decade. Unfortunately, more time has been spent on the low hanging fruit of defining the community, than getting after maximizing the impact of these uniquely qualified and well-placed practitioners. Recognizing that the security cooperation workforce is small, overtaxed, and has multiple bosses, the Department of Defense may consider applying some of its innovative "gig" worker thinking to augment security cooperation officers' knowledge and collaborations with non-traditional industry. Such approaches might include rotating select technology sector-adjacent reservists or National Guard State Partnership Program members with specific non-traditional industry experience through Offices of Defense Cooperation or creating a reverse skill-bridge program. This continuous cross-pollination would allow mid-career, non-government professionals with non-traditional commercial exposure the opportunity to advance co-innovation opportunities. A competitive submission process, informed by any number of the competitive submissions processes the Department of Defense already runs, should address any implied favoritism risks.

From Stovepipes to Cells

At the unit level, there are several efforts by the services to create innovation cells to foster local solution development. Taking these lessons, and lessons from the National Guard State Partnership Program, the security cooperation community could consider piloting a series of multilateral unit-level innovation cells. These cells could allow the United States and foreign partners to share common small-unit challenges, conduct unit-level solution generation competitions, and open avenues for participating companies to gain economies of scale.

This type of collaboration would require leadership direction from the service secretaries and service chiefs to prioritize and drive interoperability requirements through their Small Business Innovation Research programs, policy and operations directorates, and in partnership with the wider security cooperation community. The good news is that efforts like the Navy's new Project 33 and the Army's Transformation in Contact, combined with existing task force and innovation cell activities, provide necessary leader-level signaling. The next step is acting.

Allies and Partners Capacity Building Institutional Reinforcement

On the structural front, an approach the security cooperation community should explore is advocating for country level Joint Interagency Innovation Cells at priority U.S. embassies. This cell could receive fellows, gig workers, or reverse skill-bridge participants, act as a node for defense innovation teams, and coordinate with security cooperation stakeholders. The Defense Security Cooperation Service could act as the entity that coordinates the various elements of this program. It would require the White House, National Security Council, and congressional support but, as with every other recommendation here, the pieces of the puzzle are there for alignment.

Conclusion

The risk that the existing military-industrial complex currently poses to the effectiveness of America's critical technology cooperation with allies and partners demands prompt action. The good news is, there is an established and

willing community ready to support the development and integration of critical technologies with allies and partners. The security cooperation community, with appropriate prioritization and resourcing, will play a seminal role in facilitating alliance capability development. But this shift will require a fundamental change to the defense acquisition system *status quo*.

The bottom line is a security cooperation community focused on delivering legacy program sales should diversify its approach to prioritize delivering innovation. A unified security cooperation community emphasis on fostering this co-innovation ecosystem, in partnership with the Department of Defense's existing innovation centers of excellence, could very well provide the potent mix necessary to build resiliency for the warfighter in the not-so-distant battlespace.

Nick Iorio is a senior advisor with Forge Group LLC and supports government clients and commercial entities in designing and implementing the delivery of ally and partner programs across the Indo-Pacific. The views expressed here are his alone.

Scott DeWitt is the executive director for Forge Group LLC's Regional Policies and Strategies Practice, a specialized group of international engagement practitioners focused on maximizing defense collaboration with allies and partners.

Image: Senior Airman Antwain Hanks

COMMENTARY

youremail@domain.com

SUBMIT

GET MORE WAR ON THE ROCKS

SUPPORT OUR MISSION AND GET EXCLUSIVE CONTENT

BECOME A MEMBER

FOLLOW US

NEWSLETTER

youremail@domain.com SUBSCRIBE

SIGNING UP FOR THIS NEWSLETTER MEANS YOU AGREE TO OUR DATA POLICY

ABOUT

MISSION

PEOPLE

FOUNDER'S CLUB

CONTACT

MEMBERS

JOIN

WAR HALL

PODCASTS

WOTR

NET ASSESSMENT

JAW-JAW

HORNS OF A DILEMMA