DEFENSE INNOVATION BOARD

OPTIMIZING INNOVATION COOPERATION WITH ALLIES AND PARTNERS

innovation.defense.gov

Table of Contents

Preface

Since World War II, the United States' network of allies and partners has stood as the cornerstone of our global strength and the envy of our adversaries. This network covers at least 76 countries, including formal relationships with 32 NATO and 19 major non-NATO allies, and varying defense agreements and other military-to-military engagements with at least 25 other strategic partners. These nations are force multipliers, leaders in innovation, science and technology, and champions of shared values, principles, and norms. Recognizing this, U.S. national security documents broadly highlight the profound importance and urgency of working through this network. The 2022 *National Security Strategy* states that “we will work in lockstep with our allies and partners and with all those who share our interests,” and the 2022 *National Defense Strategy* affirms that “we will prioritize coordinated efforts with ... international partners in the defense ecosystem to fortify the defense industrial base, our logistical systems, and relevant global supply chains."

Yet, the Department of Defense (DoD) is failing to fully integrate allies and partners into a networked defense industrial base, and to modernize the concepts, systems, and processes that enable these relationships to flourish. The need to work with allies and partners has outpaced the DoD's ability to do so. Be it munitions, export controls, co-development, co-production, and co-sustainment, capability integration, communications interoperability, or crowding-in trusted capital across global industry, the DoD is failing to address shortcomings in international engagement amid a rapidly evolving global security landscape. Fundamentally, the risk we face today is not that we accidentally release classified information to an ally, or that we allow the export of a protected technology to an unprepared partner. The risk we face today is that on day-one of a conflict, we have failed to properly integrate and align with the nations that underpin our military strength.

Sharing sensitive technologies and information while maintaining security is a delicate balance, and trust-building is an often difficult and frustrating process. Different nations use different communication systems, equipment, and protocols, and ensuring seamless data exchange and communications interoperability across these systems is not easy. Establishing common standards across allies and partners for hardware, software, and procedures is essential, however, reconciling existing systems with new standards can be a tall order within the DoD, let along across different countries. Coordinating logistics for joint operations involving complex supply chains, transportation, and maintenance also requires extensive planning. Finally, absent senior leadership demonstrating repeatedly the political will to think big, domestic political incentives wrapped up in concerns about protecting U.S. firms will continue to hinder opportunities to strengthen American industrial competitiveness through deepened collaboration among allies and partners. Harmonizing legal and policy frameworks is necessary, but under the existing regime of incentives, there remains considerable political pressure to maintain standing rules such as domestic sourcing requirements. Further still, each military has its own culture, doctrine, and decision-making processes, and bridging these gaps across allies and partners requires monumental understanding and compromise.

Still, working with allies and partners is important now more than ever as they lead increasingly in key areas of defense-related technology innovation, and given the expectation for integrated operations with multinational coalitions. According to the 2023 *National Defense Science and Technology Strategy*: “In the past, the Department’s leadership in science and technology provided the United States and our allies and partners with unmatched capabilities. However, advanced science and technology are now available worldwide.” The DoD's latest strategy addressing this challenge, its first-ever *National Defense Industrial Strategy* published in January 2024, crystallizes the problem now facing the United States:

> "Over three decades the People's Republic of China became the global industrial powerhouse in many key areas – from shipbuilding to critical minerals to microelectronics – that vastly exceeds the capacity of not just the United States, but the combined output of our key European and Asian allies as well. … These threats, along with transboundary challenges like COVID-19, demonstrate the imperative for increased and improved defense capabilities for both the United States and our allies and partners."

Throughout the DoD, numerous efforts are underway to integrate allies and partners and to reform the systems managing these relationships, but significant structural and cultural issues abound. Addressing these issues is not just a matter of ceremony, it is essential to honing the DoD's competitive edge and warfighting excellence to ensure US global leadership in the 21st century.

The Defense Innovation Board (DIB) is chartered with the authority and responsibility to provide independent, practical, and actionable recommendations to the Secretary of Defense and other DoD leaders on catalyzing innovation within the Department to strengthen our national security and warfighting capabilities. The following report addresses a multitude of concerns identified in the international engagement space and provides a body of recommendations that will meaningfully address the key issues inhibiting the DoD's ability to work with allies and partners effectively.

This study reflects the passion and commitment of the Defense Innovation Board members to drive change and scale innovation at the Department in support of our national defense mission. Their findings are supported by a rigorous research approach triangulating academic insights, industry practice, and Department of Defense context and equities from across the services.

Acknowledgements

Defense Innovation Board Members

Michael R. Bloomberg, Chair
Charles Phillips
Hon. Sue Gordon
Mary Meeker
Hon. Dr. Will Roper
with
Dr. Gilda Barabino
Reid Hoffman
Admiral (Ret.) Mike Mullen
Ryan Swann
Hon. Mac Thornberry

Executive Director & Designated Federal Officer

Dr. Marina Theodotou

Alternate Designated Federal Officer

Carrie Shideler

Staff

Jacob Sharpe
Elliot Silverberg

Khalia Alexander
Zackariah Crahen
Logan Hatfield
Melanie Heinlein
Kimberly Hidalgo
Christina Hilf
Abigail Linman
Dr. Juan Merizalde

Executive Summary

The Defense Innovation Board (DIB) was tasked to deliver a study that provides specific and actionable recommendations on optimizing innovation cooperation with allies and partners. Effectively integrating allies and partners is essential to building global stability, buttressing collective strengths, and ensuring that U.S. and allied and partner nation warfighters have access to the capabilities they require for the full spectrum of conflict. Properly developed, these networks will ensure technology advantage for the United States and its allies and partners in the 21st century.

To better understand the Department of Defense (DoD)'s successes and failures in innovating with allies and partners, the DIB convened discussions across the Department, the U.S. federal government, U.S. industry, and foreign counterparts to identify pragmatic insights, best practices, and solutions to specific challenges. In the process, we noted that:

- The United States is no longer the leading source of progress across critical areas of defense-related technology innovation, such as 5G, hypersonics, and electronic warfare, while our allies and partners increasingly lead in other areas, including semiconductors, directed energy, and quantum science.
- The price point of deterrence is decreasing as evidenced by recent conflicts in Ukraine, Gaza, and the Red Sea, often demonstrated by the attritive use of low-cost surveillance and sensor-shooter networks. Maintaining deterrence hinges now more than ever on cooperating with allies and partners.
- There is a significant gap within the DoD between rhetoric and action regarding co-development, co-production, and co-sustainment, particularly outside of the Five Eyes and NATO allies. Longstanding regulatory and compliance frameworks, such as International Traffic in Arms Regulations (ITAR), remain primary blockers to collaboration.
- Addressing key barriers to collaboration requires significant, sustained, and well-aligned U.S. federal interagency coordination, particularly between the DoD, Department of State, and Department of Commerce.

Accordingly, the DIB identified several overarching key priorities:

- **Interoperability & Resource Sharing –** The United States and its allies and partners need to prioritize interoperability, allowing them to send resources quickly across established systems to support one another against intertwined global threats. This is crucial for effective cooperation in multinational operations.
- **Defense Production –** The United States in conjunction with the broader international industrial base must enhance defense manufacturing capacity. While NATO and Indo-Pacific allies possess sophisticated armaments, there is a collective shortage of materiel. Improving production capacity is critical for deterrence.
- **Seamless Distribution –** Streamlining distribution processes for U.S. military sales and transfers is vital. Currently, domestic and foreign orders are fulfilled by the same assembly lines, but there are procedural differences for DoD foreign military sales (FMS) which are primarily overseen by the Department of State. The DoD should continue working with State to claw back FMS rules that delay arms shipments to key allies and partners.
- **Exportability –** The United States possesses numerous exquisite systems that allies and partners desire, including advanced combat aircraft, nuclear-powered submarines, space capabilities, and

autonomous vehicles. Moreover, the DoD has a history of sharing high-end defense technology, such as the F-35 fighter jet. The DoD should vastly expand its efforts to incentivize U.S. industry to consider exportability to allies and partners as a first principle of capability development.

- **Leveraging Allied Strengths –** Allies and partners can and should be allowed to contribute within their areas of expertise. For example, Japan and Republic of Korea (ROK) shipbuilding, Norway anti-ship missiles and munitions, Israel air and missile defense, Poland missile production facilities – the list goes on. The DoD should leverage these strengths through new and innovative mechanisms of cooperation.
- **Vendor Lock –** Legacy systems and platforms are subject to vendor lock with specific industrial base participants, hindering efforts to rapidly divert and scale their production for allies and partners. The DoD should leverage existing authorities to avoid vendor lock, such as a 2017 law requiring a modular open systems approach for defense acquisition, while introducing time limits on intellectual property (IP) protections for legacy, non-exquisite, lower-end systems. Resembling the pharmaceutical industry's approach of maintaining IP protections for innovators while leaving the door open for third-party drug manufacturing as time passes or as demand shifts, this would enable vendor switching and scale production of legacy systems that allies and partners require urgently.

Key Recommendations

A) **Leadership –** Given the global, multi-theater challenges facing the U.S. defense industrial base, *the DoD must prioritize international defense industrial cooperation and elevate that portfolio to the level of continuous, seamless, and thoughtful attention and execution that it now deserves.* The 2018 USD(AT&L) split into the USD(A&S) and USD(R&E) left the international defense industrial cooperation portfolio disjointed, without an empowered authority to singlehandedly engage international industrial base partners as the Secretary and Deputy Secretary of Defense's principal advisor on all industrial base issues.

B) **International Cooperation Priorities –** The DoD needs a more centralized process of collaborating with foreign partners at the project level, including a more strategic approach with standards and guidelines for how program managers identify and select collaborative technology development initiatives with allies and partners. Progress requires starting small, building viable proofs of concept, assuaging historical or cultural distrust issues, and making incremental adjustments throughout to entrenched government bureaucracy that interferes in cooperation.

C) **Regulatory & Compliance Reform –** In order to build a networked defense industrial base, the DoD must first create a regulatory and compliance environment that allies and partners feel comfortable navigating and, with time, harmonizing with their own. ITAR serves a necessary mission, safeguarding U.S. treasure, but has not been fit-for-purpose for some time. Other DoD frameworks, namely the Technology Security and Foreign Disclosure (TSFD) and Cybersecurity Maturity Model Certification (CMMC) processes, are also interfering with core national security and foreign policy objectives.

D) **Information Sharing & Communications Technology –** The importance of information sharing and communications technology, and how far behind we are in effectively modernizing the systems and processes governing this space, cannot be understated. Within the DoD, frustration regarding the ability to get information to allies and partners is omnipresent. Defense personnel, especially below the senior level, are not empowered to take decisive action regarding what information can and should be shared, and instead are paralyzed by fear of non-compliance and security violations.

E) **AUKUS –** AUKUS is the primary opportunity for the DoD to get openness and collaboration right. It is between longstanding allies who share a common language, values, and strategic vision, and was formulated in a time of emphasis on allies and partners. Unlike NATO and other established

multilateral institutions, the vestiges of Cold War secrecy that shaped their evolution do not have to define AUKUS's future. Properly realized, AUKUS can serve as a 21st century model for co-innovation with allies and partners, and a resounding success as the DoD continues down a new path of innovation cooperation.

F) **NATO & Europe –** While NATO has long been a cornerstone of DoD international engagement and cooperative innovation, numerous barriers persist to fully realizing the alliance's potential. Traditionally, NATO has been a source of military hardware sharing, maintenance, logistics, and mutual defense. These efforts are generally conducted on an "as-needed" basis and, since the end of the Cold War, have not been a source of long-term strategic coordination.

G) **Indo-Pacific –** As the DoD's priority theater, and an integral source of economic prosperity, technological development, and military capability, the Indo-Pacific is an increasingly essential hub for co-innovation. Despite this, outside of AUKUS, the DoD is not adequately integrating key allies and partners, thereby leaving significant resources and capabilities underutilized. Early efforts, such as GMLRS co-production in Australia, are encouraging indications of greater integration, but remain nascent. Properly integrating emerging partners into its collaborative innovation network should be a top priority for the DoD, and for the DIB's proposed Undersecretary of Defense for International Industrial Cooperation (USD(IIC)).

Across numerous stakeholder interviews and engagements, it was abundantly clear that DoD leaders and warfighters alike are deeply committed to the mission of more seamlessly integrating allies and partners. However, achieving defense interoperability is a complex and long-term operation demanding technical, cultural, and logistical realignment, along with overcoming legal and security challenges. In order to adequately address these issues, and to heed the call of our guiding strategic documents, significant senior leadership attention and collaboration across departments and agencies will be required. Adoption of the recommendations found in this report will need a high-level approach paired with open and efficient cooperation across allies and partners.

Introduction

Allies and partners have been a cornerstone of U.S. strength since our nation's founding. These nations, across the world, have fought alongside us, innovated with us, and championed our shared values. Today, this network remains a vital component of U.S. power, and has continued to forge a more secure and prosperous world. Within the Department of Defense (DoD), the importance of this network is well-recognized, and considerable efforts are ongoing to further integrate nations across it. Nevertheless, significant challenges persist, and numerous laws, policies, and processes inhibit our ability to embrace our allies and partners in the ways that this strategic moment demands.

Today, the United States needs its allies and partners more than ever. Our competitors – namely, China – are making unprecedented investments across numerous technological areas, and increasingly threatening stability in key regions.[1] One study in 2023 has assessed that "China's global lead extends to 37 out of 44 technologies … spanning defense, space, robotics, energy, the environment, biotechnology, artificial intelligence (AI), advanced materials and key quantum technology areas."[2] Another recent report underscores that "China's defense industrial base is operating on a wartime footing … and acquiring high-end weapons systems and equipment five to six times faster than the United States."[3] Likewise, amid initial battlefield and economic setbacks after its full-scale invasion of Ukraine, Russia has maneuvered around international sanctions and continued investing in its defense industrial base.[4] The problem is clear: in order to maintain defense technology and manufacturing primacy, the United States cannot afford to go it alone.

Failure to fully integrate and collaborate with allies and partners will inhibit our ability to innovate, deter threats, and win conflicts. The DoD needs senior leadership to aggressively promote the values emphasized in our guiding strategic documents; demand integration as a fundamental tenet of national security; mitigate and eliminate key blockers to collaboration; and push for necessary cultural changes across the Department.

The Defense Innovation Board (DIB) launched this study to identify specific and actionable steps that the DoD can take to achieve these goals. In the past six months, the DIB met with over 150 experts across the DoD ecosystem, U.S. federal interagency, academia, industry, and allied and partner nation networks. These included strategic leaders, actions officers, servicemembers, industry leaders, embassy representatives, and leaders from allied and partner nations across echelons.

This report is a reflection of that work in mapping the current state of allied and partner nation innovation collaboration and providing specific recommendations that will make meaningful and foundational changes to the systems that underpin these networks.

Current State

Recent U.S. innovation alliance-building efforts have resulted in the growth of a "latticework" of "mini-lateral" coalitions framed around various security, economic, and technological challenges, such as the United States-

[1] The DoD's 2023 *China Military Power Report* highlights the continued rapid growth of the People's Liberation Army (PLA).
[2] Australian Strategic Policy Institute. (2023). APSI's Critical Technology Tracker. Retrieved June 25, 2024, from https://www.aspi.org.au/report/critical-technology-tracker.
[3] Jones, S. G., & Palmer, A. (2024, March 6). China Outpacing U.S. Defense Industrial Base. CSIS. https://www.csis.org/analysis/china-outpacing-us-defense-industrial-base
[4] Snegovaya, M., Bergmann, M., Dolbaia, T., Fenton, N., & Bendett, S. (2024, April 22). Back in Stock? The State of Russia's Defense Industry after Two Years of the War. CSIS. https://www.csis.org/analysis/back-stock-state-russias-defense-industry-after-two-years-war

European Union Trade and Technology Council (USEUTTC), the Indo-Pacific Economic Framework for Prosperity (IPEF), the Quadrilateral Security Dialogue (Quad), and the Australia-United Kingdom-United States Security Partnership (AUKUS). These initiatives have been paired with landmark domestic industrial legislation, such as the 2022 *CHIPS and Science Act*, and a series of comprehensive bilateral "initiatives on Critical and Emerging Technology (iCETs)" with the Republic of Korea (ROK), India, Singapore, and Israel.[5]

With its substantial resources, the DoD necessarily plays an important role in laying the groundwork for this multilayered system of technology partnerships and has continued to leverage a series of well-shorn tools to support this new terrain in innovation cooperation with allies and partners. These tools include:

- **General Security of Military Information Agreement (GSOMIA) –** GSOMIA allow sharing of classified information with third countries as well as acquisition of high-end U.S. military equipment through Foreign Military Sales (FMS) and Excess Defense Articles (EDA).
- **Acquisition and Cross Servicing Agreement (ACSA) –** ACSA, sometimes referred to as Logistics Support Agreements (LSA), Mutual Support Agreements (MSA), or Mutual Logistics Support Agreements (MLSA), along with Acquisition Only Agreements (AOA) are how the DoD acquires or provides logistic support, supplies, and services to eligible countries and international organizations. They provide access to designated facilities for refueling and replenishment.
- **Reciprocal Defense Procurement Memorandum of Understanding (RDP MoU) –** RDP MoU agreements promote rationalization, standardization, and interoperability of conventional defense equipment with allies and other friendly governments and provide a framework for ongoing communication regarding market access and procurement matters that enhance effective defense cooperation.
- **Communication Interoperability and Security Memorandum of Agreement (CISMOA) –** CISMOA or similar bilateral information security agreements (e.g., COMSEC MoUs, INFOSEC Equipment Agreements, or Communications Compatibility and Security Agreements) provide use of high-end communication equipment on military platforms for communications interoperability. They are vital frameworks for facilitating secure communication and sharing of classified information with allies and partners.
- **Basic Exchange and Cooperative Agreement (BECA) –** BECA are additional mechanisms for sharing high-end equipment and geospatial information on maps and satellites.

Moreover, in accordance with its 2020 *International Science and Technology Engagement Strategy*, the DoD prioritizes technical exchanges for identifying synergies in critical technology areas, and further deep dives and technical workshops to outline potential collaborative efforts.[6] According to interviews, current DoD international technology engagement covers approximately 244 negotiated project agreements with 16 countries. OSD leads significant bilateral engagements with the United Kingdom, Canada, Australia, France, Italy, the Netherlands, Norway, Japan, ROK, Singapore, India, and Israel, and has evolving bilateral relations with at least 17 additional NATO, major non-NATO, and strategic partners.[7]

[5] Gramer, R. (2024, April 11). Biden's "Coalitions of the Willing" Foreign-policy Doctrine. Foreign Policy. https://foreignpolicy.com/2024/04/11/biden-minilateralism-foreign-policy-doctrine-japan-philippines-aukus-quad/

[6] Under Secretary of Defense for Research and Engineering (2020). Retrieved June 25, 2024, from https://www.cto.mil/wp-content/uploads/2020/12/Signed-International-ST-Engagement-Strategy.pdf

[7] DIB interview with DoD stakeholder (2024, February 28)

Foreign military sales (FMS) transferring U.S. defense articles and services to allies and partners, the linchpin of many DoD security cooperation programs, have reached record highs amid a huge increase in demand since the war in Ukraine.[8] European countries, such as Sweden, Poland, and the Netherlands, have evolved into huge customers of U.S. military hardware. In FY2023, the United States inked a record $80.9 billion in FMS, including grant assistance.[9] Approximately $18 billion was used for the Ukraine Security Assistance Initiative and for Building Partner Capacity programs conducted by the DoD and other programs under the Foreign Assistance Act.[10] Israel, too, has been a leading recipient of security assistance. Before October 7, 2023, the United States annually provided Israel with $3.3 billion in grant- or loan-based financing and $500 million for cooperative programs for missile defense.[11]

Source: Who is an ally, and why does it matter?, Defense Priorities (2022, October 12)

Note: According to the Department of State, the United States is committed to defending more than 1.4 billion people in at least 51 countries (highlighted red) across the Americas, Europe, and Indo-Pacific. These countries include 32 NATO and 19 major non-NATO countries (recent NATO additions Sweden and Finland not highlighted). President Biden recently pledged to designate Kenya (also not highlighted) as a major non-NATO ally. The United States has defense relationships of varying scope and formality with at least 25 other partner nations.

---

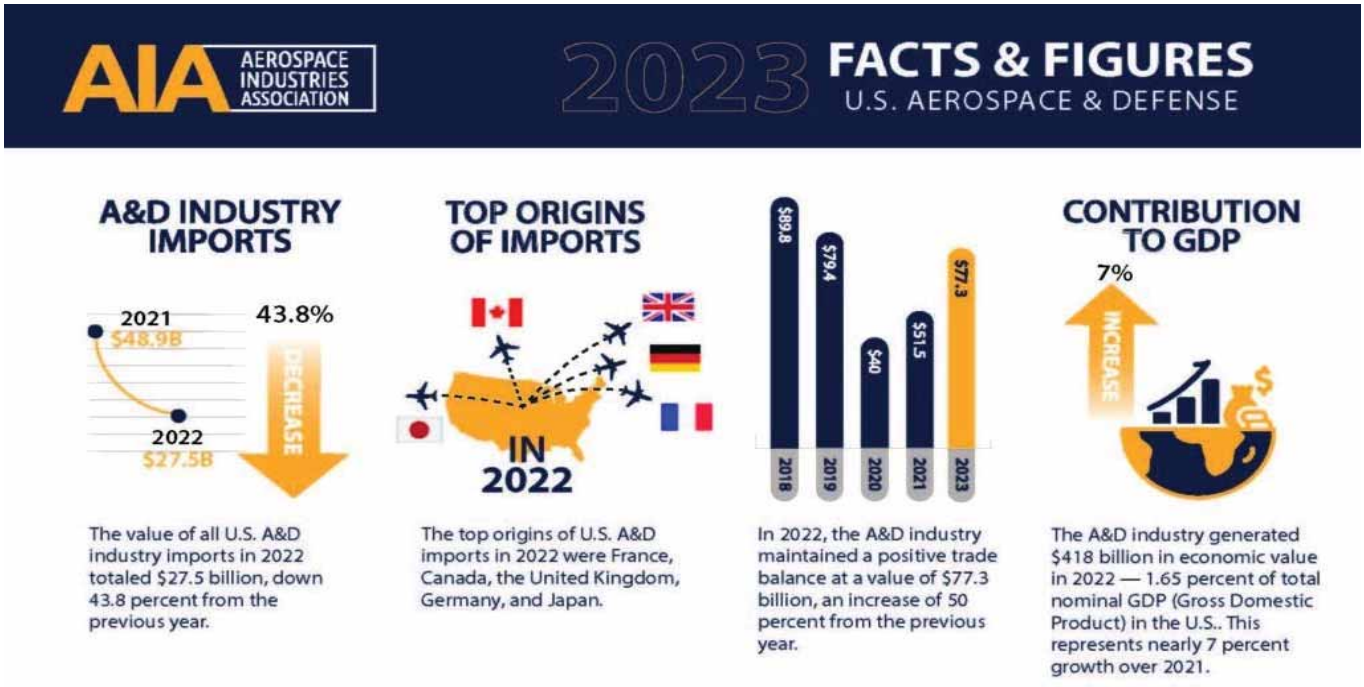
[8] Tirpak, J. (2024, January 29). Foreign Military Sales sets new record, up 55.9 percent in 2023. Air & Space Forces Magazine. https://www.airandspaceforces.com/foreign-military-sales-new-record-2023/
[9] Ibid.
[10] Arabia, C. L., Bowen, A. S., & Welt, C. (2024, May 22). U.S. Security Assistance to Ukraine. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12040
[11] Bureau of Political and Military Affairs. U.S. Security Cooperation with Israel. U.S. Department of State. Retrieved July 3, 2024, from https://www.state.gov/u-s-security-cooperation-with-israel/

Exhibit 1. International Traffic in Arms Regulations (ITAR)

The International Traffic in Arms Regulations (ITAR) is a key tool for regulating the proliferation of advanced U.S. military technology to potential adversaries and for adjudicating FMS agreements with allies and partners. However, ITAR, along with other U.S. export licensure regimes for dual-use technologies, such as the Export Administration Regulations (EAR), are hampered by a slow and cumbersome review process involving too many undifferentiated steps. While limiting access to sensitive technologies is essential, the current execution of ITAR impedes U.S. military readiness and stockpiling efforts.

ITAR remains crucial for national security despite these challenges, but finding the right balance between control and efficiency is necessary. Inherent to current ITAR processes is a Cold War-era risk aversion to sharing technology with allies and partners. In previous decades, when the United States maintained a significant technological advantage over the rest of the world, this stance was more reasonable. However, with advanced technologies proliferating and U.S. companies partnering with foreign suppliers to maintain competitiveness, modern realities make this risk aversion dangerous to the United States as well as to allies and partners. We are failing to get our friends around the world the technologies they need, and to grant our warfighters access to the best technologies from allies and partners. Foreign companies maintain a desire to stay 'ITAR-free', leading to missed opportunities for pulling advanced capabilities from even our closest friends. As a result, cutting-edge technologies are kept far away from the defense marketplace out of sheer fear of 'ITAR taint', and the system is failing to achieve its stated purpose to enhance "U.S. national security and foreign policy objectives."

There has been significant effort put toward improving ITAR for allies and partners. In 2010, Congress approved defense trade cooperation treaties with the United Kingdom and Australia allowing exemptions to ITAR for certain defense articles and services and covered persons from



Source: 2023 Facts & Figures, Aerospace Industries Association (2023, September 13)

those countries.[12] However, implementation of the treaties was poorly conceived and did not result in significant changes to the way exports to those countries were managed. In 2013, the Obama administration and Congress collaborated to reform ITAR focusing on tighter restrictions around fewer items and applying EAR's more flexible regime to a greater number of less sensitive items. The comprehensive reform effort had some success, rebuilding the ITAR U.S. Munitions List (USML), shifting various items from ITAR to EAR, recalibrating and harmonizing definitions and regulations, updating licensing procedures, establishing a consolidated licensing database, and creating an Export Enforcement Coordination Center within the Department of Homeland Security.[13]

Within the DoD, recent developments to improve the FMS program have focused on the use of these agreements to strengthen strategic partnerships, particularly with NATO and Indo-Pacific allies, while continuing to provide support for global counterterrorism and counterinsurgency operations. Increasingly, FMS agreements include advanced capabilities, such as cyber defense, space systems, and unmanned aerial systems, reflecting the growing influence of emerging technologies on warfare. In terms of streamlining processes, the Defense Security Cooperation Agency (DSCA), which oversees the FMS program, is transitioning to a continuous process improvement posture as it implements its 16th reform effort in just the last 20 years.[14] These lessons are instantiated in the most recent comprehensive DoD FMS Tiger Team assessment launched in August 2022 and completed in June 2023.[15]

Following the FMS Tiger Team recommendations, DSCA, with oversight from OSD Policy and Acquisition and Sustainment (A&S) components, is in the process of implementing a series of changes to improve the DoD's understanding of international military requirements, provide allies and partners with more relevant priority capabilities, incorporate these requirements into DoD plans to expand defense industrial base production capacity, and ensure broad government-wide support for FMS efforts. Notable reforms include the establishment of an FMS Continuous Process Improvement Board to provide an enduring governance structure to ongoing changes, a new Security Cooperation Execution Focus Forum to elevate important FMS case challenges for fast-tracked resolution, and enhanced business processes and metrics for every FMS process stage. DSCA is also establishing its own embassy-level Defense Security Cooperation Service intended to complement the Defense Attaché Service. To improve the FMS program's attention to relevant priority capabilities, the Tiger Team has also prompted formal discussions with allied and partner nations on U.S. grant-funded capability requirements, as well as prioritized deliveries of high-demand/low-supply munitions. In addition, the Tiger Team instructed relevant DoD components to improve the Department's ability to include Non-Program of Record (NPOR) acquisitions in the FMS program.[16]

[12] Amendment to the International Traffic in Arms Regulations: Removing Requirement for Prior Approval for Certain Proposals to Foreign Persons Relating to Significant Military Equipment (2010).
[13] Revisions to the Export Administration Regulations: Initial Implementation of Export Control Reform (2013).
[14] DIB interview with DoD stakeholder (2024, May 31)
[15] Lopez, C. T. (2023, June 13). Tiger team recommendations aim to optimize Foreign Military Sales. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3427294/tiger-team-recommendations-aim-to-optimize-foreign-military-sales/
[16] Ibid.

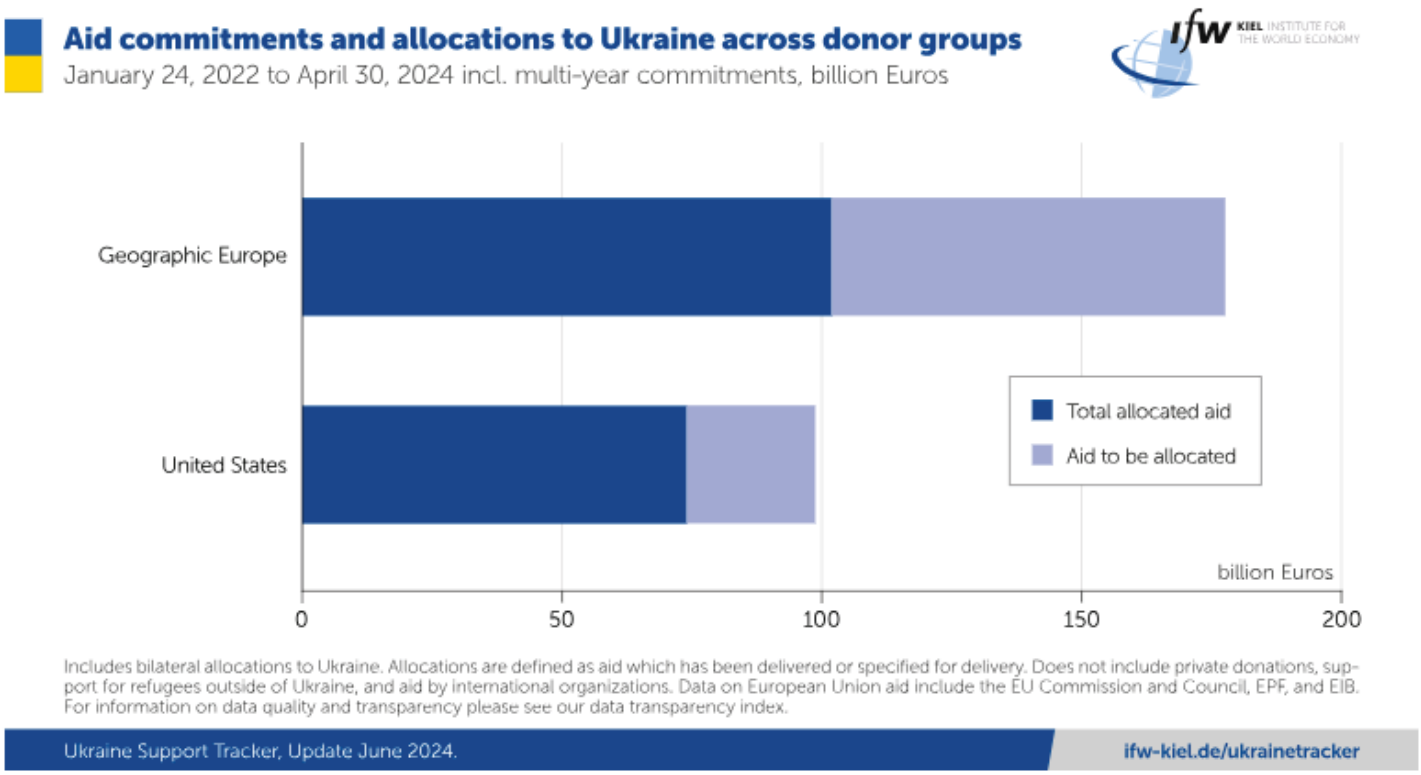
Direct commercial sales (DCS), the other method for U.S. arms exports to allies and partners, are sales made under a Department of State-issued license by U.S. industry directly to a foreign buyer and are not administered by the DoD through FMS procedures. In 2018, a revised State policy and implementation plan for conventional arms transfers (CAT) was introduced, easing restrictions on U.S. export of conventional arms and simplifying the direct commercial arms transfer process for allies and partners. Since the new policy, DCS arms transfers have soared. In FY2019, DCS transfers totaled $55.1 billion; by FY2020, they reached $124.3 billion. Further revisions to the CAT policy were unveiled in February 2023, demonstrating continued effort to reform how the United States administers arms exports, and in FY2023, DCS transfers stood at $157.5 billion.[17]

Given this record demand for defense articles, and the challenges with defense manufacturing this has exposed, co-development, co-production, and co-sustainment of defense systems are increasingly important for offsetting gaps in allied defense industrial capacity. Poland offers an important and relevant example of this growing appetite for co-production, with the DoD fronting $60 million of a $2 billion direct loan agreement to support Poland's defense modernization. U.S. and Polish companies are working to surge munitions production capacity closer to Ukraine by manufacturing Javelin anti-tank missiles, Stinger anti-aircraft weapons, and other critical depleted systems.[18] FMS programs often include co-production and co-sustainment elements as part of government-to-government agreements. DCS agreements, on the other hand, are generally not as effective at building allied industrial capabilities, although they do strengthen the U.S. industrial base by extending production lines for aging systems being phased out of the U.S. inventory.

Source: Ukrainian Defence Ministry Press Service

[17] Bureau of Political Military Affairs. (2024, January 29). Fiscal Year 2023 U.S. Arms Transfers and Defense Trade. U.S. Department of State. https://www.state.gov/fiscal-year-2023-u-s-arms-transfers-and-defense-trade/

[18] Office of the Spokesperson. (2023, September 25). New U.S.-Poland Foreign Military Financing Direct Loan Agreement Showcases Strong Security Partnership. U.S. Department of State. https://www.state.gov/new-u-s-poland-foreign-military-financing-direct-loan-agreement-showcases-strong-security-partnership/



Source: Ukraine Support Tracker, Kiel Institute (2024, June 6)

Note: Both the United States and European partners have committed more aid to Ukraine than has actually been allocated. Total U.S. commitments stand at 98.7 billion euros ($175 billion), with 24.7 billion euros ($43.8 billion) remaining to be allocated. For Europe, commitments have also increased to 177.9 billion euros, but the gap with allocations is higher, with 75.8 billion euros still unallocated. This underscores the critical need to fast-track capability and other aid to the Ukrainians.

Exhibit 2. Ukraine Defense Contact Group (UDCG)

The Ukraine Defense Contact Group (UDCG, also known as the Ramstein Group) stood up in April 2022 currently comprises all 32 NATO members, with an additional 24 partners and the European Union.[19] The UDCG tracks Ukrainian capability gaps, oversees training programs for the Ukrainian Armed Forces, and coordinates long-term support for the war effort. The national armaments directors of over 40 UDCG members meet regularly to coordinate efforts on industrial base and sustainment challenges facing Ukraine.[20] In addition, the UDCG houses a multitude of capability coalitions, for example, focused on artillery, de-mining, and information technology, and has been the starting point for a number of collaborative efforts stemming from this conflict. In conjunction with key Pentagon efforts, such as the Joint Production Accelerator Cell and Joint Rapid Acquisition Cell, the UDCG plays a critical function in the rapid transfer of capabilities to the Ukrainian Armed Forces.

[19] Special Online Briefing with Ambassador Julianne Smith, U.S. Permanent Representative to NATO. U.S. Department of State. (2023b, February 13). https://www.state.gov/special-online-briefing-with-ambassador-julianne-smith-u-s-permanent-representative-to-nato/
[20] Howard, M. (2024, April 25). National Armaments Directors Maintain Urgency in Support for Ukraine. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3756624/national-armaments-directors-maintain-urgency-in-support-for-ukraine/

In conjunction with these government-driven efforts, the private sector has deployed a vast array of technologies and services to Ukraine. Palantir, Google, Microsoft, Amazon, Starlink, and countless other tech companies are deeply involved in the war effort.[21] Be it facial recognition for identifying participants in war crimes, managing refugee resettlement, or military planning, commercial industry is demonstrating its value across the spectrum of conflict. Ukraine has worked to manage this massive influx of assistance, and better integrate cutting-edge systems from the private sector.[22] Ukrainians have risen to the occasion with aplomb and modeled an innovation ecosystem with the speed and urgency that the DoD aspires to.

Exhibit 3. Ukrainian Defense Innovation

- **Brave1**: A Ukrainian government-supported platform to aggregate ideas and ensure that a range of interested parties can participate in the Ukraine defense innovation community, including defense technology companies and private citizens.
- **Innovations Development Fund**: Also known as the Ukrainian Startup Fund (USF), the USF helps early-stage start-ups raise funds and launch projects. Broad in scope, it is focused on the defense technology sector and has supported key unmanned aerial vehicle projects.

Source: Sameer Al-Doumy/AFP via Getty Images

- **UNIT.City Innovation Park:** UNIT.City, Ukraine's first innovation park established in 2016, is an Eastern European research and development center for over 100 Ukrainian companies across advanced technology sectors covering agriculture, unmanned logistics, telecommunications, and energy efficiency, among others. It awards grants, provides consultations, and supports regular communications between local start-up industry and foreign investors and companies.
- **Rapid Capability Group:** Across Ukraine, industry and private citizens have contributed massively to the war effort. One such example, the Rapid Capability Group (RCG), aims to rapidly bring military capabilities from concept to deployment on the battlefield. It works to implement and share best practices in the space, leverages commercial and dual-use technologies, and draws on a network of national and international stakeholders to augment the military capabilities of the Ukrainian Armed Forces.

[21] Bergengruen, V. (2024, February 8). Tech Companies Turned Ukraine into an AI war lab. Time. https://time.com/6691662/ai-ukraine-war-palantir/

[22] Defense Innovation Unit. (2024, June 24). Battlefield Realities, Pace of Innovation at Center of NATO-Ukraine Defense Innovators Forum. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3815552/battlefield-realities-pace-of-innovation-at-center-of-nato-ukraine-defense-inno/

Meanwhile, in the Indo-Pacific, the United States continues to deepen innovation cooperation with key regional allies such as Australia, Japan, ROK, and the Philippines, while deploying new frameworks for pursuing cooperation in areas such as maritime domain awareness, cybersecurity, and countering sanctions evasion.[23] As Indo-Pacific allies and partners continue to invest in defense modernization, the United States is actively extending its regional deterrence capabilities through a variety of enhanced partnerships to strengthen interoperability in response to growing insecurity in the Taiwan Strait, China's unlawful maritime claims in the South China Sea, and provocations from North Korea. For example, it is collaborating with Japan and ROK on broad security, economic, and technology issues; pursuing integrated development with Australia and Japan of new technologies, such as autonomous systems and collaborative combat aircraft; and mobilizing capacity-building support for the Philippines with Japan.[24] It has also undertaken further bilateral cooperation with Australia, ROK, Japan, and the Philippines, signed new defense cooperation agreements with Indonesia and Papua New Guinea, and designated the Association of Southeast Asian Nations (ASEAN), Vietnam, and Indonesia as "comprehensive strategic partners".[25] In addition, it is improving collaboration with other countries in the region, such as Thailand, Malaysia, and Cambodia.

Exhibit 4. AUKUS Trilateral Partnership

Established in September 2021, AUKUS may be the most promising institutional framework in terms of growing multilateral defense technology cooperation in the Indo-Pacific. AUKUS has helped expose the limits of U.S. shipbuilding capacity, prompting billions in new investment into expanding the U.S. submarine industrial base.[26] While AUKUS is centrally focused around delivering nuclear-powered attack submarines to Australia, Pillar II of the partnership, focused on developing advanced military capabilities between the three countries, holds perhaps greater long-term potential for enhancing combined defense innovation among partner nations in the region. Currently, the scope of Pillar II is broad, covering eight areas: cyber capabilities, AI and autonomy, quantum technology, undersea capabilities, hypersonics and counter-hypersonics, electronic warfare, innovation, and information-sharing.[27] Still, AUKUS Pillar II holds the ability to focus collective resources around the problem of China's tech rise if the political rhetoric behind it can be turned into practical deliverables that leverage the combined advantages of the Indo-Pacific allied community.

Source: U.S. Navy

[23] A work in progress: The Indo-Pacific Partnership for Maritime Domain Awareness. Pacific Forum. (2023, June 23). https://pacforum.org/publications/pacnet-48-a-work-in-progress-the-indo-pacific-partnership-for-maritime-domain-awareness/

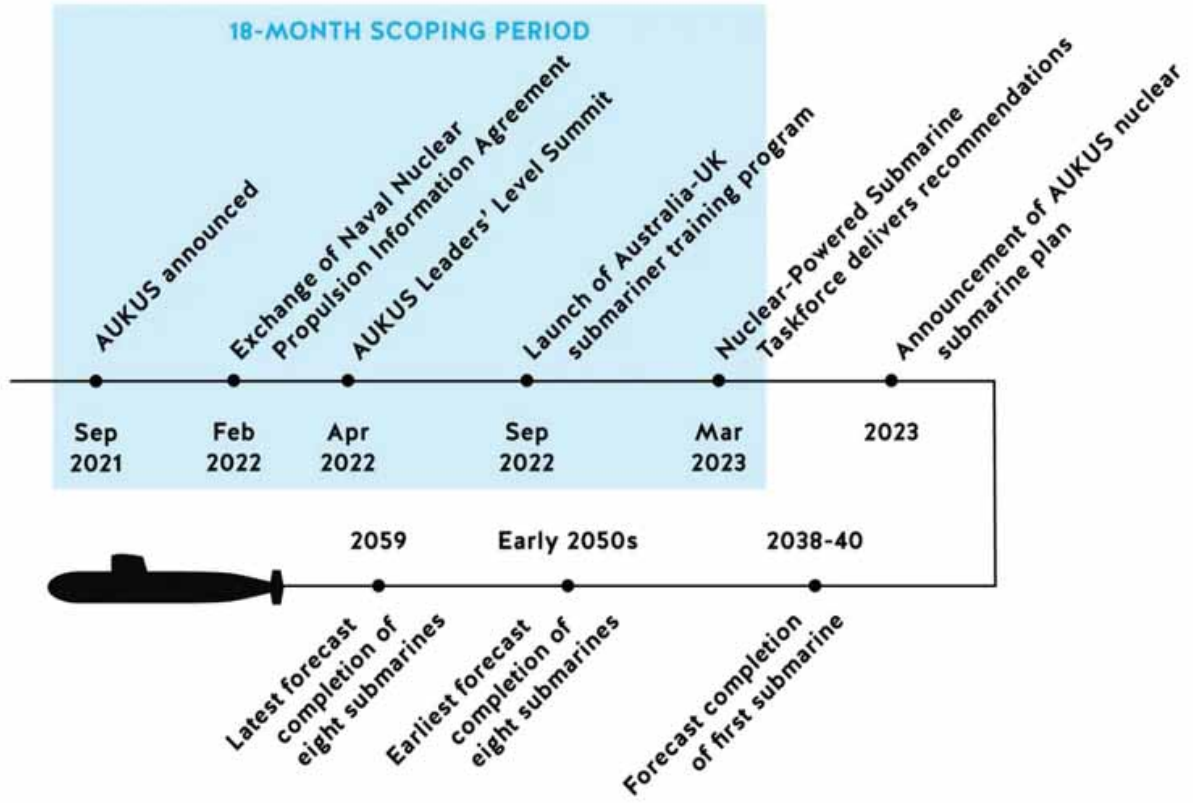
[24] United States-Japan-Republic of Korea Trilateral Ministerial Meeting (TMM). U.S. Department of Defense. (2024, June 2). https://www.defense.gov/News/Releases/Release/Article/3793913/united-states-japan-republic-of-korea-trilateral-ministerial-meeting-tmm-joint/

[25] Fact Sheet: U.S.-ASEAN Comprehensive Strategic Partnership, One Year On. The White House. (2023, September 6). https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/05/fact-sheet-u-s-asean-comprehensive-strategic-partnership-one-year-on/

[26] Joint Leaders Statement on AUKUS. The White House. (2021, September 15). https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/

[27] Christianson, J., Monaghan, S., & Cooke, D. (2023, July 10). AUKUS Pillar Two: Advancing the Capabilities of the United States, United Kingdom, and Australia. CSIS. https://www.csis.org/analysis/aukus-pillar-two-advancing-capabilities-united-states-united-kingdom-and-australia

Together, these efforts point to an essential finding: allies and partners across Europe and the Indo-Pacific are increasingly demonstrating both the will and the means to unravel years of underinvestment in defense industrial capacity. Countries are even expanding their collaboration without direct U.S. involvement. For example, the United Kingdom, Japan, and Italy are collaborating on a jointly developed advanced stealth fighter.[28] Japan and Finland are engaged in co-production of armored vehicles.[29] With Japan, Australia is developing advanced drones, other autonomous systems, and integrated radar and sensors.[30] Similarly, with ROK, Canberra is pursuing enhanced defense industry cooperation.[31] Australia is also deepening collaboration with the ASEAN community, as well as expanding co-production efforts with Germany and France.[32] [33] Furthermore, when left out of prominent U.S.-led partnerships, countries are seeking ways to integrate themselves regardless, whether as regular observers, occasional participants, or future members. Germany and Japan continue to seek membership in the Five Eyes. ROK and Singapore have eyed collaboration with the Quad. To date, Japan, ROK, Canada, and New Zealand have also expressed hopes of joining AUKUS someday. Others continue to propose various configurations of states engaged on industrial development. It is incumbent upon the DoD to utilize this collective energy to realign the innovation ecosystem for sustained allied and partner nation collaboration.



Source: United States Studies Centre (USCC)

Note: Modeled AUKUS production timelines highlight the need for accelerated industrial cooperation.

[28] Yamaguchi, M. (2023, December 14). Japan, UK and Italy Formally Establish a Joint Body to Develop a New Advanced Fighter Jet. AP News. https://apnews.com/article/japan-uk-italy-fighter-jet-signing-military-52b2f50ba62e0b6580c3fbc78108fd66

[29] Arata, S. (2024, May 8). Japan Steel Works lands first defense deal for armored vehicles. Nikkei Asia. https://asia.nikkei.com/Business/Aerospace-Defense-Industries/Japan-Steel-Works-lands-first-defense-deal-for-armored-vehicles

[30] Yamaguchi, M. (2023, October 19). Japan and Australia Agree to Further Step-up Defense Cooperation Under 2-month-old Security Pact. AP News. https://apnews.com/article/japan-australia-defense-china-talks-kihara-fd4f2fa3b84db43553720f288bbbcbf1

[31] Sixth ROK-Australia Foreign and Defense Ministers' (2+2) Meeting. Republic of Korea Ministry of Foreign Affairs. (2024, May 7). https://www.mofa.go.kr/eng/brd/m_5674/view.do?seq=320998

[32] ASEAN, Australia Reaffirm Commitment to Advance Comprehensive Strategic Partnership. ASEAN. (2024, May 13). https://asean.org/asean-australia-reaffirm-commitment-to-advance-comprehensive-strategic-partnership/

[33] Clark, C. Australia racks up biggest arms export deal: $1B AUD for Boxers to Germany. Breaking Defense. (2024, March 21). https://breakingdefense.com/2024/03/australia-racks-up-biggest-arms-export-deal-1b-aud-for-boxers-to-germany/

Key Barriers and Risks

Despite various efforts, initiatives, and programs to improve collaboration with allies and partners, the DoD is failing to fully integrate these nations across its innovation, operational, and strategic ecosystems. The Pentagon must prioritize integrating collaborators in new ways that mirror today's more interconnected world. At present, however, we are leaving investment and production on the table. Key allies and partners are kept at bay and lack formal pathways toward integration with U.S. capabilities. Foreign technology companies are frequently rebuffed due to U.S. export controls and compliance costs. Essential technological advances are going unnoticed as they occur outside of the United States, and DoD efforts to identify mature foreign-developed technologies across allies and partners, such as the Foreign Comparative Testing (FCT) program, remain fragmented, overwhelmed, and underfunded. Finally, Buy American laws are overly restrictive for ensuring speedy and efficient delivery of capabilities to warfighters, key reciprocal defense trade agreements are poorly understood and utilized, and private markets are increasingly being inundated with hostile capital. Undersecretary of Defense for Acquisition and Sustainment Dr. William LaPlante has stated that U.S. defense industrial capacity is "dialed down to the minimum amount ... [with] very few development programs, [a] minimal amount, and then very few production programs."[34] While the latent potential for co-innovation is immense, the DoD faces a number of key barriers and risks to optimizing cooperation with allies and partners:

- **Cultural Barriers –** Collaboration with allies and partners is difficult in the best of scenarios. Once outside of the traditional Anglosphere, namely the Five Eyes, this difficulty is greatly magnified. Language and cultural differences heighten barriers to entry, and the DoD has failed to address these struggles. Key allies and partners (e.g., Japan and ROK) demonstrate both the capacity and willingness to engage more fulsomely, but have lacked clear pathways for pursuing these desires. Even within traditional frameworks, a growing appetite for engagement has not been met with commensurate effort from the DoD.
- **Foreign Industry Engagement –** Like their government counterparts, allied and partner nation industries have also struggled to engage the U.S. defense sector. A common complaint during discussions was the lack of options for foreign companies seeking further inroads to open U.S.-based factories and local subsidiaries, and the lack of mechanisms and resources for navigating U.S. export control systems and filling gaps in the U.S. defense industrial base. Absent this support, these would-be partners struggle to identify who to engage across the U.S. government, much less develop the trust, relationships, and expertise necessary to succeed in the defense sector. The inability to articulate to foreign industry a clear pathway for working with the DoD is leaving supply chains less robust and failing to return critical production to the United States.
- **Return on Investment –** The defense sector, while substantial, is ultimately a small component of global commerce and exchange. As such, insufficient return on investment is a common impediment to private industry developing facilities for subscale production. Economies of scale, particularly for foreign companies that lack local or regional buyers large enough to sustain a business, are simply inadequate to attract necessary investment. Properly integrating allies and partners, and their

[34] Strengthening the U.S. Industrial Base with Hon. Dr. William A. LaPlante. CSIS. (2023, September 26). https://www.csis.org/analysis/strengthening-us-industrial-base-hon-dr-william-laplante

accompanying defense and dual-use technology markets, would make the defense and dual-use sectors significantly more attractive to global vendors.

- **Supply Chain Resilience –** Supply chain risks are not unique to the DoD, but they become urgent when national security is at stake. Aging weapon systems rely on a finite number of repair parts suppliers, some of which are financially precarious. The U.S. defense industry depends on certain materials, such as antimony, lithium, and rare-earth minerals. In particular, it is heavily reliant on China, and to a lesser extent Russia, for procuring antimony vital for producing ammunition, armor-piercing bullets, explosives, and other military equipment. China additionally commands a near-monopoly over advanced battery supply chains covering lithium hydroxide, electrolyte, lithium carbonate, anodes, and cathodes. Currently, the defense industry faces constraints in producing critical components, such as solid rocket motors, processor assemblies, castings, forgings, ball bearings, microelectronics, and seekers for munitions. These shortages hinder production capabilities. Sub-tier suppliers, often operating on narrow profit margins, are especially susceptible to cyclical defense demands and budget changes, and will struggle to remain in the defense marketplace. The DoD needs to create new conditions to diversify its defense industrial supplier base and invest in new production methods. This includes working with allied and partner nation suppliers.

- **Export Controls –** As the FMS program continues to grow exponentially, allied and partner nation governments and industry have grown increasingly frustrated by Cold War-era processes for information and technology sharing. Successive failures to reform FMS processes have kept critical technologies out of the hands of our allies and partners when they need it most. In its 2023 review of the FMS process, the Department of State emphasized that 95 percent of FMS cases were evaluated and approved within 48 hours. Despite this, throughout DIB conversations, changes to ITAR, and export controls more broadly, remained a chief topic of interest. Failure to coordinate the U.S. federal interagency process, inadequate resourcing of responsible offices, and a fundamentally flawed mindset to sharing will continue to hinder collaborative work. Even within AUKUS, a small and relatively focused effort among longstanding allies, the current ITAR regime may completely derail any actual co-innovation.

- **Information Sharing –** Information sharing is of the utmost importance from the earliest stages of research, development, testing and evaluation, to the management of complex military operations. Despite this, the DoD (and the federal government writ large) has fundamentally failed to develop a system which intelligently manages risk while ensuring allies and partners receive the information they need to properly prepare for and participate in coalition operations. We continue to overclassify information, defaulting to “no foreign dissemination (NOFORN)” protocols, and even fail to develop suitable processes for communicating “controlled unclassified information (CUI)” in today’s shared threat environment. Much ink has been spilled on this topic, but the issue persists and must be addressed.

- **Fundamental Risk Assessment –** Finally, central to every issue for allies and partners is a fundamental misunderstanding of the primary risk facing the United States today. The risk we face is not that we lose control of a technology, that a foreign counterpart receives an email with an attachment they technically should not see, or that we forget to mark a document “NOFORN”. The risk is that by failing to properly integrate our allies and partners, on day-one of a conflict we have failed to integrate and align with the nations that underpin our military strength. The risk, then, is that we are forced to learn

costly lessons during a conflict that should have been avoided. The risk is that we lose a war. Until the DoD fundamentally rethinks its approach to risk, its efforts to spur meaningful co-innovation with allies and partners will remain wanting in an era defined by openness and interdependence.

Recommendations

Over the course of this study, major allies and partners approached the DIB with surprisingly uninformed questions regarding the state of DoD defense innovation and industrial base engagement.[35] [36] Today, the DoD does not have a central standing mechanism for interfacing with allies, partners, and international organizations, resulting in a state of considerable fragmentation, duplication, and lack of coordination across workstreams. Moreover, we observed that DoD senior leaders are stretched thin by the many duties pressed upon them, and that international defense industrial cooperation is often relegated in the face of competing priorities. The Department's principals responsible for international cooperation accordingly struggle to devote an adequate level of attention, care, and focus to addressing the barriers and risks facing the international industrial base.

As a result, we heard confusion from allies and partners regarding who to engage within the Pentagon bureaucracy to understand its decision-making structures.[37] The congressionally mandated reorganization in February 2018 of the Undersecretary of Defense for Acquisition, Technology and Logistics (AT&L) into undersecretary-level positions focused on Acquisition and Sustainment (A&S) and Research and Engineering (R&E) exacerbated this uncertainty, leading to considerable appetite for some formulation of a 'one-stop-shop' or 'designated lead' for these issues.[38] Industry experts pointed to examples set by countries like the United Kingdom, Australia, Singapore, Estonia, and other allies and partners that tend to be more effective at identifying, attracting, and integrating foreign capabilities into their respective industrial bases.[39]

A) Leadership

Given the global, multi-theater challenges facing the U.S. defense industrial base, *the DoD must prioritize international defense industrial cooperation and elevate that portfolio to the level of continuous, seamless, and thoughtful attention and execution that it now deserves.* The 2018 USD(AT&L) split into the USD(A&S) and USD(R&E) left the international defense industrial cooperation portfolio disjointed, without an empowered authority to singlehandedly engage international industrial base partners as the Secretary and Deputy Secretary of Defense's principal advisor on all industrial base issues. With this new environment created by the split, a new construct that reconsolidates international defense industrial cooperation under a single USD is needed. Such an executive should be able to delegate responsibility for and oversee the full spectrum of international defense industrial cooperation responsibilities across OSD, the Military Departments, Combatant Commands, and instrumental fourth-estate defense agencies such as DSCA, the Defense Technology Security Administration (DTSA), and Defense Advanced Research Projects Agency (DARPA). Accordingly, the DIB recommends the following enhancements to existing DoD leadership:

1. Establish a new Undersecretary of Defense for International Industrial Cooperation, or USD(IIC). This position would designate a senior political executive as the primary point of contact at the DoD and the principal staff assistant to the Secretary and Deputy Secretary for all matters pertaining to international defense industrial cooperation. The USD(IIC) would address the common complaint among allies and partners that the DoD and federal interagency lack the

[35] DIB interview with ally/partner stakeholder (2024, April 10)
[36] DIB interview with ally/partner stakeholder (2024, April 12)
[37] DIB engagement with ally/partner stakeholders (2024, May 10)
[38] DIB engagement with ally/partner stakeholders (2024, May 10)
[39] DIB interview with industry stakeholder (2024, April 17)

necessary capacity, transparency, and harmonization for effective international industrial base cooperation.

2. Under the new USD(IIC), there should be two Assistant Secretaries of Defense for Combined Requirements Development (CRD) and International Integration and Interoperability (II&I). The ASD(CRD) would be responsible for enhancing collaboration with allies and partners during the initial stages of requirements development. This function would create improved pathfinders for bringing allies and partners into the requirements development process, identify requirements and shared investments across the partner community, and oversee initial investments to progress projects from concept to production at scale. The ASD(II&I), meanwhile, would be responsible for managing classification guidelines for allies and partners, harmonizing technical standards, capabilities, and policies, and ensuring interoperability of communications protocols and networks.
3. The USD(IIC) would work closely with OSD Policy and Comptroller to align international defense industrial cooperation goals to the force development priorities of the Secretary as defined in the annual Defense Planning Guidance (DPG) and Planning, Programming, Budgeting, and Execution (PPBE) processes.
4. The USD(IIC) would incorporate and elevate the international defense industrial base portfolio of OSD A&S, presently overseen by a Deputy Assistant Secretary of Defense for Industrial Base Development and International Engagement. The USD(A&S) will retain its oversight of all domestic defense industrial base policy as the U.S. National Armaments Director – and attend all annual conferences of national armaments directors in that capacity – but otherwise relegate authority for international defense industrial cooperation to the USD(IIC). This will allow A&S to focus on its primary mission of maintaining U.S. defense industrial base resilience.
5. The USD(IIC) would adopt the international outreach and policy portfolio of OSD R&E, with primary oversight of implementation of the DoD's international science and technology (S&T) engagement efforts. While the USD(R&E) should remain closely involved in the DoD's international technology scanning efforts, given that role's function as the Department's Chief Technology Officer, actual implementation of taskings and deliverables regarding international S&T cooperation should be reassigned to the new USD(IIC). This would allow R&E to devote its full resources toward ensuring the continuous advancement of technology and innovation within the DoD enterprise.
6. Other OSD entities that engage on aspects of international defense industrial cooperation should be nested with the priorities dictated by the USD(IIC). For example, the Defense Innovation Unit (DIU) conducts international engagement with its counterpart DIUs in allied and partner nations, and the Chief Digital and AI Officer (CDAO) engages in international consultations on data and AI-related issues.

Given the 2018 AT&L split, the DIB believes this new USD(IIC) will be needed to conclusively mitigate supply chain vulnerabilities, address production limitations, and navigate the international industrial cooperation bureaucracy. The role is fit-for-purpose in the current geopolitical and leadership environment, and while erecting new bureaucratic scaffolding bears its own risks and challenges, centralizing all OSD directorates, divisions, and resources that focus on different aspects of international defense industrial cooperation is a necessary act. Properly integrated, the new USD would free OSD A&S, R&E, Policy, and other relevant components to prioritize their core missions.

In place of a new undersecretary, Congress may consider[40] reconsolidating the USD(A&S) and USD(R&E) into an Undersecretary for the Industrial Base focusing on innovation research and development, supply chains, production capacity, and access to technologies both domestically and *globally*. This alternative might be equally suitable, as it would address the disjointedness that characterizes current OSD structures while minimizing bureaucratic growth and responding to (a) known post-COVID supply chain vulnerabilities, (b) current production capacity limitations exposed by global contingency operations, and (c) the principal conclusion of our report that international cooperation is byzantine and absurd in its bureaucratic complexity.

B) International Cooperation Priorities

The DoD needs a more centralized process of collaborating with foreign partners at the project level, including a more strategic approach with standards and guidelines for how program managers identify and select collaborative technology development initiatives with allies and partners. Progress requires starting small, building viable proofs of concept, assuaging historical or cultural distrust issues, and making incremental adjustments throughout to entrenched government bureaucracy that interferes in cooperation. The DoD – and proposed USD(IIC) – should emphasize the following priorities as it aligns plans, resources, and doctrine for international defense industrial cooperation:

1. **Implement an "Integrated-by-Design" Policy –** The DoD must implement an "integrated-by-design" policy, bringing allies and partners into the capability design cycle early.[41] Integrating "qualifying countries" into the early stages of development and production phases would amplify the effectiveness of international security assistance and cooperation. This policy should not hinder or fully replace existing collaborative security efforts but rather create spaces to "make decisions together on interoperability, resource investment, information sharing, force development and strategy from the very beginning."[42] Part of this challenge requires acknowledging and addressing the broader cultural obstacles to allied and partner nation innovation cooperation created through existing incentive structures within the DoD that discourage risk-taking and collaboration essential to innovation. While these incentives are beyond the remit of this study, we underscore the need for a more strategic, proactive, and direct approach to international defense industrial cooperation that resources and rewards the ability to get things over the finish line at speed and scale. In the context of addressing barriers to cooperating with allies and partners, this requires chipping away at the entrenched bureaucratic mindset of "hide and protect" and embracing a "share and enable" approach that empowers allies and partners, particularly where they are hindered from close cooperation with the United States given disparities in the maturity of respective innovation ecosystems.
2. **Require Justifications for Non-Exportability –** The DoD should require program managers to provide justifications for lack of interoperability and exportability of systems with allies and partners. A recent bipartisan report by Congress on the DoD's FMS program recommended that exportability not be eliminated from contracts

[40] This is not a review nor a specific critique of the roles of the USD(A&S) and USD(R&E), but rather an acknowledgement that creating a new USD for the Industrial Base is additive to already stymying bureaucracy, and that consolidating to one is subtractive, especially given most of the A&S and R&E roles (formerly under AT&L) are delegated to the Services. In other words, our recommendation is 'have the Services manage and be accountable for programs, have OSD manage and be accountable for the industrial base'.

[41] Then-Air Force Chief of Staff General Charles Q. Brown Jr., currently the Chairman of the Joint Chiefs of Staff, described the need for an "integrated-by-design" approach to allies and partners in an August 2022 speech at the American Enterprise Institute. An (Air) Force to Be Reckoned With: Defense Strategy and Innovation with Gen. Charles Q. Brown Jr. American Enterprise Institute. (2022, August 29). https://www.aei.org/events/an-air-force-to-be-reckoned-with-defense-strategy-and-innovation-with-gen-charles-q-brown-jr/

[42] Ibid.

without review and certification.[43] The starting point for any new capability development project should emphasize interoperability and the importance of a collaborative design approach. The DoD's Defense Exportability Features (DEF) program, launched in 2011 as a pilot to develop and incorporate technology protection features in designated defense systems during research and development, is one example of an important, underutilized effort for ensuring that projects are designed to be interoperable from the outset.[44] Its goals to reduce costs, improve competitiveness, strengthen interoperability, and promote international cooperation provide a vital service for DoD program executive offices seeking to define and design exportable versions of their systems across initial development phases. Yet, the program is currently underfunded and, given its outsized impact, should be vastly expanded and properly resourced.[45] To augment this process, DSCA should conduct a comprehensive internal-classified review of legacy systems that the DoD is no longer producing and acquiring, and consider appropriate guidelines for allowing transfer of their production rights to allies and partners in greater need of those systems.

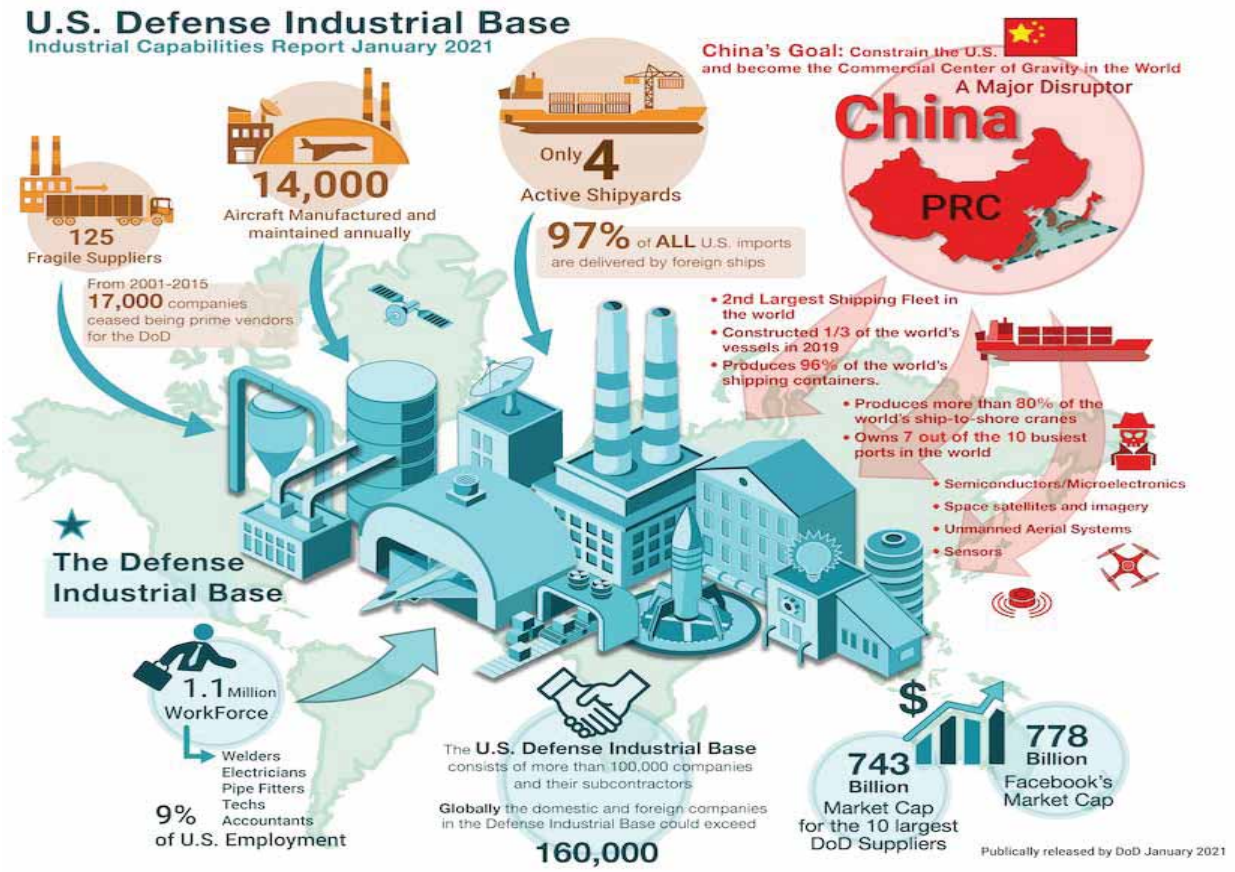
3. **Grow the Trusted-Nation Industrial Base –** In the absence of dedicated senior-level attention, the DoD has a tendency to big-brother essential partners such as Japan and ROK who are outside of the traditional Anglosphere of World War II-era allies.[46] While countries like these face limitations such as industrial security and sustainment challenges, they bear significant means and the will to apply those resources. These allies and partners should be engaged in good faith, and the DoD should endeavor to bring them into the fold more fulsomely. The National Technology and Industrial Base (NTIB) initially established in the FY1993 *National Defense Authorization Act* (NDAA) designates its members – which now include Canada, the United Kingdom, Australia, and New Zealand – as one national technology industrial base.[47] The NTIB's membership should be considered for expansion to countries beyond the Five Eyes.

4. **Mitigate 'Buy American' for Key Allies and Partners –** While underscoring the importance of leveraging allies and partners, the 2024 *National Defense Industrial Strategy* neglects to call out the potential of the DoD's RDP MoU agreements.[48] This omission reflects a systemic lack of awareness and understanding of the RDP MoUs, which establish agreed-upon procurement principles that foster transparency and openness to competition in each country's respective defense marketplace, including a waiver from Buy American rules when competing for DoD programs.[49] All DoD program managers should be trained on the RDP MoU and additional Buy American waivers and exemptions. In addition, the office that negotiates these waivers must be empowered to inform and educate the DoD contracting and acquisition workforce on the proper use of these existing authorities. Finally, other important allies and partners that do not currently have an RDP MoU with the DoD should be prioritized for negotiation and approval of this crucial agreement.

5. **Develop New Pathfinders for Capability Integration –** The NTIB is used as a pretext for government-to-government sharing of best practices, but it has not had much

[43] Foreign Military Sales Tiger Task Force: Report. Foreign Affairs Committee. (2024, February 7). https://foreignaffairs.house.gov/wp-content/uploads/2024/02/2.7.24-FMS-TIGER-Task-Force-Report.pdf
[44] Defense Exportability Features. Director - International Cooperation. https://www.acq.osd.mil/ic/def.html
[45] DIB engagement with internal DoD stakeholders (2024, March 29)
[46] DIB interview with national security expert (2024, March 19)
[47] Sanders, G., Hunter, A. P., McCormick, R., Mooney, S., & Herschlag, D. (2018, March 9). National Technology and Industrial Base Integration. CSIS. https://www.csis.org/analysis/national-technology-and-industrial-base-integration
[48] The National Defense Industrial Strategy (NDIS). OUSD A&S - Industrial Base Policy. (2023, November 16). https://www.businessdefense.gov/NDIS.html
[49] Assistant Secretary of Defense for Acquisition. ASD(A) - DPC - Contract Policy. (n.d.). https://www.acq.osd.mil/asda/dpc/cp/ic/reciprocal-procurement-mou.html

success in fostering actual international industrial base collaboration.[50] The NTIB's utility as a vehicle for industrial cooperation must be enhanced with new incentives for companies across industrial bases to partner with each other. Since the 2017 addition of Australia and the United Kingdom to the NTIB, efforts to implement the spirit of the law emulating a defense free-trade area, breaking down export control barriers, creating incentives for co-development of new capabilities, and establishing projects beyond the bare minimum, have been limited. The DoD should challenge an NTIB ally or partner with niche expertise applicable to a specific program to develop a capability better than what is being produced domestically as the program of record, and then purchase the system from that ally or partner through an RDP MoU if desired. This arrangement avoids the limitations of international agreement title codes and other cooperative technology agreements, including the need for higher-level political approvals. Alternately, the DoD could select a handful of key allies outside of the Anglosphere to co-develop a weapons system, prioritizing reciprocity from the very beginning meaning that development and production are pursued on a fully 50-50 basis. While such co-development and co-production can be painstaking at times, programs such as these are essential for enhancing defense technology cooperation with allies and partners. From our conversations, we have also seen the immense and growing appetite among countries for pursuing this sort of collaboration with the U.S. defense industrial base.[51] [52]



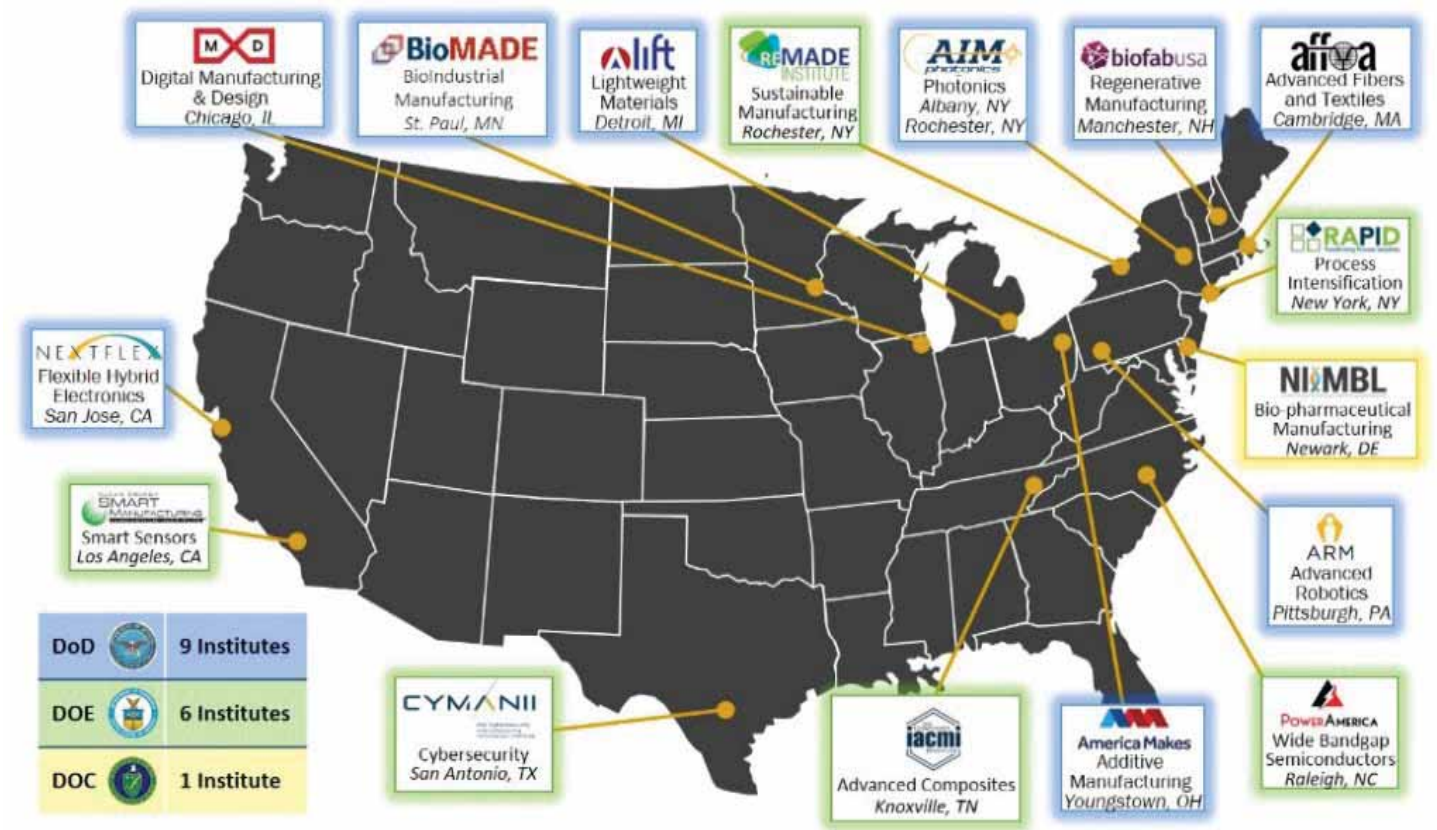
Source: DoD Annual Industrial Capabilities Report to Congress for FY2020

[50] Greenwalt, W. (2022, June 1). The NTIB is Dying: Is AUKUS Next? Congress Must Apply Life Support Soon. American Enterprise Institute. https://www.aei.org/op-eds/the-ntib-is-dying-is-aukus-next-congress-must-apply-life-support-soon/

[51] DIB interview with national security expert (2024, April 26)

[52] DIB engagement with ally/partner stakeholders (2024, April 12)

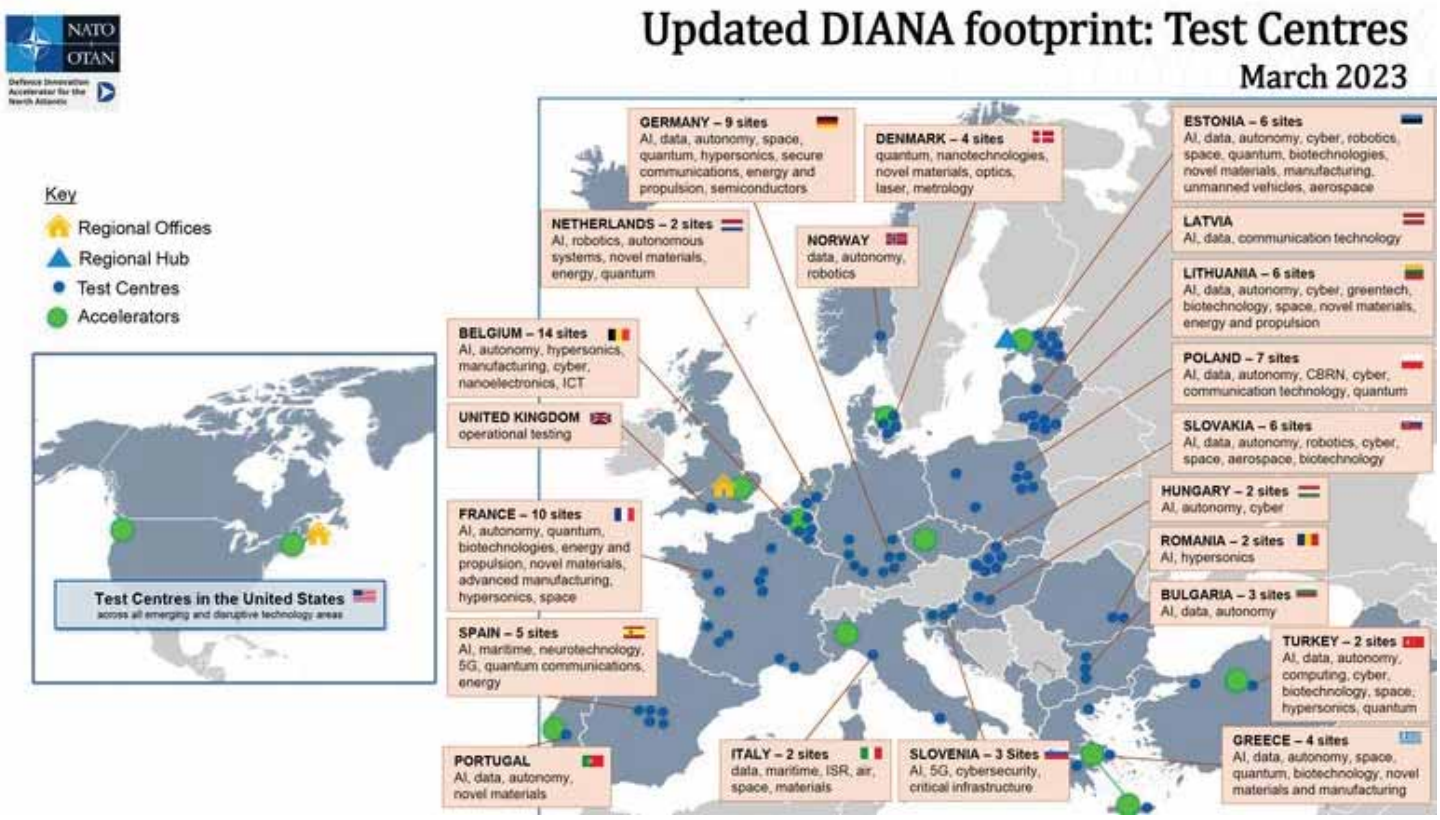
6. **Align Dual-Use Industrial Base Expertise Across the Interagency –** To better leverage dual-use technologies for the warfighter, the DoD must more effectively align expertise, networks, and resources with its interagency partners, particularly the Department of Commerce – an increasingly critical partner in domestic and international industrial policy. During engagements with the interagency, there was an evident lack of mutual understanding regarding the intersection of DoD and Commerce portfolios covering the defense and dual-use technology industrial bases, respectively. To the extent that it exists, DoD and Commerce alignment appears to be based largely on personal relationships and focused on specific areas such as export control rulemaking and next-generation wireless network development, rather than covering the vast array of cross-cutting issues facing the modern U.S. and allied industrial base. One important area of domestic cooperation has been the Manufacturing USA/Innovation Institute network, which Commerce leads with support from the DoD Manufacturing Technology (ManTech) office.[53] To continue strengthening the DoD's access to commercial technologies, and to enhance its international industrial cooperation, the DoD and Commerce should greatly expand their efforts beyond existing areas of collaboration by sharing information and expertise, maintaining close and continuous communication, and aligning efforts and resources domestically and internationally where appropriate.



Source: DoD Manufacturing Technology (ManTech) Program

Note: Interagency collaboration to enhance U.S. global industrial competitiveness should be greatly expanded beyond existing efforts such as the Manufacturing USA/Innovation Institute network, overseen by the National Institute of Standards and Technology (NIST) under the Department of Commerce.

[53] Manufacturing USA. Department of Defense Manufacturing Technology Program. https://www.dodmantech.mil/Manufacturing-Collaborations/Manufacturing-USA/



Source: NATO

7. **Establish Special Innovation Zones for Key Allies and Partners –** To reinforce the U.S. national security industrial base and ensure U.S. warfighters are able to benefit from the best technologies across allies and partners, the DoD should consider establishing special innovation zones among key foreign partners that further institutionalizes existing regulatory frameworks to support reciprocal defense procurement and co-development, co-production, and co-sustainment. Akin to special economic zones, these special innovation zones should integrate a network of development sandboxes for various emerging technologies in controlled environments where developers from allies and partners can safely test new software, algorithms, and other technologies without affecting production systems. These sandboxes would create conducive allied and partner nation environments for co-innovation, provide capacity-building through strengthened regulatory expertise and cooperation, improve regulatory clarity and compliance, and foster future networks and services. OSD cooperative oversight programs – where participating U.S. services and other entities develop capabilities with their counterpart foreign organizations – demonstrate the utility of assembling different entities under one roof as opposed to pursuing parallel service-based approaches to addressing the broad challenges of supporting allied and partner nation industrial base growth.

8. **Create an International Defense Innovation Community of Interest –** The DoD must more proactively foster an international network of researchers, engineers, and innovators sharing general concepts and information about their work to address shared security challenges. This community of interest would enable allies and partners to gain greater awareness of workstreams among their counterparts,

much like in private industry where companies may share general information about their work without disclosing to competitors their intellectual property and other proprietary information. This community of interest could exist as a combination of physical and virtual hubs, leveraging existing frameworks such as DSCA's regionally focused security studies organizations (e.g., German Marshall Center and Hawaii Asia-Pacific Center), NATO DIANA, NATO Innovation Network, NATO-accredited centres of excellence, and other engaged research institutes, universities, and labs. This community of interest would also support the need for greater collaboration on upskilling and reskilling the international defense industrial labor force, building on domestic efforts such as the Manufacturing USA/Innovation Institutes and new U.S. AI Safety Institute**.**

Exhibit 5. Innovation Hotline Recommendation

To help allies and partners better understand the DoD's sprawling innovation ecosystem, the proposed USD(IIC) should consider establishing a 'hotline' with a select group of trusted nations to include the NTIB members, Japan, ROK, and others as appropriate. The purpose of this hotline should be to exchange general information and best practices about the countries' respective defense innovation ecosystems. During the DIB's interactions, allies and partners had numerous basic questions about the U.S. defense innovation ecosystem, underscoring a need for greater information sharing between key DoD innovation organizations, such as DIU, DARPA, and CDAO, and their foreign counterparts.

9. **Launch an Allied Digital Engineering Hub –** As the DoD embraces further digitization to address ongoing supply chain issues, as well as longer lead times and talent shortages caused by increased demand for defense materiel, it should focus resources and expertise across allies and partners to develop digital engineering solutions for defense manufacturers. Digital engineering ("digital twin") technologies can play a crucial role in improving quality and efficiency of defense production. Creating digital replicas of physical assets can help engineers simulate designs, test prototypes virtually, and optimize manufacturing processes. This supports accelerated product development, speeds up design iteration, and enables supply chain optimization through real-time monitoring and predictive maintenance for identifying supply bottlenecks and streamlining logistics. Digital platforms can also facilitate communication and collaboration among suppliers, improving coordination and reducing lead times. The DoD should work with allies and partners to scale access to these tools.

10. **Form a Trusted Capital Marketplace for Allies and Partners –** The DoD should work with allies and partner nations to ensure that foreign defense technology and dual-use companies are able to identify trusted capital. Leveraging the NATO DIANA and Innovation Fund efforts for educating NATO member industry and capital allocators about the risks of predatory financing, alongside domestic efforts such as the Office of Strategic Capital (OSC) to crowd-in private capital in critical technology areas, the DoD should invest in a new information system accessible to allies and partners resembling an earlier concept for a Trusted Capital Digital Marketplace (TCDM). Finalizing pilot work begun in 2019 at the behest of that year's NDAA, TCDM was launched shortly before the Biden administration took office, to promote trusted sources of funding for small and medium

sized innovative defense companies.[54] TCDM was intended as a gateway to an investment ecosystem for trusted sources of capital, in response to concerns about predatory investment by foreign adversaries. The program was designed to connect vetted investors with qualifying domestic companies, and to use rapid acquisitions contracting vehicles to down-select participating companies and expose them to a range of 'trusted' capital solutions. A new trusted capital marketplace for allies and partners could fill a similar function internationally as TCDM aimed to domestically.

C) Regulatory & Compliance Reform

In order to build a networked defense industrial base, the DoD must first create a regulatory and compliance environment that allies and partners feel comfortable navigating and, with time, harmonizing with their own. ITAR serves a necessary mission, safeguarding U.S. treasure, but has not been fit-for-purpose for some time. Other DoD frameworks, namely the Technology Security and Foreign Disclosure (TSFD) and Cybersecurity Maturity Model Certification (CMMC) processes, are also interfering with core national security and foreign policy objectives.

Exhibit 6. Cybersecurity Maturity Model Certification (CMMC) Recommendations

Cybersecurity Maturity Model Certification (CMMC) is designed to enforce defense industrial base cybersecurity standards and provide assurance that defense contractors and subcontractors are meeting cybersecurity requirements. CMMC 1.0 was published in September 2020 and outlines the basic structure of the framework along with a five-year phase-in period. CMMC 2.0 was announced in November 2021 and is currently undergoing rulemaking efforts.[55]

While CMMC 2.0 is not yet fully required for DoD contracts, allies, partners, and industry are hurrying to realize the forthcoming contractual requirements. Despite the partial implementation and intended streamlining through 2.0, these changes have caused significant struggles and concerns throughout the industrial base. Smaller domestic industrial partners are struggling with associated costs – one company we heard from spends $1 million of its $30 million annual revenue on CMMC compliance – while allies and partners are fearful of nationality and qualification requirements, as well as a general lack of clarity regarding guidelines for overseas operations.[56] To mitigate these concerns and better align CMMC for allies and partners, the DIB recommends the following:

1. Open the CMMC ecosystem to selected individuals from allied and partner nations. As it currently stands, CyberAB (the official accreditation body of the CMMC ecosystem and non-governmental DoD partner) requires that Certified CMMC Assessors (CCA) and Certified CMMC Professionals (CCP) be U.S. citizens. Concurrently, Career Pathway Certified Assessor (CPCA) 612 certification is only open to people within the United States and will prevent foreign partners from meeting CCA requirements. The proposed ecosystem will be stifling to allies and partners and necessitates foundational changes in approach to certification. Properly training and integrating trusted partners is essential for ensuring the necessary scale and security within the defense industrial base.
2. Introduce specific measures for establishing Certified Third Party Assessment Organizations (C3PAO) outside the United States. The lack of specific measures requires international

[54] Department of Defense Announces Establishment of the Trusted Capital Digital Marketplace. U.S. Department of Defense. (2021, January 13). https://www.defense.gov/News/Releases/Release/Article/2470485/department-of-defense-announces-establishment-of-the-trusted-capital-digital-ma/

[55] About CMMC. Chief Information Officer. (n.d.). https://dodcio.defense.gov/CMMC/About/

[56] DIB engagement with industry stakeholders (2024, April 26)

supply chain operations to comply with U.S. C3PAO institutions and complete compliance verification across national borders, a process that causes cost overruns due to additional time and material expenses. Allowing allies and partners to establish their own C3PAO mechanisms in alignment with the United States would streamline compliance verification, reducing costs and incentivizing further engagement from foreign companies.

3. Allow allied and partner nation institutions to publish localized training materials and obtain formal recognition as a resource for CMMC compliance. Foreign institutions should be allowed to apply to become Licensed Training Providers (LTP) certified to assist foreign industry with compliance requirements and industrial base security. Current proposed rules allow only U.S. companies to act as LTPs and Licensed Partner Publishers (LPP), which will cause significant delays in international partners understanding and adopting proper compliance reforms.

This is not a new observation. Numerous reports, comments, recommendations, and reform efforts have been undertaken to improve the ITAR process in particular, but many of the same barriers persist. In response to an enormous backlog of approximately $22 billion in FMS sales to Taiwan, Congress has undertaken steps to expedite arms transfers to Taipei through the Foreign Military Financing program, as well as Presidential Drawdown Authority making available up to $1 billion annually in defense weapons using DoD stocks.[57] In January 2024, Congress found that senior officials at the DoD and Department of State remain lacking in accountability for significant delays in FMS cases, "creating a lack of urgency to speed the process up."[58] The congressional review also concluded that the DoD "does not consistently value the strategic benefit of sharing major defense articles with our allies" and "there is no common operating picture for the FMS process across the DoD, State, Congress, Industry, and our allies and partners, leading to confusion and inefficiency."[59] In short, we are failing to move technologies across borders when appropriate and failing to integrate capable and willing partners across foreign industry.

Given the breadth and severity of these shortcomings, a dedicated, empowered executive is needed who is equipped with the necessary authority and resources to negotiate process improvements involving these regulatory and compliance frameworks across the U.S. federal government. As a direct report to the Secretary and Deputy Secretary of Defense, the DIB's proposed USD(IIC) would hold the power to holistically address these issues both within the DoD and in conjunction with the federal interagency and other partners. Currently, DTSA represents the DoD in the interagency process responsible for compliance with multinational export control regimes, and coordinates the DoD position with regard to proposed changes to ITAR and EAR. A higher-altitude strategic leader is necessary to properly coordinate this account. Ultimately, the Departments of State and Commerce must decide with Congress how to prioritize reforms to these regimes, but the DoD must be equipped to represent its position fulsomely to the interagency on all matters pertaining to technology sharing with allies and partners.

Building on the 2023 DoD FMS Tiger Team's recommendations, the DIB identified the following actions for our proposed USD(IIC) to accelerate efforts to unravel this regulatory and

[57] Report to Congress on Taiwan Defense and Military Issues. USNI News. (2024, March 1). https://news.usni.org/2024/03/01/report-to-congress-on-taiwan-defense-and-military-issues
[58] Foreign Military Sales Tiger Task Force: Report. Foreign Affairs Committee. (2024, February 7). https://foreignaffairs.house.gov/wp-content/uploads/2024/02/2.7.24-FMS-TIGER-Task-Force-Report.pdf
[59] Ibid.

compliance framework in collaboration with the interagency. These recommendations represent a sincere effort to advance technology sharing practices, improving co-innovation with allies and partners while maintaining paramount security standards. These recommendations are not comprehensive solutions – we acknowledge that these are complex challenges requiring careful thought that prior and ongoing reform initiatives are already undertaking adroitly. However, these recommendations highlight some ideas for addressing core problems that may serve as foundational action items to drive momentum toward improved technology sharing practices.

1. Grant the Secretary of Defense authority to waive ITAR constraints at will, and further, delegate to the proposed USD(IIC) similar blanket waiver authority for any technologies *not* on some restricted list. In addition, the Secretary should designate a single authority – ideally the new USD(IIC) – as responsible for implementation of FMS reform within the DoD. Reforms should be enforced not by committee vote but by a sole authority. The Tiger Team's transition to a continuous process improvement posture, overseen by the FMS Continuous Process Improvement Board, completes the necessary interim step of bringing together the various stakeholders who oversee the FMS process across different stages. The accompanying Security Cooperation Execution Focus Forum does an important job of motivating further DoD urgency around key FMS cases that are languishing, raising attention around specific barriers and pain points by bridging the gap between decision-makers and the Security Cooperation Office (SCO) and new Defense Security Cooperation Service personnel who are the primary U.S. embassy points-of-contact responsible for facilitating day-to-day FMS coordination with foreign counterparts. Our recommendation for a new USD(IIC) would motivate a higher degree of top-cover and senior-level attention, ensuring that DSCA, DTSA, and other DoD components have the requisite authorities, resources, and latitude to ensure smooth and efficient FMS operations. This official would also be at the appropriate altitude to enforce a new set of incentives to steer partners toward defense acquisitions that meet their needs – even if delivered from Non-Program of Record (NPOR) acquisition programs – and to assess contracting officers on their FMS contracting performance.
2. Develop a formal process for allowing allied and partner nation representatives as well as industry experts to recommend the relocation of dual-use items from the ITAR U.S. Munitions List (USML) to the EAR Commerce Control List (CCL). The current speed of the interagency review process is untenable, and foreign partners and industry are generally more up to date on the proper placement of their technologies. The modern technology environment has significantly blurred the lines between dual-use, commercial, and military systems, and a more agile and modern approach is necessary to maintain proper identification.
3. Reform and streamline the ITAR Technical Assistance Agreement (TAA) requirements for NATO member entities. Currently, if a company or individual in the United States wants to provide defense services with foreign companies or governments within NATO, a TAA must be completed listing each of NATO's 32 members, regardless of their involvement. This requires an execution signature from each nation and presents an undue burden on the entities working through this process. To simplify this, we recommend a broad "NATO Alliance" selection which addresses the alliance's full complement of 32 members, and any future expansion given the ten-year expiration for TAAs. Any specific technological restrictions could be addressed through provisos attached to the TAA approval.
4. Bolster the ITAR application database with new capabilities. In July 2013, when the Department of State transitioned from

DTRADE2 to the DoD's secure export licensing database, called USXports, the intention was to make the export licensing review process a more seamless one. However, by accounts, USXports has also been problematic. Reportedly, during one recent summer at the height of the Ukraine war, the entire database crashed for weeks, leaving FMS case officers at State scrambling, for example, hand-carrying classified ITAR application materials between government buildings to canvass for approval signatures manually.[60] This should never happen again. Furthermore, the database should be fortified with new analytic and automated capabilities to make it easier to identify and tag cases in the system for review and signature.

5. Expand FMS training and education programs. The Tiger Team recommended improvements to SCO training focused on FMS pre-Letter of Request (LOR) efforts. Pre-LOR efforts are essential for streamlining the subsequent FMS process. From stakeholder interviews with companies, foreign partners, and anonymous current and former officials involved with the FMS approval process, there needs to be enhanced training, mentorship, and professional development opportunities to enable personnel across the U.S. federal government to gain diverse and hands-on experience across different facets of security cooperation. This would include increasing the number and regularity of Temporary Duty (TDY) and rotation opportunities, organizing regular training seminars and workshops both for FMS licensing officers and for industry to better understand the FMS process, and frequent Industry Days to foster stronger relationships with defense industry and particularly dual-use industry who are less familiar with government export rules. Personnel should be rotated between DSCA, DTSA, and key offices at the Department of State, namely the Directorate of Defense Trade Controls (DDTC) and Office of Regional Security and Arms Transfers (RSAT), and the Department of Commerce, namely the Bureau of Industry and Security (BIS), to strengthen relationships and connections between these vital organs of the multilateral export control process. In particular, DoD embeds from DSCA and DTSA to State and Commerce, and vice versa, would enhance the DoD's position on proposed changes to the ITAR and EAR regimes.[61] These personnel enhancements should provide a holistic solution involving at least a few of the following actions for bolstering the workforce tasked with implementing ITAR:

   - Direct DSCA and DTSA to collaborate with DDTC to host a regular series of in-house seminars for industry on the ITAR process. Currently, DDTC provides seminars roughly twice a year.[62] Seminars are mostly presentations, when they should be more interactive, creating opportunities for industry to ask questions of licensing officers. These seminars should be held offsite from government facilities so that stakeholders can engage from across the ecosystem, including foreign embassies and smaller companies. Other programs, such as Society for International Affairs (SIA) coursework on export control policies, can be leveraged.
   - Develop a training module for Foreign Service Officers and Foreign Area Officers to improve their knowledge and understanding of multilateral export control regimes, FMS review processes, as well as technical information regarding sensitive technologies and weapons systems.
   - Increase the number of DoD uniformed officers assigned to DDTC from the current standard of between six and eight. These servicemembers provide an

[60] DIB interview with industry stakeholder (2024, April 9)
[61] DIB interview with ITAR expert (2024, April 24)
[62] Ibid.

outsized impact on an office that at times lacks sufficient knowledge of weapons systems and military technologies.

- Encourage and assist DDTC with receiving the resourcing necessary for this capability augmentation.
- Utilize non-competitive hiring authorities, such as the Intergovernmental Personnel Act (IPA) and U.S. Digital Corps pathways, to recruit a qualified team of engineering and other STEM-trained talent who understand the advanced defense and dual-use technologies under ITAR or EAR review.
- Recommend that Congress request a Government Accountability Office (GAO) report on DDTC resourcing levels and what a lack of ITAR reform is costing the U.S. taxpayer and industry.

Exhibit 7. AUKUS Exemption Recommendations

On May 1, 2024, DDTC proposed a rule[63] that would amend ITAR and establish:

- Licensing exemptions for ITAR-controlled defense trade between the United States, United Kingdom, and Australia.
- An expedited licensing process (to include Canada) when exemptions did not apply.
- An expanded exemption for the transfer of classified information for dual nationals who meet specific criteria and are Australian or British citizens.

The proposed rule also includes several limitations:

- The exemption only applies to export activities originating within the AUKUS countries.
- Involved parties must be authorized by DDTC, or by relevant Australian and British authorities developed in coordination with DDTC.
- Transferors must maintain detailed records of transactions.
- The exemption does not apply to transfers requiring congressional certification.
- A new Excluded Technologies List (ETL) appended to the rule lists items and services that are not exempt.

The proposal is pursuant to new authorities and requirements contained in Section 1343 of the FY2024 NDAA which, in part, directed the Department of State to implement an ITAR exemption for the AUKUS countries.[64] Short of a complete ITAR exemption for AUKUS, to help ensure that proposed ITAR rule changes are effective and utilized, the DIB recommends the following:

1. Eliminate the ETL, or dramatically simplify, shorten, and explain it to industry partners. In its current form, the ETL is long and complex and will cause industry – particularly less-resourced, non-traditional defense and dual-use technology start-ups – to revert to complying with the full range of ITAR commitments.[65] Many of these commercial technologies will be crucial to the development of advanced capabilities under AUKUS Pillar II, and the ETL has been fashioned as a way of capturing Pillar II technologies in order to safeguard shared capabilities, while making these technologies attainable through the appropriate export licensing procedures. As currently presented, the ETL will essentially exclude AUKUS

[63] International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation Among Australia, the United Kingdom, and the United States. Federal Register. (2024, May 1). https://www.federalregister.gov/documents/2024/05/01/2024-08829/international-traffic-in-arms-regulations-exemption-for-defense-trade-and-cooperation-among

[64] National Defense Authorization Act for Fiscal Year 2024

[65] DIB interview with industry stakeholder (2024, April 10)

technologies from the AUKUS exemption, i.e., maintaining the status quo of ITAR, and repeating the mistakes of previous reform efforts.[66]

2. Implement an AUKUS checkbox on ITAR application forms that would trigger the application to process immediately to the DoD for review. Checking this box would signal that the export involves defense articles or services related to AUKUS, indicating that the application should bypass the standard DDTC review and proceed directly to the DoD for assessment. The checkbox could help speed up review times for AUKUS-related applications without requiring further extensive changes to ITAR like the recent export control revisions introduced by the Department of Commerce.
3. Streamline export control processes and procedures for AUKUS countries – by executive order, if necessary. The President of the United States has discretion to classify different rulesets for programs or categories of technologies. AUKUS-specific program licenses and open general licenses (OGLs) should cover pre-existing defense items, facilitating their operational use and maintenance. This will encourage interoperability and interchangeability of defense capabilities. The industrial base for these licenses and OGLs should be defined mutually by the AUKUS countries, incentivizing participation by smaller companies. Specific program licenses and OGLs would enable the transfer of U.S. technologies for production capabilities in Australia and the United Kingdom, leveraging a trusted group of industry firms working in the United States.

6. Conduct a comprehensive review of the TSFD process. TSFD has never been fully examined and is one of the key drivers for delays in the defense trade system.[67] The Military Departments and other DoD stakeholders are an overlooked but major driver of tech release to allies and partners and can sometimes act as significant blockers to cooperation.[68] Section 918 of the FY2024 NDAA instructed the Secretary of Defense to undertake a review of the TSFD process and propose changes to the system that would enhance transparency among the various stakeholders involved in the TSFD process, streamline the various parallel TSFD processes to better assist DoD components and their acquisition program officers, and improve interagency collaboration to enhance the speed and effectiveness of TSFD.[69]
7. Enhance the Special Defense Acquisition Fund (SDAF). As the war in Ukraine has revealed by the White House's reliance on Presidential Drawdown Authority to fund rapid weapons transfers to Ukraine, the United States needs a better mechanism to anticipate future demand so that it can stockpile high-demand, disposable items. The SDAF, a revolving fund that is utilized by the DoD in consultation with the Department of State, is resourced for this specific purpose, but remains underutilized.[70] A recent report by Congress recommended that the DoD and State utilize a funding-swap mechanism to knit their resources and acquisition decisions together.[71]
8. Strengthen Security of Supply Arrangements (SOSA). These initiatives are intended to enhance "mutual interdependence of supplies needed for national security." However, SOSA are "best effort"

[66] DIB engagement with industry stakeholders (2024, April 26)
[67] DIB interview with industry stakeholders (2024, April 26)
[68] DIB correspondence with industry expert (2024, June 21)
[69] National Defense Authorization Act for Fiscal Year 2024
[70] Defense Security Cooperation Agency (2016). Retrieved June 27, 2024, from https://samm.dsca.mil/policy-memoranda/dsca-16-19.
[71] Foreign Military Sales Tiger Task Force: Report. Foreign Affairs Committee. (2024, February 7). https://foreignaffairs.house.gov/wp-content/uploads/2024/02/2.7.24-FMS-TIGER-Task-Force-Report.pdf

international arrangements rather than binding international agreements, and thus relatively informal and voluntary frameworks that are mainly about confidence-building. Turning these arrangements into agreements would ensure that the United States and signatories feel obligated to invoke the SOSA as a formal commitment to provide solutions for achieving supply assurance.[72]

Across these processes, we have failed thus far to adequately reform and streamline relevant areas, and industry remains skeptical that we will achieve the necessary change. Both domestic and foreign companies emphasized in the strongest of terms that DDTC requires further support, TSFD is underemphasized, and CMMC compliance is imposing inordinate costs on smaller companies.[73] [74] Ensuring that we approach regulatory and compliance issues with the necessary speed is of the utmost importance.

D) Information Sharing & Communications Technology

The importance of information sharing and communications technology, and how far behind we are in effectively modernizing the systems and processes governing this space, cannot be understated. Within the DoD, frustration regarding the ability to get information to allies and partners is omnipresent. Defense personnel, especially below the senior level, are not empowered to take decisive action regarding what information can and should be shared, and instead are paralyzed by fear of non-compliance and security violations.

Within the current system for classification, information classified at higher levels of secrecy is generally easier to move and share when deemed necessary. There is more latitude in law and policy to make decisions and move quickly.[75] It is paradoxical that CUI and Secret information are frozen by numerous laws and regulations, making less sensitive information more difficult to share. The workforce often must make the grim calculus that sharing information with allies and partners is not worth the level of effort required.[76] Nations deserve their space to make decisions and withhold highly classified information when deemed necessary, but the CUI and Secret ecosystem must be reformed. The system as it currently stands is fundamentally broken. If we are all-in on allies and partners, we must act like it.

Exhibit 8. USINDOPACOM Joint Mission Accelerator Directorate (JMAD)

In August 2023, USINDOPACOM launched the Joint Mission Accelerator Directorate (JMAD) to better connect the theater command's critical mission needs with commercial industry capabilities and ongoing programs across the defense innovation community.[77] The organization is charged with developing a common technical roadmap for key INDOPACOM programs for improving information sharing, namely, the Joint Fires Network, INDOPACOM Mission Network, Pacific Multi-Domain Training and Experimentation Capability, and STORMBREAKER. The JMAD coordinates with other DoD organizations, including DIU, CDAO, and OSD R&E, and maintains an industry engagement team for identifying mature commercial solutions. The JMAD is an encouraging effort to source and acquire unique capabilities while considering allied and partner nation requirements at the theater-command level.

[72] McGinn, J., & Roche, M. T. (2023, June 26). A "Build Allied" Approach to Increase Industrial Base Capacity. George Mason University School of Business Baroni Center for Government Contracting. https://business.gmu.edu/news/2023-06/build-allied-approach-increase-industrial-base-capacity
[73] DIB engagement with industry stakeholders (2024, April 26).
[74] DIB interview with industry stakeholder (2024, April 10)
[75] DIB interview with DoD stakeholder (2024, May 24)
[76] Ibid.
[77] Gill, J. (2024, February 28). INDOPACOM Stands Up New Directorate to Better Connect Industry, DOD Innovation Efforts. Breaking Defense. https://breakingdefense.com/2023/08/indopacom-stands-up-new-directorate-to-better-connect-industry-dod-innovation-efforts/

These issues are not new, but a genuine effort to overhaul classification, information sharing, and communications systems and processes has yet to succeed. A healthy information sharing ecosystem will provide the DoD with the latitude to manage its most closely held secrets while simultaneously empowering the workforce to get information to our allies and partners as necessary. To develop this new information sharing paradigm, the DIB recommends the following:

1. The DoD should change foreign release guidelines for CUI and Secret information to default from "NOFORN" to "YESFORN". Modeled on decades of success within the Intelligence Community, particularly the Five Eyes, the DoD and allied and partner nation defense workforce must assume a collective responsibility for information sharing and security. DoD Directive 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations* provides a ready-made policy to this end, stating that disclosure must be "consistent with U.S. military and security objectives."[78] Strategic realities and the emphasis on allies and partners clearly meet this criterion.
2. The DoD should update its standards for communication and information sharing so that allies and partners can harmonize their technical standards, capabilities, and policies. Clearance adjudication, cybersecurity infrastructure, and personnel training requirements should be clearly addressed. The renewed effort to create interoperable Mission Partner Environments (MPE), allowing communication and sharing of sensitive information securely and in real-time with allies and partners, is fueling a new commitment to integrate mission and coalition partners. As the DoD moves from a U.S.-centric to a global information technology environment, allies and partners are pursuing updated information sharing capabilities, but lack clear roadmaps to do so. The existence of a clear DoD framework would also provide guidelines to classify nations who meet the "YESFORN" standard.
3. The DoD should develop additional handoff protocols and controls to share information with any foreign partner it might have to engage in the future. Systems for exchanging cross-domain military data date back decades to platforms such as CRONOS (NATO's longstanding secure-messaging network), the Combined Enterprise Regional Information Exchange System (CENTRIXS) (which was mobilized for NATO coalition operations in Iraq and Afghanistan), Battlefield Information Collection and Exploitation Systems (BICES) (also widely used in NATO operations today), and the Combatant Command MPE-Information System networks which currently support USCENTCOM, USEUCOM, USAFRICOM, and USINDOPACOM operations. The DoD is making progress to collapse the speed and effectiveness of secure networks for sharing information with coalition partners with its Secret and Below Releasable Environment (SABRE), which allows partner nations to use their own networks to connect and share information seamlessly. But fundamental efforts are needed to prepare for automated but secure data sharing with a range of partner nations that the DoD might need to engage with in future operations.
4. Resource new theater command MPEs. Development and implementation of next-generation MPEs such as the INDOPACOM Mission Network (IMN) requires adequate funding and alignment within the DoD. Without sufficient resources, cohesive

[78] Under Secretary of Defense for Policy. (n.d.). Disclosure of Classified Military Information to Foreign Governments and International Organizations. Department of Defense.

governance structures, and top-down leadership, even the best-conceived initiatives will falter or not progress. Over the last five years, and perhaps longer, IMN and its precursor MPE have been a recurrent unfunded Commander's priority. Although the Indo-Pacific is the DoD's priority theater, IMN's $124 million cost remains unfunded for FY2025 and should be prioritized.[79]

5. The DoD should develop a cyber and information security assistance program to help allies and partners stand up systems and processes suitable for a modern information sharing environment. This should include technology acquisition, policy and process implementation, and exercises and training. Increasingly there are allies and partners demonstrating both the will and means to be more effective information sharing partners. It is incumbent upon the DoD to assist allies and partners when these conditions are met.
6. The DoD should consider adopting a category of 'burner phone'-esque commercial point-to-point technologies to facilitate the transfer of CUI with allies and partners. To this end, the DoD should conduct an analysis of existing technologies for the communication of CUI with allies and partners, and explore their potential applications in combined multi-domain operations. These platforms may include, but are not limited to, Signal, WhatsApp, and Discord. Ukraine has made extensive innovative use of industry technologies such as mobile platforms and applications to manage battlefield operations, much less sharing CUI. A notable example is its Delta Situational Awareness System turning satellite imagery, targeting information, and battlefield position tracking into a real-time battle command mobile app.[80] Another example is Diia, a Ukrainian government app originally built for civil uses such as paying taxes that, due to its ubiquity among Ukrainian mobile users, became a tool for collecting citizen data on enemy movements via encrypted messages.[81] As conventional military tactics are being fused with cyber and information warfare, seamless data sharing is needed to effectively counter and respond to multifaceted threats.

Taken as a whole, this set of recommendations should provide an actionable roadmap to a healthier information sharing environment for allies and partners. It is necessary for the DoD to internalize the increasingly essential truth that the real risk in this space is not a technical manual being read by someone that should not have seen it, or a CUI email making it into the public domain. It is that we are insufficiently integrating our allies and partners into key information networks and undertaking preparations for a future informatized conflict.

E) AUKUS

AUKUS is the primary opportunity for the DoD to get openness and collaboration right. It is between longstanding allies who share a common language, values, and strategic vision, and was formulated in a time of emphasis on allies and partners. Unlike NATO and other established multilateral institutions, the vestiges of Cold War secrecy that shaped their evolution do not have to define AUKUS's future. Properly realized, AUKUS can serve as a 21st century model for co-innovation with allies and partners, and a resounding success as the DoD continues down a new path of innovation cooperation. Some early AUKUS wins include Section 1080 of the FY2024 NDAA which streamlines technology sharing among the AUKUS countries under the umbrella of Title III of the U.S. *Defense Production Act*, the Deep Space Advanced Radar Capability (DARC) program which is building three ground-based radars

[79] Beinart, M. (2024, March 19). INDOPACOM's $11 billion Unfunded List Includes Guam Defenses, Classified Space Efforts. Defense Daily. https://www.defensedaily.com/indopacoms-11-billion-unfunded-list-includes-guam-defenses-classified-space-efforts/pentagon/

[80] Ukraine to introduce Delta Situational Awareness System for military. The Kyiv Independent. (2023, February 4). https://kyivindependent.com/government-introduces-nato-standard-delta-management-defense-system/

[81] Dickinson, P. (2023, May 31). Ukraine's Diia Platform Sets the Global Gold Standard for E-government. Atlantic Council. https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-diia-platform-sets-the-global-gold-standard-for-e-government/

(one in each country) for space situational awareness, and the continuation of a series of AUKUS AI and autonomy trials to advance initial joint development of coalition autonomous systems.

Despite this opportunity and the many good intentions surrounding it, AUKUS is far from a guaranteed success. Pillar I is still a long-term project requiring sustained commitment and industrial heft, while Pillar II is still nascent and has yet to attract committed funding lines and full buy-in from industry. Properly orienting AUKUS requires careful management of the balance between more urgent defense needs and long-term capability investment. We have yet to find this equilibrium. Industry demonstrates real excitement at the prospect of Pillar II collaboration but remains skeptical as it awaits appropriate demand signals from the three governments.[82] Additionally, the regulatory and compliance challenges discussed in the above pages stand as significant roadblocks to success. One industry commentator noted that without proper reform, ITAR may largely nullify AUKUS Pillar II.

Primarily focused on Pillar II, this study examined a series of actions to build interoperability among the existing AUKUS countries, address the barriers that private sector will face in participation, achieve demonstrable wins through integration of new capabilities into combined operations, and drive momentum for potential expansion of Pillar II to like-minded nations in the region and beyond.

1. The DoD should establish a network of AUKUS centers of excellence nested to key Pillar II priorities, building on the Australian *Defence Industry Development Strategy*'s recognition that such institutions are needed for enhancing research cooperation within the pillar.[83] To ease start-up costs and minimize risk, initial efforts should target lower barrier-to-entry topics. These may include an AI and machine learning taskforce focused on ethics, research, and collaborative defense use-cases, as well as a cyber taskforce modeled on the NATO Cooperative Cyber Defense Centre of Excellence to serve as a knowledge and training hub for cyber professionals across the three countries. In addition, building on the NATO-Australia *Individually Tailored Partnership Programme*, Australia should be brought in as an observer-nation to the NATO Cyber COE.
2. The DoD should establish an AUKUS Defense Innovation Accelerator and Fund (DIAF) modeled on the NATO DIANA and Innovation Fund efforts. The AUKUS DIAF would similarly aim to decrease costs for deep technology testing and evaluation, improve rapid acquisition for dual-use technologies, build a trusted investor community to combat adversarial capital, and spotlight and network innovation hotspots across the AUKUS countries. The AUKUS DIAF should also be leveraged to enable dual-use technology scanning across the Indo-Pacific with a trained corps of science and technology experts embedded in AUKUS-affiliated universities, labs, and other academic or industry research facilities. This would enable AUKUS regulators to keep abreast of industry developments to understand how changes stemming from ongoing revisions to defense trade controls across the three countries impact costs and benefits and thus the viability of existing business models. It would also address the imperative of developing compatible technology and certification standards among the AUKUS countries. Participation in the DIAF should be kept open to individuals or companies from non-AUKUS countries, fulfilling the simmering appetite among other countries in the region such as Japan, ROK, New Zealand, and the Philippines for participation in allied defense innovation.

[82] DIB engagement with industry stakeholders (2024, April 26)
[83] Defence Ministers. (2024, February 28). Landmark Strategy to Maximise Support for Defence Industry. Defence Ministers. https://www.minister.defence.gov.au/media-releases/2024-02-29/landmark-strategy-maximise-support-defence-industry

3. The DoD should work with the AUKUS countries to ensure their industrial security standards and data-sharing protocols are aligned. Urgent investment is needed in collaborative associated infrastructure, information technology, and cybersecurity. The United Kingdom's *Defence Standardization* (DStan) and Australia's *Defence Industry Security Program* (DISP) must align better with the U.S. *National Industrial Security Program* (NISP), sharing resources, benchmarking and possibly even merging some critical functions. In the same vein, the AUKUS countries should collaborate to establish common open system architecture (OSA) standards which are increasingly important as software updates have become part of almost all military equipment.
4. The DoD should establish a shared data center for the AUKUS countries (i.e., an AUKUS GovCloud) operating under a centralized AUKUS body to maintain data hygiene and organization. Funding for data centers is happening across the AUKUS countries, and much of the foundational work (e.g., large language model development) is being replicated. Unifying this work under a single cloud infrastructure would decrease costs and eliminate redundancies while demonstrating an effective starting point for future information sharing and communications interoperability within AUKUS.

Getting AUKUS right is an essential task not only as a key component of Indo-Pacific security, but as a signal that the DoD and United States writ large are committed to the values set forth in our guiding strategic documents.

F) NATO & Europe

While NATO has long been a cornerstone of DoD international engagement and cooperative innovation, numerous barriers persist to fully realizing the alliance's potential. Traditionally, NATO has been a source of military hardware sharing, maintenance, logistics, and mutual defense. These efforts are generally conducted on an "as-needed" basis and, since the end of the Cold War, have not been a source of long-term strategic coordination. This status quo is no longer viable. Comprising nearly 50 percent of global GDP, this community remains an immense source of relatively untapped potential. Nascent efforts such as the NATO DIANA and Innovation Fund are important initiatives, but they only start to address the fundamental issues.

NATO's 32 members have struggled to fully embrace innovation and interoperability. Adversarial capital abounds in the NATO innovation space, acquisition remains too slow, defense outlays for future modernization are not being spent efficiently or at all, the innovation community is fragmented and communication is difficult, and competing national interests and Buy European tendencies remain prevalent.[84] The DoD must recognize that there is a strategic interest in protecting and fostering innovation ecosystems within NATO, and work to ensure a thriving defense innovation ecosystem across the alliance.

Exhibit 9. NATO Innovation Ecosystem

Following Russia's annexation of Crimea in 2014, NATO members committed to reversing their trend of shrinking defense budgets. This year, 23 of NATO's 32 members will hit their 2 percent of GDP defense spending pledges, compared to only three in 2014.[85] Beyond that, 31 of the 32 members have committed to a timeline for reaching 2 percent. Building on the *NATO 2030* agenda at the 2021 Brussels Summit, NATO's 2022 *Strategic Context* defines the risks and opportunities of emerging and disruptive technologies and aims to promote innovation and

[84] DIB engagement with ally/partner stakeholders (2024, May 24)
[85] Knickmeyer, E., & Kim, S. M. (2024, June 18). A Record Number of NATO Allies are Hitting their Defense Spending Target During War in Ukraine. AP News. https://apnews.com/article/nato-defense-spending-stoltenberg-biden-5246409eec70745e6e936d997073a6f4

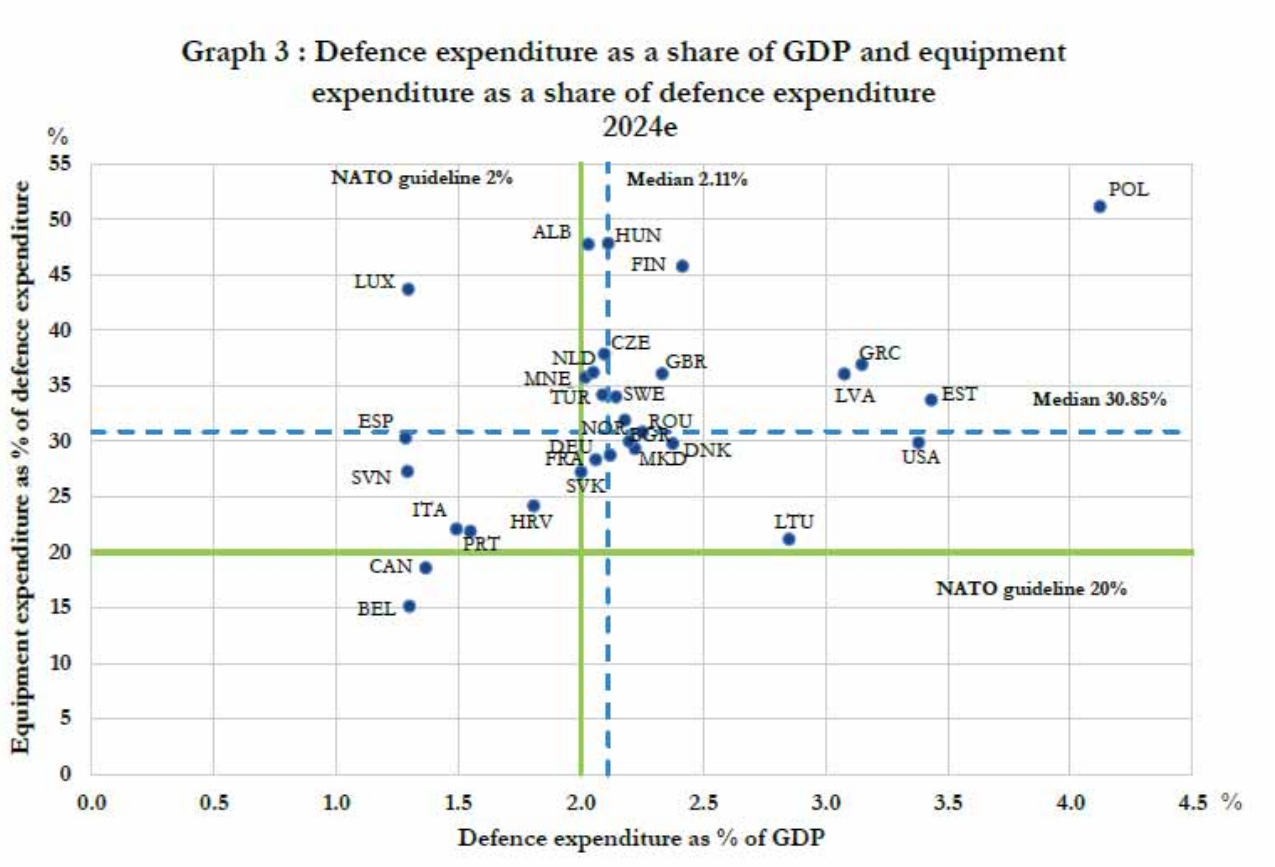
investment in these critical technologies to strengthen interoperability and military advantage.[86] NATO's overarching strategy on critical technologies, outlined in February 2021, focuses on "fostering a coherent approach to the development and adoption of dual-use technologies." Several NATO efforts are underway to enhance innovation cooperation and support this new strategic approach:

- **Defence Innovation Accelerator for the North Atlantic (DIANA)**: Established in 2023, NATO DIANA is a network of 23 accelerators and 182 test centers across the alliance. It assembles end-users and technology innovators to develop impactful dual-use solutions for NATO's most pressing needs. DIANA's first cohort, selected from a competitive process that involved 1,300 applicants, consists of 44 companies from 19 allied nations. Each company is provided with a $100,000 non-dilutive grant, mentorship, test sites, and pathways to market entry. DIANA launched three challenge calls in 2023 and will conduct five calls this year and up to ten in 2025.
- **NATO Innovation Fund (NIF)**: NIF is a standalone venture capital fund, stood up as part of *NATO 2030*, that invests independently across the defense, security, and resilience space. It provides equity funding and lead investment from capital originating from the 24 participating members. Currently, the United States is not a participating member.
- **Centres of Excellence (COE):** The COEs are a NATO-accredited network of organizations which educate and train people from across the 32 NATO members. They identify best practices, assist in doctrine development, and test and evaluate concepts through experimentation on behalf of the alliance. For instance, the MilMed COE has been a foremost source on Tactical Combat Casualty Care (TC3) lessons learned from Ukraine, and the Cooperative Cyber Defence COE is a highly respected source for cyber expertise.

Source: Dursun Aydemir/Anadolu via Getty Images

[86] NATO 2022 Strategic Concept. (2024, March 3). https://www.nato.int/cps/en/natohq/topics_210907.htm

- **NATO Innovation Network (NIN):** NIN is a platform for members to share insights and expertise on defense innovation. It operates as a hub for open military innovation and comprises staff from innovation cells across the alliance.
- **NATO Innovation Board:** The Innovation Board assembles senior leadership within NATO to coordinate innovation efforts and drive practical solutions, particularly in the wake of AI, autonomy, and biotechnology advancements.



Source: Defence Expenditure of NATO Countries (2014-2024), NATO (2024, June 17)

In parallel, the European Union (EU) is actively pursuing a more cohesive, full-throated, and forward-looking approach to defense innovation. Since the war in Ukraine, multiple initiatives have been launched to drive change. The *European Defence Industry Reinforcement Through Common Procurement Act* (EDIRPA) seeks to minimize capability gaps and streamline joint procurement, and the *Act in Support of Ammunition Production* is working to increase munitions production.[87] [88] More comprehensively, the *European Defence Industrial Strategy* (EDIS) lays out a path forward for more integrated European defense research, development, procurement, and sustainment.[89] These EU efforts are still in their infancy, but early signs point to the pursuit of more collaborative defense investment.

[87] European Defence Industry Reinforcement through Common Procurement Act (EDIRPA). Think Tank | European Parliament. (n.d.). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739294
[88] Act in Support of Ammunition Production (ASAP). Think Tank | European Parliament. (n.d.). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)749782
[89] The European Defence Industrial Strategy at a Glance. Defence Industry and Space | European Commission. (n.d.). https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en

To better leverage and enable NATO, the DIB recommends the following:

1. The DoD should convene a temporary innovation taskforce with DIU, USEUCOM, and SACEUR to rapidly develop a NATO multi-domain deterrence system leveraging low-cost surveillance and sensor-shooter networks. This work should pull from recent USCENTCOM and Ukrainian efforts to leverage unmanned systems and AI with operations at land, sea, and air. Experts argue[90] that the first phase of this buildout should focus on integrating a maritime surveillance network for the Baltic, Black, and Mediterranean seas. Subsequent phases should focus on ground force lethality, supplying targeting information to ground units and unmanned aerial vehicles (UAV) with ground attack capabilities, as well as a UAV-based ubiquitous sensing and targeting grid for control in the tri-sea area. These efforts should be capped with a sensing and targeting grid against Russian land forces to round out a modern Air-Land Battle targeting mesh concept. These efforts should be achievable at in a relatively short amount of time and incorporate a network of simple sensors based on commercial technologies.
2. The DoD should work with NATO partners to develop a mechanism, modeled on the private sector and academia, for informing the NATO research and development community about ongoing research projects across the alliance. As it currently stands, duplicative efforts across the alliance are siloed and oftentimes unaware of ongoing parallel work. This structure will avail researchers to more collaboration but maintain competitive opportunities while minimizing risk and duplication.
3. The DoD should appropriately fund the NIF and embrace it alongside NATO DIANA as a key developmental effort for the European defense ecosystem. Currently, 24 NATO members are investors in NIF's Subfund 1; the United States is not one of them.[91] So long as the United States is not a NIF participant, U.S. investors will not be able to support funded start-ups and contribute their voluminous capital and expertise to the NATO innovation community. While the U.S. start-up and investing ecosystem is already robust, this leaves money on the table and represents a lost opportunity for enhanced NATO collaboration. Faced with concerns that U.S. private capital would simply shift to competing industry in Europe, the DoD could consider a new sub-fund that focuses on specific rapid technology acquisition and adoption efforts nested with U.S. strategic priorities, e.g., low-cost surveillance and sensor-shooter networks (Replicator).[92]
4. The DoD should lead the development of a NATO AI and machine learning taskforce and centre of excellence to address responsible use and adoption of autonomous capabilities. Currently, NATO's centre of excellence network does not include a focus on AI and autonomy, representing a significant gap in a high-priority technology area and a missed opportunity for identifying early wins in a critical domain. This new centre of excellence should include the United Kingdom and Australia as observer nations to ensure that collaborative efforts and algorithmic advances are shared across NATO and AUKUS.
5. The DoD should work with NATO to establish "special innovation zones" in high-potential areas. As highlighted above, these zones could feature relaxed regulatory controls and

[90] Kramer, F., Dailey, A. M., & Brodfuehrer, J. (2024, March 1). NATO Multidomain Operations: Near- and Medium-Term Priority Initiatives. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/

[91] NATO Innovation Fund closes on EUR 1BN Flagship Fund. NATO. (2023, August 1). https://www.nato.int/cps/en/natohq/news_217864.htm

[92] DIB interview with ally/partner stakeholder (2024, March 27)

act as central hubs for research. Specifically, the Baltics represent a primary opportunity for testing this framework. They have existing close working relationships and punch above their weight in digitization, cybersecurity, and start-up culture.[93] Properly constructed, these zones could bolster innovation economies of scale across smaller nations and be used as platforms for strengthened NATO defense research collaboration.

6. The DoD should conduct a review of the NATO centres of excellence to identify key nodes of best practices and lessons learned, and to better understand where the DoD and NATO counterparts elicit value from these centres. For example, we heard anecdotally that the NATO MilMed COE has been an integral source of best practices and lessons learned in Tactical Combat Casualty Care (TC3) from Ukraine, but has seen limited engagement from the DoD.[94] A full review would help leverage these centres to ensure NATO warfighting excellence is maintained, particularly as the Ukraine war continues to reveal lessons for NATO in a wide range of areas such as sensing, communications, command and control and fires, unmanned aerial vehicles, and cyber resilience.
7. The DoD should track NATO members' '20 percent investments' to resource modernization goals across the alliance. NATO members are required by their 2014 and 2023 *Defense Investment Pledges* to appropriate at least 20 percent of their defense outlays for major new equipment, including research and development.[95] The additional 20 percent pledge, though not as closely watched as the 2 percent requirement, is critical for NATO modernization and interoperability.
8. The DoD should collaborate with NATO to establish a cybersecurity and critical infrastructure surge capability. Building on lessons learned from the Ukrainian response to Russian targeting of critical infrastructure, NATO and the DoD must leverage increased engagement from private sector experts. Housed within NATO, this surge capability should formalize a network of private sector critical infrastructure experts (e.g., cybersecurity, water supply, electrical grid) willing and able to respond in the event of conflict-caused service disruptions.
9. Work with the Department of State to develop parallel ITAR regulatory changes for NATO similar to those for AUKUS as ratified in Section 1343 of the FY2024 NDAA.

Exhibit 10. Ukraine Recommendations

Ukraine's battlefield successes have been undergirded by the conversion and integration of readily available commercial technologies into military capabilities, a model of rapid capability development powered by direct interaction between forward-deployed programmers, engineers, and project managers, and military operators. This model is sustained by volunteers and start-ups and funded by private sources. However, this important grassroots approach, while effective precisely owing to a lack of government capacity and red tape, is difficult to scale at the national level and can be opaque to foreign partners, thus limiting the potential for international cooperation.[96]

While Brave1 has done yeoman's work to develop the Ukrainian defense innovation ecosystem, promoting international contacts and expediting aspects of the national defense procurement process, the Ukrainian Ministry of Defense (MoD) and General Staff (GS) lack a coherent approach to rapid capability development. Challenges such as persistent enemy surveillance by Russian Orlan and ZALA drones are not systematically analyzed. Efforts across the defense

[93] DIB interview with ally/partner stakeholder (2024, March 27)
[94] DIB interview with national security expert (2024, April 19)
[95] Funding NATO. NATO. (2023, July 31). https://www.nato.int/cps/en/natohq/topics_67655.htm
[96] DIB engagement with Ukrainian defense innovation leaders (2024, June 14)

enterprise to develop solutions are poorly resourced and not coordinated. Coherent requirements, challenges, and demand signals are not well-communicated to industry or foreign partners. In addition, the Ukraine Defense Contact Group (UDCG) drone and IT capability coalitions have been deprioritized by the MoD/GS, in favor of capability coalitions addressing major platforms such as armor, artillery, and ammunition.[97] This prioritization reflects the urgent need for major platforms, but also reflects the lack of capacity within the MoD/GS to articulate and lead a rapid capability development process. To address this imminent challenge:

1. The DoD should make it a policy to cooperate with Ukraine on rapid capability development and communicate this policy to the Ukrainian defense leadership. The MoD/GS will not focus on this topic unless they understand that it is a U.S. priority.
2. The DoD should launch defense and technology capacity-building projects that help Ukraine develop the personnel, IT, and equipment necessary to rapidly develop and field capabilities. DoD representatives should be current practitioners, well-versed in cutting-edge technology, capable of illustrating best practices to Ukrainian counterparts and properly understanding lessons learned relevant to the DoD. These projects should not be managed by retired Foreign Area Officers bearing PowerPoint presentations on PPBE and JCIDS processes. Relevant domains of focus should include: 1) operations analysis, 2) technology scouting, 3) modelling and simulation, 4) testing and evaluation, and 5) lessons learned. Foreign partners providing grants to Ukrainian NGOs to deliver defense capacity building programs is a well-established practice, with nations such as Canada, the United Kingdom, and Norway actively utilizing such structures.
3. The DoD should leverage capabilities not requiring in-country presence, to include remote consultations, remote mentoring, and access to modeling and simulation software (e.g., Advanced Framework for Simulation, Integration, and Modeling (AFSIM)) to assist rapid capability development projects in Ukraine.

The DoD should collaborate with Ukraine to support targeted rapid capability development programs (similar to Replicator). These can be a source for rapidly scaling successful defense innovation across the Ukrainian Armed Forces, adopting successful innovations within the DoD, and more holistically understanding frequent but disparate defense innovations occurring in Ukraine.

NATO remains unmatched for its military power and innovative potential. Proper integration of resources and elimination of the numerous barriers to collaboration described above is of the utmost importance. The suggested USD(IIC) can drive innovation within the alliance framework and utilize these recommendations to make meaningful changes in this space. Through continued evolution, NATO will remain a source of power and innovative dynamism.

Source: Voice of America

[97] DIB engagement with Ukrainian defense innovation leaders (2024, June 14)

G) Indo-Pacific

As the DoD's priority theater, and an integral source of economic prosperity, technological development, and military capability, the Indo-Pacific is an increasingly essential hub for co-innovation. Despite this, outside of AUKUS, the DoD is not adequately integrating key allies and partners, thereby leaving significant resources and capabilities underutilized. Early efforts, such as GMLRS co-production in Australia, are encouraging indications of greater integration, but remain nascent.[98] Integrating emerging partners into its collaborative innovation network should be a top priority for the DoD and for the DIB's proposed USD(IIC).

Unlike Europe, the Indo-Pacific theater brings unique, pacing challenges which are largely avoided in the NATO space. There is a lack of historical interoperability between the various nations, the tyranny of distance creates numerous fundamental barriers, and the lack of a shared language and cultural background makes communication more time-consuming and difficult.

Exhibit 11. The Quad and INDUS-X

Through the Quadrilateral Security Dialogue (Quad) with Australia, Japan, and India, the United States has supported a working group on critical and emerging technologies, focusing on next-generation wireless connectivity, undersea cable infrastructure, and technology standards-development. Through the Quad, the United States also launched the Indo-Pacific Partnership for Maritime Domain Awareness (IPMDA) to bring advanced satellite-based radio frequency data to the region.[99] The Quad Investors Network (QUIN), a public-private effort established by a group of investors and technologists from across the four Quad nations, held its inaugural Quad Investment and Technology Dialogue in October 2023 focusing on strategies for unlocking private capital to foster co-investment in critical technologies and supply chain resilience.[100] Subsequently, in November 2023, the United States hosted the Quad Technology, Business, and Investment Forum on the sidelines of the San Francisco APEC Summit.[101] The Quad has also promoted annual fellowships for graduate students in STEM and infrastructure programs.

Source: AP Photos

The United States is also elevating India's role as a regional leader utilizing the India-U.S. Defense Acceleration Ecosystem (INDUS-X), launched in June 2023, as a mechanism for building a defense innovation bridge to India.[102] Initially focused on maritime intelligence, surveillance, and reconnaissance, INDUS-X has been paired with a wide-ranging bilateral effort on strategic technology and defense industrial issues.

---

[98] Clark, C. (2023, July 31). Aussies, US agree to joint Intel Center, co-production of GMLRS. Breaking Defense. https://breakingdefense.com/2023/07/aussies-us-agree-to-joint-intel-center-co-production-of-gmlrs/

[99] A Work in Progress: The Indo-Pacific Partnership for Maritime Domain Awareness. Pacific Forum. (2023, June 23). https://pacforum.org/publications/pacnet-48-a-work-in-progress-the-indo-pacific-partnership-for-maritime-domain-awareness/

[100] QUIN Holds Inaugural Quad Investment and Technology Dialogue. Quad Investors Network. (2023, October 20). https://quadinvestorsnetwork.org/news/quin-holds-inaugural-quad-investment-and-technology-dialogue

[101] SCSP Hosts Quad Technology, Business, and Investment Forum. (2023, November 15). Retrieved June 27, 2024, from https://www.scsp.ai/2023/11/scsp-hosts-quad-technology-business-and-investment-forum/.

[102] Launch of the India-U.S. Defense Acceleration Ecosystem (INDUS-X). USINDOPACOM. (2023, June 22). Retrieved June 27, 2024, from https://www.pacom.mil/JTF-Micronesia/Article/3436228/launch-of-the-india-us-defense-acceleration-ecosystem-indus-x/.

To appropriately address barriers and seize key opportunities within the Indo-Pacific theater, the DIB recommends the following:

1. The DoD should convene a temporary innovation taskforce with DIU, USINDOPACOM, the AUKUS countries, and potentially Japan, ROK, and the Philippines, to rapidly develop an Indo-Pacific deterrence system leveraging low-cost surveillance and sensor-shooter networks. Like the similar recommendation for a NATO system, this work should pull from recent lessons learned in Ukraine and the Middle East regarding the use of unmanned systems and AI in multi-domain operations. The objective of this taskforce should be to develop asymmetric concepts and technologies in response to People's Liberation Army (PLA) advances in short- and medium-range ballistic missiles and Chinese mainland air defenses. The taskforce should maximize U.S. advantages in the event that the PLA deploys a large-scale invasion force transiting the Taiwan Strait in a complex amphibious operation. These efforts should be achievable in a relatively short amount of time and align to the effort of Taiwan's new Defense Innovation Unit to invest in mature low-cost capabilities such as unmanned aerial and maritime vehicles and counter-drone systems.

Exhibit 12. Taiwan

Taiwan receives significant defense support from the United States in accordance with longstanding diplomatic protocol based on the Taiwan Relations Act, three communiques, and six assurances. This support arrives mostly in the form of transfers of substantial advanced military equipment, including fighter jets, missiles, naval vessels, and other defense articles. There has been a concerted effort since the Bush Sr. and Clinton administrations to enhance military-to-military relations, increasing the contact surface between the U.S. and Taiwanese defense establishments to strengthen trust and interoperability. There is broad recognition that a major conflict in the Taiwan Strait would result in thousands of casualties and jeopardize trillions of dollars in global economic activity. None would be hurt worse by the resultant economic depression than China itself. To deter and, if necessary, respond to this scenario, Taiwan is working to enhance its military capabilities and foster innovation in its defense sector.

Taiwan's Ministry of National Defense (MND) recently announced plans to create a Defense Innovation Unit resembling the U.S. entity of the same name. Its goal is to integrate research on military and civilian defense technologies in order to foster greater momentum and innovation in the commercial defense sector. Inspired also by DARPA, Taiwan's DIU aims to facilitate the adoption of emerging technologies by bolstering collaboration between academia, industry, and government.[103] The new DIU may aim to combine resources and capabilities from the National Chung-Shan Institute of Science and Technology (NCSIST). To support this build-up, Taiwan has grown its defense budget since 2017 at an average annual rate of 5 percent between 2019 and 2023. Its latest defense budget reaches approximately 2.6 percent of GDP.[104] The DoD should consider new and innovative ways of supporting Taiwan's efforts to build a globally engaged defense innovation ecosystem and defense industrial base aligned to regional security goals.

[103] Yu, M., & Yeh, J. (2024, June 3). Taiwan to form Defense Innovation Unit: New defense chief. Focus Taiwan - CNA English News. https://focustaiwan.tw/politics/202406030005
[104] Dotson, J. (2023, September 21). Taiwan Announces an Increased Defense Budget for 2024. Global Taiwan Institute. https://globaltaiwan.org/2023/09/taiwan-announces-an-increased-defense-budget-for-2024/

2. The DoD should conduct a proper Indo-Pacific capability mapping such that defense modernization goals can be properly tracked and resourced across the region's allies and partners. On the sidelines of the recent Shangri-La Dialogue, the United States and 10 countries endorsed a new *Statement of Principles for Indo-Pacific Defense Industrial Base Cooperation*.[105] The statement, initially co-signed by Japan, Australia, ROK, the Philippines, New Zealand, and Canada – as well as NATO partners including Sweden, Italy, Germany, and the Netherlands – seeks to devise new solutions for common defense industrial challenges, to enhance standardization, reduce redundancy, improve interoperability, and promote co-development and co-production of fundamental, lower-end capabilities for the allied and partner nation warfighter. A classified DoD review of capabilities across these and other countries, such as India, would help operationalize this statement of principles by identifying common problems and an initial tranche of potential capability integration projects.
3. The DoD should adopt a special operations forces (SOF) doctrine among Indo-Pacific allies similar to NATO SOF Headquarters' Allied Joint Publication (AJP)-3.5, *Allied Joint Doctrine for Special Operations*. Released in 2013, AJP-3.5 was NATO SOF's first published doctrine, now used by at least 47 countries across NATO and Europe. The Secretary of Defense should instruct USINDOPACOM to develop similar doctrinal guidance for conducting joint special operations with Indo-Pacific allies across the spectrum of conflict.
4. With Japan and ROK, the DoD should launch a series of co-development, co-production, and co-sustainment projects on a fully 50-50 basis. With Japan, the DoD has begun to build momentum on this front with its inaugural Defense Industrial Cooperation, Acquisition, and Sustainment (DICAS) Forum in June 2024.[106] The outcomes from that meeting – a concurrence of principles for defense industrial cooperation and the launch of working groups focused on missile co-production, navy and air force co-sustainment, and supply chain resiliency – are important for setting table-stakes. The three working groups should move rapidly to launch their projects, not on a months-long basis, but on a timescale of weeks. The groups should set short-term targets to ensure that the DICAS can meaningfully boost production for shared challenges in the Indo-Pacific and beyond. The DoD should establish a parallel DICAS with the ROK as our other priority defense industrial partner in the Indo-Pacific. These DICAS fora should also send emissaries to the INDUS-X convenings to ensure that partners are sharing best practices for future co-innovation.
5. The DoD should sign Reciprocal Defense Procurement Memorandum of Understanding (RDP MoU) agreements with the ROK, Philippines, and India soonest. Historically, RDP MoUs have predominantly targeted the European theater, but further expansion to the Indo-Pacific is a key step in demonstrating the DoD's commitment to its priority theater. The absence of such agreements harms defense procurement, weakens supply chains, and diminishes the military capabilities of these countries. Effectively integrating these key regional allies and partners will ensure more robust regional supply chains, grow regional cooperation, and enhance regional stability. The DoD should also prioritize these

[105] Vergun, D. (2024, June 3). Austin: Boosting military-industrial bases with Indo-Pacific nations a priority. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3794031/austin-boosting-military-industrial-bases-with-indo-pacific-nations-a-priority/

[106] Global Partners for the Future. The White House. (2024, April 10). https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/10/united-states-japan-joint-leaders-statement/

countries for future Security of Supply Arrangements (SOSA).

6. The DoD should conduct regular annual or biennial reviews of industrial security standards and data-sharing protocols in Japan, ROK, the Philippines, and other close regional allies. As these countries upgrade their industrial security standards, security clearance systems, and cybersecurity practices, the DoD should update its policies regarding technology sharing with these countries. Otherwise, the DoD may miss opportunities to collaborate with these countries on capability integration and to bring them into the fold more fulsomely.
7. The DoD should launch a quadrilateral shipbuilding initiative with Japan, ROK, and the Philippines. The U.S. Navy has expressed interest in utilizing commercial shipyards in Japan and ROK for sustainment of forward-deployed forces.[107] Those countries also possess some of the world's most advanced digital engineering technologies for shipbuilding. The Philippines, meanwhile, rests on a strategic maritime corridor overlooking Taiwan and the South China Sea, and is home to critical shipyards in Subic Bay. In 2022, U.S. private equity firm Cerberus acquired Subic Bay Freeport, a former U.S. naval base, amid national security concerns that the shipyard would be taken over by Chinese state-backed firms.[108] However, the strategically situated shipyard now sits mostly vacant, and recently Cerberus leased part of the shipyard to a Korean firm for building offshore wind platforms. The now private and mostly dormant facility presents a unique opportunity to build something new and innovative that rebuilds U.S. Navy shipyard capacity in partnership with a consortium of Japanese, Korean, and Filipino shipbuilders and other advanced manufacturing companies. This new four-nation effort, like the existing Quad, should be shaped at the leader-level to ensure that domestic political, regulatory, and technical hurdles across all participating nations do not hinder implementation.
8. The DoD, in collaboration with the Departments of State and Commerce, should model U.S. Embassy Seoul's Joint U.S. Military Affairs Group-Korea (JUSMAG-K), which is the embassy's SCO responsible for U.S.-ROK defense trade. Unique among SCOs, JUSMAG-K maintains close coordination with a combined forces command structure, a legacy of the Korean War, and sits directly under the U.S. Ambassador while reporting to USINDOPACOM through its military chain of command. In addition, JUSMAG-K boasts a strong working relationship with the embassy's commercial section, which is staffed by commercial service officers who have worked at the DoD and understand the defense acquisition bureaucracy.[109] This unique formulation integrating the diplomatic, commercial, and defense considerations necessary to manage complex multinational defense innovation and production should be replicated at other important allied capitols in the region and around the world. Recognized as a best practice in our study, U.S. Embassy Seoul's approach offers valuable insights that could benefit U.S. embassies elsewhere as DSCA builds out its Defense Security Cooperation Service.
9. The DoD should invest in innovation talent corridors that create fully immersive experiences to develop stronger defense innovation and civil-military communities with key Indo-Pacific allies and partners. In the vast cultural expanse of the Indo-Pacific, especially, in order to build force

[107] Moriyasu, K. (2024, March 3). U.S. Seeks to Revive Idled Shipyards with Help of Japan, South Korea. Nikkei Asia. https://asia.nikkei.com/Politics/Defense/U.S.-seeks-to-revive-idled-shipyards-with-help-of-Japan-South-Korea

[108] Morales, N. J. (2022, March 8). Cerberus to Buy Philippine Shipyard at Ex-U.S. Navy base for $300 Million. Reuters. https://www.reuters.com/business/cerberus-buy-philippine-shipyard-ex-us-navy-base-300-mln-sources-2022-03-08/

[109] DIB interview with interagency partner (2024, March 14)

interoperability and cohesion, persistent and immersive cross-cultural exchanges are necessary to establish trusted, informal networks and cultural empathy at lower force levels. Full-immersion training programs can bolster cultural intelligence, informal networks, and mindset adaptability. These networks can also strengthen cross-cultural ties between innovators in the United States and elsewhere, thereby supporting efforts among allies and partners that seek to convene international civil and military technology experts, such as Japan's forthcoming research institute modeled on DARPA and DIU.[110]

[110] Shimbun, Y. (2024, February 25). Japan Plans Defense Tech Innovation Body with 100 Staffers; Institute Modeled on Foreign Examples Like DARPA, DIU. The Japan News. https://japannews.yomiuri.co.jp/politics/defense-security/20240224-170847/

Conclusion

Despite top-level strategic guidance to embrace allies and partners, the DoD has yet to fully dispense with its Cold War-era approach to technology security, export controls, and innovation collaboration. Numerous reform efforts have been undertaken, and have faltered, with most resulting changes occurring at the margins.

Today, technology development is rapidly outpacing U.S. decision-making abilities, underscoring the imperative of more mutually collaborative efforts with allies and partners that better integrate the DoD within this global network. While there is broad support within the DoD for this maxim, the tangled web of inhibiting regulations, compliance requirements, and entrenched cultural norms listed above continually stymie these efforts. Proper integration and preparation with allies and partners cannot be a formality, it must be treated as a critical first step in ensuring preparedness to deter and fight future conflicts.

This report attempts to meaningfully address that reality. Central to our proposed recommendations is a singular, basic truth that the DoD is failing to embrace: the core threat the United States faces today is no longer the potential spillage of information or overzealous sharing of technology, it is that on day-one of a conflict U.S. warfighters will be poorly integrated with allies and partners, underequipped with the most advanced capabilities wherever they originate, and therefore at greater risk of defeat.