



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Winning the Future Together:

Evolving Cooperative Security Approaches for Tomorrow's Realities

John Watts





SCOWCROFT CENTER FOR STRATEGY AND SECURITY

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Forward Defense (FD), housed within the Scowcroft Center, generates ideas and connects stakeholders in the defense ecosystem to promote an enduring military advantage for the United States, its allies, and partners. Our work identifies the defense strategies, capabilities, and resources the United States needs to deter and, if necessary, prevail in future conflict.



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Winning the Future Together:

Evolving Cooperative Security Approaches for Tomorrow's Realities

John Watts

Cover: Japanese and Indian naval members touring the guided missile cruiser USS Princeton, 2017. *Source:* Navy Petty Officer 3rd Class Kelsey J. Hockenberger

ISBN-13: 978-1-61977-298-4

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

December 2023

Table of Contents

Introduction	1
Defining Key Security Cooperation Terminology	2
The Modern Threat Landscape: What it Means for Security Cooperation	4
Challenges to Twenty-First Century Security Cooperation	6
The Path Ahead	8
Conclusion and Recommendations	14
About the Author	15
Acknowledgements	16

Introduction

The United States should adapt its approach to security cooperation to ensure allies and partners are more highly capable, stable, and resilient in an era of great power competition. US security cooperation, which are military aid activities led or executed by the US Department of Defense, is immensely valuable if done right and can help the United States achieve its goal from the 2022 National Security Strategy (NSS) by building a strong coalition of allies to confront shared challenges.

The last decade has seen rapid and profound changes in geopolitical realities, technological developments, and US and allied concepts for both what national security objectives should be and how to achieve them. This has had broad implications for all facets of military operations and planning, and the security cooperation enterprise is no exception. While the US Department of Defense's approach

to security cooperation has been evolving and improving over the same period, lessons learned from recent conflicts—along with shifts in the geopolitical context—point to the need for a deeper re-conceptualization of generating high-end cooperative security.

This paper reframes elements of US security cooperation, particularly with the United States' most capable allies and partners, and proposes small but realistic reforms that could improve the value and utility of US security cooperation activities. In many cases, those responsible for addressing these issues are already taking steps in this direction; still, it is critical to amplify, draw attention to, and reinforce the arguments in favor of these efforts. This paper draws upon discussions and workshops with experts from across the vast security cooperation enterprise, including participation from US and allied industry, academia, and government entities.

Defining Key Security Cooperation Terminology

In simplistic terms, military aid is an extension of diplomatic efforts, and most of these efforts are led by the Department of State and categorized as *security assistance*. Military aid activities that are led or executed by the Department of Defense (DOD) are broadly categorized as *security cooperation* and can range from the provision of training and equipment, to embedded advisors, joint exercises, meetings between senior leaders, and even forms of humanitarian assistance and disaster response (HA/DR) undertaken by military units.¹

While conversations around security cooperation tend to narrowly focus on “train and equip” objectives, doing so ignores the vast array of other incredibly important security cooperation activities—such as key leader engagements (KLE), institutional capacity building through the Ministry of Defense Advisor (MODA) program, and professional development courses—which build the capacity and capability of less advanced US allies and partners in more indirect ways, and arguably have greater potential return on investment (ROI) than traditional, systems-oriented security cooperation activities. These activities are not just about the cost vs impact, however, as they are often critical enablers for all systems-based cooperation. No amount of military-to-military cooperation or interoperability can be effective if the foundation of institutional conditions is missing. For example, Ukraine’s success in absorbing and employing vast amounts of Western military aid is built upon institutional capacity-building investments made over the last decade. Nontraditional and nonmilitary approaches to security cooperation will only become more critical as the proliferation of new technologies expand the battlespace to include the space, cyber, Arctic, and information domains. Moreover, many of the most pressing security threats fall outside the military domain completely, such as the risks posed by economic instability, competition for influence and trust-worthy information and a changing climate.

Security cooperation activities are national geopolitical tools that are employed by the DOD on behalf of the US government to achieve national and defense objectives. Although it is called aid, it is not charity. These activities

are meant to bolster US national security, and often in a cost-effective way. They are a means to achieving geopolitical and national security objectives. Even so, the sovereignty of US allies and partners is important and they must always have the final say in what and how they build and deploy their military capabilities, regardless of how they are sourced. What makes the US-led alliance network so powerful is that, unlike its competitors, the United States sees global security and prosperity—enabled by a rules-based-order that protects nations small and large—as in its core interest.

Differentiating Between the Types of Cooperative Security Partners and Approaches

Security cooperation means and ends vary by nation and region. The diversity of partner nations means that US security cooperation objectives and activities with each country are similarly diverse to match the partner’s capacity, size, level of training, and funding. As the objectives differ, so, too, should the basis and metrics for evaluating the effectiveness and therefore the value of different security cooperation activity. For instance, military aid that is used as a package to achieve political concessions will look distinct from that used to assist nations in maintaining internal security, responding to natural disasters, or protecting themselves against a foreign aggressor. The objectives of each US security cooperation activity should be policy-led, and have a clear articulation of the objective, why it is being sought, and how success will be measured. Unfortunately, this has not historically been the case. In 2017, the National Defense Authorization Act (NDAA) included reforms around security cooperation to improve DOD’s approach to this issue. Despite this, change is happening slowly and unevenly, and there is still a lack of understanding of the value and objectives of different types of security cooperation activities and how they apply to different categories of allies and partners.²

This paper focuses in on two specific categories of US allies and partners as described in the short-lived Guidance

1 Security assistance can, for instance, involve aid and support to police and other non-military security forces. In contrast, DOD security cooperation activities almost exclusively involve another formal foreign military and can cover almost any DOD interaction with that partner to build military- or security-related capacity, or achieve military or security interests. The scope and scale of activities considered to fall under the security cooperation umbrella is quite broad, and often overlapping with State Department-led security assistance activities. Foreign Military Sales (FMS), for instance, is approved and led by State, but executed by the DOD.

2 Bilal Y. Saab, “Security cooperation deserves a fair evaluation,” War on the Rocks, May 2, 2023, <https://warontherocks.com/2023/05/u-s-security-cooperation-deserves-a-fair-evaluation/>.



President Biden meets with military and civilian defense leaders at the White House, including Secretary of Defense Austin and Chairman of the Joint Chiefs of Staff Gen. Milley, 2022. Source: Lisa Ferdinando

for the Development of Allies and Partners (GDAP). First, “most capable” partners encompassing advanced militaries with some near-peer capabilities (e.g., the United Kingdom and Japan) and, second, “frontline” nations facing potential aggression and direct threat (e.g., Ukraine and Iraq). In both categories, the US aim is to build the military capacity and capability³ of an allied or partner nation to

fight alongside the United States in combined operations. In certain circumstances, this is done by supporting partner forces to undertake contingency operations on their own without US presence, being enabled by US forces, or utilizing US authorities and agreements (also known as the “by, with, and through” strategy)—thereby reducing the requirement for direct action by US forces themselves.⁴

3 A military capability is the sum total of inputs required to generate a desired military effect in an operational context—i.e., *what* function can a military force successfully complete (e.g. the ability to undertake armored operations, intercept enemy missiles, or move personnel or supplies via air). These ‘inputs’ include everything needed to undertake that function – the personnel, training, logistics, infrastructure, operating concepts, enabling systems, and the equipment itself. Capacity, on the other hand, is the quantity of a capability that a military force can generate and employ—i.e., *how much* of that function can it undertake.

4 Joseph L. Votel and Eero R. Keravuori, *The By-With-Through Operational Approach*, 2018, National Defense University, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89_40-47_Votel-Keravuori.pdf?ver=2018-04-11-125441-307.

The Modern Threat Landscape: What it Means for Security Cooperation

Like all facets of military operations, security cooperation should be strategy-driven and therefore threat-informed—the threat environment has changed, and so, too, must security cooperation. During the post-Cold War era, when there were few clear and present threats and Russia was the primary adversary, US security cooperation activities promoted presence, dependability, and engagement across the globe. Following the 9/11 attacks, US security cooperation activities shifted toward capacity-building to support counterterrorism and counterinsurgency operations largely in the middle east, still with few limits as to where and with whom. Now, as the United States refocuses its efforts in an era of strategic competition with China and Russia, it must similarly reimagine and broaden its approach to security cooperation. All elements of US national power should be mobilized and coordinated to achieve stated objectives. While US practitioners recognize the need to evolve, the US defense enterprise is not changing quickly enough and at a scale large enough to meet the magnitude of the threats at hand. Particularly, the security cooperation enterprise must evolve to prioritize those partners who play a critical or central role in achieving specific objectives and recognize the impact of emerging and advanced technologies.

Prioritization of Partnerships

Today's strategic environment is characterized by pervasive contestation with near-peer competitors across multiple domains, and prioritization of efforts to tackle these challenges has become imperative. The United States and its allies and partners can no longer do a little bit of everything, everywhere and expect uncontested results. As highlighted in the 2022 National Defense Strategy (NDS), the United States will need to accept risk in some areas and strategically expend its limited resources where they will have the greatest effect. In doing so, the United States must be realistic about which allies and partners could (and would) undertake military actions alongside the United

States in a high-end, conventional contingency.⁵ In the likely case that only a few partners are willing or capable of undertaking frontline roles in a high-end fight, the United States ought to rethink what capabilities they require to play an effective role—which, in many cases, will mean a larger quantity of second-tier or legacy capabilities such as F-16s or simpler 3rd party capabilities such as Leopard 2 tanks rather than a handful of the most advanced and cutting-edge systems like F-35s and Abrams tanks. DOD's GDAP guidance provided a helpful starting point for letting the roles of allies and partners guide capability and capacity decisions in security cooperation. However, changes in the strategic landscape have altered the roles of allies and partners, which necessitated a reframing of the security cooperation focus with them. If the United States is realistic about the roles allies and partners play in each region and in relation to US national objectives, then US priorities and therefore its acceptance of risk in certain regions or nations, may change. This discussion is not receiving proper attention in Washington, DC or elsewhere, least of all in the public domain.

Emerging and Advanced Technologies

Advancements in military technology, and the subsequent changes in the way conflicts are being fought, have further implications for the roles of allies and partners and the capabilities and capacities the United States seeks to build through security cooperation. This is most evident from the war in Ukraine and the role security cooperation played in assisting Kyiv. Ukraine, a smaller and less technologically advanced military force, can—when sufficiently supplied, trained, and motivated—impose significant losses on Russia, a larger and more sophisticated force (supposedly the world's third most advanced and capable), using a combination of legacy and 'second tier'⁶ equipment, supplemented with some key 'tier 1' capabilities and an array of cheaper alternatively sourced systems (such as the highly effective Turkish made Bayraktar TB2.⁷) The value

5 Dave Lawler, Han Chen, and Bethany Allen-Ebrahimiyan, "U.S. allies could play key roles in a U.S.-China war over Taiwan," *Axios*, May 2, 2023, <https://www.axios.com/2023/05/02/taiwan-war-us-philippines-japan-korea-australia>.

6 "Tier 1 reflects systems across the different functional areas that a major military force with state-of-the-art technology would generally have. At Tier 1, new or upgraded systems are limited to those robust systems fielded in military forces or currently developed and marketed for sale, with capabilities and vulnerabilities that can be portrayed for training. Tier 2 reflects modern competitive systems fielded in significant numbers for the last 10 to 20 years, with limitations or vulnerabilities being diminished by available upgrades. Although forces are equipped for operations in all terrains and can fight day and night, their capability in range and speed for several key systems may be somewhat inferior to U.S. capability." OE Data Integration Network, "Worldwide equipment guide," https://odin.tradoc.army.mil/How-To/WEG/Worldwide_Equipment_Guide.

7 Stephen Witt, "The Turkish drone that changed the nature of warfare," *New Yorker*, May 2022, <https://www.newyorker.com/magazine/2022/05/16/the-turkish-drone-that-changed-the-nature-of-warfare>.



A Polish Leopard 2 Tank is covered by US paratroopers during a combined training exercise in Poland, 2022. *Source:* Army Sgt. Garrett Ty Whitfield

and force multiplier effect of even a handful of exquisite weapons systems, particularly the HIMARs rocket launchers, when combined with a larger quantity of older legacy systems, and when employed with appropriate operational concepts and planning, can have a dramatic impact. Additionally, Ukraine's ability to absorb massive amounts advanced Western designed systems into a force not oriented to operate them demonstrates both how important those high-end systems remain and suggest the need for a rethinking of a military force's real-world absorptive capacity under the right conditions. That said, the difficulty

Ukraine has faced in achieving decisive gains during its counter offensive—even when equipped with high-end Western capabilities—demonstrate how challenging high-end military maneuver is for offense now, and that recent technological developments have shifted the balance back towards a natural advantage in defense. For security cooperation purposes, this means a first principles reassessment is needed of each ally and partner—not only of the role the United States wants a partner to play, but also a rethinking of the tools and systems needed to achieve the necessary capability to fulfill it.

Challenges to Twenty-First Century Security Cooperation

While the war in Ukraine, as well as other historical cases, have demonstrated the impact of security cooperation on a nation's ability to fight, it has also highlighted key challenges facing the security cooperation enterprise.

First, the conflict in Ukraine has both exposed and exacerbated the NATO alliance's insufficient industrial capacity for weapons⁸ and ammunition production to sustain a protracted high-end conflict. The United States and its allies have supplied incredible amounts⁹ of equipment and ammunition to Ukraine at the expense of drawing down their domestic stocks in some cases—which will likely take years to replace.¹⁰ Putting aside the impact this has on the United States' readiness and ability to execute other military contingencies in the short term, it is unclear how well it could sustain itself in a more costly protracted conflict in which the United States were a direct combatant—let alone also supplying critical allies. As it stands, there are already promises of equipment and ammunition that are unfulfilled.¹¹ Allies and partners cannot fight with weapons they do not have, and the United States cannot provide what it cannot produce. Moreover, the challenge for both sides in the conflict in finding personnel and equipment necessary to generate combat power raises questions about the sustainability of any nation in supporting a protracted high-end fight.

Second, expansive arsenals of weapons are of little utility if there is not political will to participate in the conflict. Take, for instance, the opening stages of international efforts to establish a no-fly zone over Libya during its 2011 civil war. European militaries not only struggled with insufficient stocks of advanced precision air munitions¹² to undertake sustained airstrikes on their own, but also struggled to build a widespread coalition of willing partners. This was despite

several European nations being strong proponents of the intervention. In reality, the United States employed much of the military capability—particularly at the outset and once ammunition supplies ran low—because partners either lacked key capabilities or the sufficient risk appetite to put the capabilities they did have in danger against what was then the second largest, if aged and limited,¹³ surface-to-missile network in Africa.¹⁴ While European nations have been steadfast supporters of Ukraine, and have now overtaken the US in absolute terms of aid provided.¹⁵ However, against a more advanced defense, with higher political stakes, and in more importantly where it occurs in regions distant from those nation's immediate interests,¹⁶ it is difficult to predict how many allied and partner nations will commit significant forces in a high-end fight. This ought to inform the level of cooperative security resources allocated across allies and partners.

Third, while the United States and its allies and partners aspire to reach a level of interoperability with one another, balancing this with cost and capacity creates a challenging conundrum. Interoperability is often a defining characteristic of train and equip efforts, encompassing a spectrum of functions from interoperable communications systems to enable deconfliction of actions, through to crews of different nations serving together on other nations systems (at its most exquisite and aspirational), as has been suggested in the recent submarine-focused elements of the AUKUS agreement between Australia, the United Kingdom, and the United States. The challenge is that US equipment is often too expensive for many partners to acquire in sufficient numbers, which leads them to look for cheaper alternatives from other—and sometimes adversarial—suppliers. As warfare becomes increasingly networked and data-driven (i.e., software- rather than hardware-driven), systems whether from the United States or another country,

8 Thomas S. Warrick, "The arsenal of democracy has hit a snag. Congress needs to step in." Atlantic Council, February 24, 2023, <https://www.atlanticcouncil.org/blogs/new-atlanticist/the-arsenal-of-democracy-has-hit-a-snag-congress-needs-to-step-in/>.

9 Jonathan Masters and Will Merrow, "How much aid has the U.S. sent Ukraine? Here are six charts.", Council on Foreign Relations, February 22, 2023, <https://www.cfr.org/article/how-much-aid-has-us-sent-ukraine-here-are-six-charts>.

10 Mark F. Cancian, "Rebuilding US inventories: Six critical systems," Center for Strategic and International Studies, January 9, 2023, <https://www.csis.org/analysis/rebuilding-us-inventories-six-critical-systems>.

11 Bryant Harris, "Taiwan is buying US weapons, but Washington isn't delivering them," *Defense News*, August 30, 2022, <https://www.defensenews.com/congress/2022/08/25/chinas-neighbors-are-buying-us-weapons-washington-isnt-delivering/>.

12 Karen DeYoung and Greg Jaffe, "NATO runs short on some munitions in Libya," *Washington Post*, April 15, 2011, https://www.washingtonpost.com/world/nato-runs-short-on-some-munitions-in-libya/2011/04/15/AF307EID_story.html.

13 Carlo Kopp, "Operation Odyssey Dawn: The collapse of Libya's relic air defense system," *Air Power Australia*, June 2011, <https://www.ausairpower.net/PDF-A/DT-Libya-Jun-2011.pdf>.

14 Ted Galen Carpenter, "How NATO pushed the U.S. into the Libya fiasco," CATO Institute, February 21, 2019, <https://www.cato.org/commentary/how-nato-pushed-us-libya-fiasco>.

15 <https://www.ifw-kiel.de/publications/news/ukraine-support-tracker-europe-clearly-overtakes-us-with-total-commitments-now-twice-as-large/>

16 <https://www.bbc.com/news/world-europe-65258129>



US Air Force, French and Royal Air Force fighter aircraft participate in formation flight. *Source:* US Air Force photo by Staff Sgt. Alexander Cook

must be interoperable or unacceptable limitations and risks will rise under operational conditions.

Fourth, as with many DOD activities, there exists a disconnect between the strategic planning, force planning, and security cooperation communities. Effective planning and coordination with allies on capabilities and force development first requires cohesive planning within these three communities. However, cross-community collaboration is often limited due to distinct organizational cultures, methodologies, incentives, languages, priorities, and decision processes. In order to achieve strategy-driven and force-informed security cooperation activities, these groups must talk to one another in a uniform language to inform, coordinate, and mutually support key priorities.

Finally, with every space contested—across all elements of national power—risks are omnipresent, and the risk

calculus of US allies for standing with the United States against an adversary become much more complex, nuanced, and with greater tradeoffs to consider. This is especially true when considering China and Russia, who are increasingly interconnected in the economies and energy grids of US allies and partners. In this environment, platitudes, well-intentioned sentiments, and policy statements must result in meaningful actions—such as improving the sharing of information and collaboration in technology development—that demonstrate the value and collaborative intentions of the DOD.

The challenges here are unlikely to reduce over time—systems will continue to become more sophisticated, and budgets will continue to be constrained. The United States must start by deciding what it wants and needs from its partners, and let that inform the way in which it designs its security cooperation systems and activities.

The Path Ahead

A number of steps can be taken to advance and evolve US cooperative security approaches, but a shift in mindset—particularly, in how the United States views and values security cooperation—must lay the foundation to achieving long-term change. The ideas below could help foster or complement this cultural shift.

Information and Technology Sharing: Take a “Collaboration-First” Mentality with the Closest and Most Capable Allies

While US adversaries cannot easily replicate, short-cut, or catch up on the advantage offered by the United States’ robust network of alliance and partnerships, the United

States can easily squander it. If the United States fails to evolve the depth and quality of its relationship with key partners; takes frontline partners for granted; or treats relationships as transactional; then the return on investment will be marginal and relationships may erode over time.

Therefore, to maximize the value of the network, DOD should take a “collaboration-first” mentality with its closest and most capable allies in information and technology sharing. For example, rather than a reflexive move to classify documents as Not Releasable to Foreign Nationals (NOFORN)¹⁷ out of an over-abundance of caution or lack of proper training¹⁸ which unnecessarily constrains information-sharing with likeminded nations, DOD personnel should seek to be as collaborative as possible. While reforms are underway across DOD to improve issues of



A soldier uses a radio comm, 2020. *Source:* US Army

17 NOFORN: “Information may not be disseminated in any form to foreign governments, foreign nationals, foreign or international organizations, or non-U.S. citizens”. [https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/DOD-CUI_Marking_Handbook-DOD_\(2020\).pdf](https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/DOD-CUI_Marking_Handbook-DOD_(2020).pdf)

18 “Use of the “Not Releasable to Foreign Nationals” (NOFORN) Caveat on Department of Defense (DoD) Information,” US Department of Defense, May 17, 2005, <https://sgp.fas.org/othergov/dod/noforn051705.pdf>



A convening of AUKUS partners, including Secretary of Defense Lloyd Austin III, British Secretary of State for Defense Ben Wallace, and Australian Defense Minister Richard Marles, 2022. *Source:* Navy Petty Officer 2nd Class Alexander Kubitza

over-classification, these efforts must be broadened to encompass the way classification is taught, the mentality of leadership and desk officers, and even adjustments in simple systems, such as changing the order of drop-down classification options in digital interfaces so that NOFORN is not the top (and laziest) choice. The United States can also learn from its friends: In some allied nations, classification of information as NOFORN-equivalent requires approval by director and above leadership. Of course, this does not mean all information should be shared—or that classifications should be abandoned—rather it means that unnecessary barriers to information sharing ought to be further examined, and the mindset changed from a simplistic ‘better to be safe than sorry’ to considering what might opportunities or benefits might be lost by not sharing, and a realistic assessment of the actual risk of sharing.

This mentality is as important—if not more so—in technology sharing as it is with information sharing: While information is often critical at a single point in time, technological advantage has a lasting impact and therefore faces even stricter access constraints. There also exists a longer history of intelligence-sharing arrangements, and so processes are more mature. The Five Eyes information sharing arrangement (between the United States, United Kingdom, Canada, Australia, and New Zealand) was formally established after World War II while the National Technology and Industrial Base (NTIB) arrangement (a roughly equivalent research and development (R&D) agreement) was only formalized in the 1990s.¹⁹ Today, partnerships like AUKUS offer the opportunity to trial technology sharing with the United States’ closes allies and potentially export this model to other likeminded nations, particularly looking at Pillar 2 which creates space for the

¹⁹ Heidi M. Peters and Luke A. Nicastro, “Defense Primer: The national Technology and Industrial Base,” Congressional Research Service, March 30, 2023, <https://sgp.fas.org/crs/natsec/IF11311.pdf>.



A US paratrooper trains a Polish soldier during a combined training event with Poland, 2022. *Source:* Army Master Sgt. Alexander Burnett

collaborative development of critical technologies.²⁰ In the AUKUS context, efforts at reforming specific bottle necks and challenges are underway, such as the Keeping Our Allies Leading in Advancement (KOALA Act) and TORPEDO Act along with a variety of others exemptions.²¹ These developments are welcome and critical, but they are yet to be progressed, and approach the problem in a largely disjointed and piece-meal way that is insufficient²² to address all concerns, even for just these two key partners. In the medium term, the AUKUS framework ought to be viewed as a pathfinder, with lessons learned through this collaboration and key elements of the approach expanded to other allies who can be considered as “most capable”.

Moreover, while there is no doubt that changes and improvements in specific elements of the process is both welcome and valuable—for instance earlier releasability of

updated capabilities could potentially halve the timeframes for building FMS cases. While eliminating transactional licenses or removing the need for recertification after approval for transfers would reduce the bureaucratic burden by reducing duplication without increasing risk, it is mostly piecemeal and disjointed—there is a broader shift in attitude and culture across multiple agencies that is needed to truly increase competitiveness. All US government agencies involved in the process should consider whether their organizational culture and staff training is sufficiently modernized for the new fight, but there are specific pain points for allies within the community. For instance, the allies consider the Defense Technology Security Agency (DTSA) to be monolithic and outdated in its approach to foreign nations, without sufficient consideration to the context of individual relationships. The teams within the Department of State that oversee the FMS processes are perceived to

20 David Brunnstrom, “More work needed on AUKUS technology sharing – British, Australian officials,” *Reuters*, March 1, 2023, <https://www.reuters.com/world/more-work-needed-aukus-technology-sharing-british-australian-officials-2023-03-01/>; William Greenwalt, “Leveraging the National Technology Industrial Base to address great-power competition: The imperative to integrate industrial capabilities of close allies,” Atlantic Council, April 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Leveraging_the_National_Technology_Industrial_Base_to_Address_Great-Power_Competition.pdf.

21 <https://www.ussc.edu.au/aukus-status-update-checking-in-on-the-advancement-of-pillar-ii>

22 <https://breakingdefense.com/2023/09/two-years-on-is-the-aukus-agreement-at-the-brink-of-failure/>

lack coordination with each other and could modernize their approaches by learning lessons from the Department of Commerce teams who oversee dual-use technologies. At the Pentagon, there are anecdotal stories of senior allied military officials being left at the entrance because of mix-ups with visitor registrations, and US staffers preparing talking points for meetings with them that were labelled NORFORN. Senior officials understand the importance of allies and have an intent to remedy these issues, but too often there is a disconnect between the staff working directly with allies, the senior leadership and the bureaucrats who manage the enabling processes. Remediating these issues would not only improve the process and eliminate outdated barriers, but also improve the perception and trust in the United States as an effective partner and ally.

US personnel must also understand the value of collaboration, rather than viewing security cooperation as a one-way street in which the benevolent superpower bestows gifts on its friends. Not only does this undermine the relationships and trust of US allies, but it also means the United States may miss opportunities to gain from new niche technologies home-grown by allies, unique operational insights from allies' own geo-political context, opportunities for experimentation that a smaller and more agile force can undertake, or even foreign-born talent and expertise. Particularly, the DOD could boost the Foreign Comparative Testing (FCT)²³ program and drop requirements for a potential technology to be sponsored by a service. As part of the Undersecretary of Defense for Research and Engineering, the FCT program seeks to find, assess, and test high readiness level technologies from foreign countries to see if they could be of use to US forces. These programs should be given the remit and resources to freely scout the best-in-class capabilities from across the network of alliances and find ways to adapt and adopt them into the US military.

Increase Cooperation in Mutual and Shared Planning and Production

As the security environment evolves, allies and partners may shift their thinking about what capabilities to acquire from the United States, as well as the depth of integration. Interoperability has long been the pinnacle aspiration for allied operations, shaping force planning and systems procurement. However, although it remains desirable, many nations are now more wary of creating dependencies. This may result from decades of operating together in the Middle East; effects of more complex geopolitical realities;

the very real considerations of cost, timelines, and supply chain capacity; a realization of the difficulty of attaining true interoperability; or simply from a shift in mindset. It may also reflect the growth and maturation of third-nation suppliers within the US partner ecosystem (such as South Korea and Taiwan). Regardless, if the United States and its partners are to find the right balance between quantity, quality, and interoperability of their forces, careful consideration is needed to identify which systems need to be US-sourced, which can be US-designed and foreign built, which can be foreign built to interoperable standards, which need to be the most exquisite in capability, and which legacy systems are sufficient with the right enhancements. All nations do this already, but the lessons from Ukraine's success in absorbing massive amounts of military aid, along with a study of the realities of that conflict, warrants a careful and in-depth reassessment of the *what*, *how*, and *why* of such decisions.

Supply chain fragility and capacity issues may²⁴ also be addressed through enhanced allied manufacturing capabilities. The United States should prioritize finding alternate means of fulfilling partner capability needs, either through bolstering co-production in third nations, increasing the options of cheaper and simpler versions of US systems, or creating pathways to integrate allied national capabilities into US operational systems (e.g., communications systems, Common Operating Picture, and other informational and targeting systems). This approach has been demonstrated through the F-35 program, but could be extended to many more systems and platforms. As systems shift from hardware-centric to software-centric, this process should become easier and increase opportunities for collaboration. That said, the shift to software-centric capability thinking needs to be deliberate and intentional, integrating the allies-first mentality and exploring creative ways to collaborate.

Elevate the Strategic Prioritization and Invest First Principles Planning of Security Cooperation Activities

Having the right capabilities is meaningless without the right strategies, concepts and plans to employ them effectively. However, current security cooperation activities are part of a lengthy and process-heavy planning system, making it difficult to elevate the strategic thinking of security cooperation. Currently, it is easier for US defense planners to retro-fit desired activities to broad strategic intents for a country or region than for them to begin the security

23 "Foreign Comparative Testing," US Department of Defense, <https://ac.cto.mil/pe/fct/>.

24 Supply chain and manufacturing capacity around the world is constrained and, in many cases, there are only so many suppliers of certain components globally. Therefore, it will not be a panacea to the challenges, though increased and steady demand signals may motivate partner nations to invest in expanding their industrial capacity.



Three F-35A Lightning IIs flying during a refueling mission near Phoenix, Arizona, 2019. *Source:* Airman Brooke Moeder

cooperation process with hard analysis of the strategic intent and let that guide the development of the proposed activity. It takes years—even decades—to identify, acquire and stand up a sophisticated combat system such as a fighter jet or naval combatant. When strategic focus shifts from, for instance, irregular counterterrorism to near-peer conventional operations, it is easier to shift the justification for an airframe from ‘close air support’ to ‘air dominance’ with the shift in armaments than it is to begin the process over with a consideration of whether it is needed in the new context. To be sure, the platform may still be relevant, or the benefits of continuing with its acquisition justified in the new context. This paper does not advocate for flip-flopping on expensive projects every few years, but there are plenty of examples through history where those shifts have come too late, so a hard rethink and reevaluation is needed when these strategic shifts occur. Moreover, when thinking about military capability-building, the US government too often lets the technology or the platform drive the analysis—often at the behest of a partner who might prioritize prestige over operational need. Instead, the analysis should help planners in determining the best capabilities to fit a given nation’s needs.

Strategic guidance should serve as a first principle for assessing national and defense objectives, rather than being aligned to the selected events retrospectively as is currently the case across security cooperation efforts. The US government must ensure security cooperation policy- and strategic goal-setting is first and foremost ‘threat-informed’ with deep consideration of the partner’s current capability gaps, needs, and future intentions. The United States already develops contingency or operational plans for each country and region, but often fail to sufficiently include its most-capable allies, or sufficiently factor in their own capability plans, to develop them into true operational plans. Often, this is hampered by the challenges of classification and information sharing discussed above. Therefore, they should consult more deeply and closely ‘most capable’ allies to enable country plans to evolve existing concepts and intents into operationalized plans with clear roles and responsibilities that each partner can plan for.

Taking a strategic lens to planning requires specialist skills, knowledge, and experience, but the security cooperation workforce is under-resourced relative to this task. The workforce requires staff with a higher quantity

of training and understanding at every level to enable more thorough planning activities, and leaders need to invest in workforce development in this sector commensurate with the strategic effects it can generate. The roles of security cooperation liaisons across the DOD and State Department are as critical as any other in the diplomatic and planning sectors, and US policymakers need to elevate and invest in them to reflect that criticality. As part of this shift, the United States must recognize the importance of personal relationships between US planners and allied counterparts and support them to achieve common goals. The Defense Security Cooperation University has recognized the need for a well-educated workforce and has already begun a process to reform its education and certification systems. Finally, all levels of the workforce require close coordination and examination: While US planners engage directly with and understand well ally and partner nations, there is often a disconnect between these action

officers and the higher echelons of leadership and policy. Shared knowledge and relationships ought to be translated across the hierarchy.

The human element is often discarded as too hard to quantify or assess in debates around the value and effectiveness of security cooperation. While certainly difficult to quantify, to dismiss the value of human capital disregards the most valuable aspect of that cooperation. Therefore, in seeking to improve oversight, accountability, and effectiveness, the US government must necessarily evolve its concept of the ROI of these activities. The building of goodwill and personal affections generated through people-to-people contact, the spreading of organizational values and culture, and the opportunities created by building people-centered networks are invaluable; they are likely to be the most resilient and vital links in times of crisis and contingency.

Conclusion and Recommendations

Security cooperation can have strategic effects. In an era of increased geopolitical complexity, strategic competition, shifting tactical considerations driven by emerging technologies, and an increasing range of non-traditional security threats, closer integration and collaboration with US allies and partners is critical. Just as all elements of DOD activities must adapt to these changing conditions, security cooperation approaches must also evolve.

While the core of the US approach is sound, seemingly small shifts in mentality, culture, focus, and approach can have deep and meaningful impacts in the way the United States is perceived by allies and the ROI from these relationships—even if they are difficult to quantify or measure. Treating allies as peers and ensuring the United States' actions towards them matches the rhetoric, trusting them with informational and technology sharing, and removing small but impactful hurdles can have a dramatic impact. The United States must reconsider and explore new ways to develop capabilities and provide the tools allies and partners need to ensure they have the capacity to meaningfully contribute to shared security goals, including alternate versions of US systems, co-production, and integrating third-party allied systems.

The United States can also learn lessons from recent conflicts to create new tools to enable partners to respond to unexpected regional security crisis and conflict. Finally, DOD leadership can enable the reform and elevation of security cooperation by realigning its place in planning and reporting hierarches, investing in the workforce that undertakes the planning and execution of the activities and ensuring strategic intent and guidance is infused at every level. While US competitors can not readily catch up to the United States' longstanding and carefully curated advantage, enacting the following recommendations can prevent the erosion of that edge and maximize the ROI provided by alliances and partnerships:

Recommendation 1: DOD should take a “lean-to-collaboration-first” mentality with its closest and most capable allies in information and technology sharing. In addition, the DOD must prioritize AUKUS Pillar 2 as a key strategic goal, and as it develops and evolves it must act as a pathfinder for wider reform on this topic.

Recommendation 2: DOD should increase the pathways to adopt and adapt allied technological developments.

For instance, DOD can do so by boosting the Foreign Comparative Testing (FCT) program and dropping requirements for a potential technology to be sponsored by a service, giving them the remit and resources to freely scout the best-in-class capabilities from across the network of alliances, and find ways to adapt and adopt them into the US military.

Recommendation 3: The United States must look for ways to reduce unnecessary and counterproductive burdens of ITAR, such as by eliminating transactional licenses for AUKUS members and removing the need for recertification after approval for transfer has already been agreed upon, and modernizing releasability processes to speed up FMS case development.

Recommendation 4: The United States should explore alternate means of fulfilling partner capability needs, either through increased co-production in third nations, increasing the options of cheaper and simpler versions of US systems, or creating pathways to integrate allied national capabilities into US operational systems. Moreover, it should take a deliberate and intentional approach to exploring the opportunities available through a transition from hardware-centric systems to software-centric capability in order to integrate the allies-first mentality and explore creative ways to collaborate.

Recommendation 5: The US government must ensure security cooperation policy- and strategic goal-setting is first and foremost ‘threat-informed’ with deep consideration of the partner’s current capability gaps, needs, and future intentions. Further, they should consult more deeply and closely ‘most capable’ allies to enable country plans to evolve existing concepts and intents into operationalized plans with clear roles and responsibilities that each partner can plan for.

Recommendation 6: DOD leadership should invest in the security cooperation workforce in a way commensurate with the importance of allies and partners and the strategic effects that security cooperation can generate, expanding it in quantity and improving its quality by investing more in the training of those who undertake it. Moreover, approaches should be shifted to prioritize the importance of person-to-person relationships, while the insights gained by that workforce need better feedback channels to every level of planning to ensure insights are actioned effectively.

About the Author



John T. Watts is a nonresident senior fellow in the *Forward* Defense practice of the Atlantic Council's Scowcroft Center for Strategy and Security and a strategic partnership manager at Signal Labs.

At the Atlantic Council, he was foundational in the development of *Forward* Defense and created the Emergent Futures Lab to develop new insights into future threats by combining experimental approaches and nontraditional perspectives with established expertise. His work there has included research and papers on creating a trusted and resilient global 5G telecommunications network, the threat and geo-political implications of hypersonic weapons in the Indo-Pacific, the threat of disinformation to national sovereignty, and a range of Indo-Pacific national-security issues and regional relationships. He is particularly noted for his work running innovative and high-profile war games to explore long-term great-power competitive technology strategies, future Army concepts of operations, alternate cybersecurity challenges, and complex Baltic and Middle East security issues.

He was recently a senior policy advisor to the Office of the Secretary of Defense—Policy. There, he managed strategic evaluations of security cooperation activities, including those relating to great-power competition and the counter-ISIS campaign, and helped establish a rigorous learning agenda through the stand-up of a series of security cooperation tabletop exercises. He also worked on the response to sensitive civilian casualty incidents.

Previously, Watts has been a partner at a defense technology consulting firm and head of consulting at a boutique strategy consulting firm. In those roles, he has advised start-up technology firms; US and international federal, state, and local governments; international organizations; and large corporate firms. Prior to moving to the United States, Watts was a staff officer at the Australian Department of Defence, working in a variety of strategic planning, implementation, evaluation, and management roles. Watts also spent more than a dozen years in the Australian Army Reserves, where he held command, training, officer-development, and emergency-management positions. His most recent position was as a liaison officer with the Virginia National Guard.

Watts holds a Master of International Law from the Australian National University and Honours of Arts in international studies from the University of Adelaide, Australia.

Acknowledgements

This report was generously sponsored by Lockheed Martin Corporation. The report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors

are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.



This report was made possible by the generous support of Lockheed Martin Corporation.



CHAIRMAN

*John F.W. Rogers

EXECUTIVE CHAIRMAN

EMERITUS

*James L. Jones

PRESIDENT AND CEO

*Frederick Kempe

EXECUTIVE VICE CHAIRS

*Adrienne Arsht

*Stephen J. Hadley

VICE CHAIRS

*Robert J. Abernethy

*Alexander V. Mirtchev

TREASURER

*George Lund

DIRECTORS

Stephen Achilles

Gina F. Adams

Timothy D. Adams

*Michael Andersson

Barbara Barrett

Colleen Bell

Sarah E. Beshar

Stephen Biegun

Linden P. Blue

Adam Boehler

John Bonsell

Philip M. Breedlove

Richard R. Burt

*Teresa Carlson

*James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

*George Chopivsky

Wesley K. Clark

*Helima Croft

*Ankit N. Desai

Dario Deste

Lawrence Di Rita

*Paula J. Dobriansky

Joseph F. Dunford, Jr.

Richard Edelman

Thomas J. Egan, Jr.

Stuart E. Eizenstat

Mark T. Esper

*Michael Fisch

Alan H. Fleischmann

Jendayi E. Frazer

Meg Gentle

Thomas H. Glocer

John B. Goodman

*Sherri W. Goodman

Marcel Grisnigt

Jarosław Grzesiak

Murathan Günal

Michael V. Hayden

Tim Holt

*Karl V. Hopkins

Kay Bailey Hutchison

Ian Ichnatowycz

Mark Isakowitz

Wolfgang F. Ischinger

Deborah Lee James

*Joia M. Johnson

*Safi Kalo

Andre Kelleners

Brian L. Kelly

Henry A. Kissinger

John E. Klein

*C. Jeffrey Knittel

Joseph Konzelmann

Keith Krach

Franklin D. Kramer

Laura Lane

Almar Latour

Yann Le Pallec

Jan M. Lodal

Douglas Lute

Jane Holl Lute

William J. Lynn

Mark Machin

Marco Margheri

Michael Margolis

Chris Marlin

William Marron

Gerardo Mato

Erin McGrain

John M. McHugh

*Judith A. Miller

Dariusz Mioduski

*Richard Morningstar

Georgette Mosbacher

Majida Mourad

Virginia A. Mulberger

Mary Claire Murphy

Julia Nesheiwat

Edward J. Newberry

Franco Nuschese

Joseph S. Nye

Ahmet M. Ören

Sally A. Painter

Ana I. Palacio

*Kostas Pantazopoulos

Alan Pellegrini

David H. Petraeus

*Lisa Pollina

Daniel B. Poneman

*Dina H. Powell McCormick

Michael Punke

Ashraf Qazi

Thomas J. Ridge

Gary Rieschel

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

Ivan A. Schlager

Rajiv Shah

Gregg Sherrill

Jeff Shockey

Ali Jehangir Siddiqui

Kris Singh

Varun Sivaram

Walter Slocombe

Christopher Smith

Clifford M. Sobel

Michael S. Steele

Richard J.A. Steele

Mary Streett

Nader Tavakoli

*Gil Tenzer

*Frances F. Townsend

Clyde C. Tuggle

Melanne Vermeer

Charles F. Wald

Michael F. Walsh

Ronald Weiser

*Al Williams

Ben Wilson

Maciej Witucki

Neal S. Wolin

*Jenny Wood

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY DIRECTORS

James A. Baker, III

Robert M. Gates

James N. Mattis

Michael G. Mullen

Leon E. Panetta

William J. Perry

Condoleezza Rice

Horst Teltschik

William H. Webster

**Executive Committee
Members*

List as of July 28, 2023



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2023 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org