Issue Brief

Coalition Operations

The Untapped Role of AI in Military Decision-Making

Authors
Emelia Probasco
Sophie Mayo
Lauren Kahn

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

September 2026

Executive Summary

U.S. military strength has long depended on the ability to fight alongside allies and partners. From the Gulf War to Operation Epic Fury, coalition operations have amplified American power, but they have also exposed persistent friction: incompatible networks, conflicting classification rules, national caveats tracked in "enormous spreadsheets," and language barriers that, at their worst, have contributed to near-fatal incidents in the field. The hope animating this paper is that AI-enabled decision support systems (AI-DSS)—software platforms that ingest, analyze, visualize, and share vast and disparate data—can help coalitions operate more effectively together. We find cause for that hope, but as with past technical evolutions, political will and bureaucratic change remain critical hurdles.

This paper examines four specific applications of AI-DSS for allied and partner operations: building a common operating picture (COP), supporting coalition targeting decisions, accelerating the foreign disclosure information-sharing process, and bridging language differences. In each case, AI-DSS offer real advantages in managing complex disclosure guidance, centralizing information, enabling real-time translation, and building a shared operational picture more quickly and reliably. We use the Maven Smart System (MSS), now deployed broadly across U.S. commands and in some cases already providing these services, as an exemplar throughout.[*]

Tempering the hope that AI-DSS can improve coalition operations are the same technical and political constraints that have confounded prior interoperability efforts. These include political restrictions on information sharing, varying technical and cybersecurity standards, and trust deficits in coalition partners and in the technology itself.

Added to these historical hurdles are newer concerns. Allies and partners are facing political backlash over deals with U.S. technology vendors, ranging from AI-DSS developers like Palantir, the prime contractor for MSS, to generative AI companies. Concerns over the reliability of U.S. commercial partners are exacerbated by recent U.S. government actions against the AI company Anthropic. When paired with increased uncertainty over America's support for allies and partners, nations are publicly seeking "sovereign AI" capabilities that may complicate future allied operations.

[*] MSS is a U.S. Department of War system; the prime contractor is Palantir.

Despite these challenges, NATO's adoption of AI-DSS has moved with unusual speed. As one example, security accreditation that can take 18 months on U.S. networks took only six months to reach initial security accreditation and one year to reach full approval in the case of NATO Maven. NATO is in a uniquely strong position to embrace AI-DSS today, with several factors we explore in this paper appearing to accelerate adoption.

Based on this research, we offer four recommendations to U.S. and international policymakers:

- **Build and calibrate confidence in AI-DSS through demonstrations, exercises, and transparency.** Uncertainty about AI-DSS can be partly addressed through direct exposure and experience. Exercises like the XVIII Airborne Corps' Scarlet Dragon and NATO Task Force Maven's outreach offer replicable models. Candid discussion of AI advantages and incidents will further calibrate allied confidence and demystify the technology for the public.

- **Presume AI sovereignty and prepare for "haves and have-nots."** The sovereign AI impulse reflects durable political and economic interests that are unlikely to dissipate. CDAO should define technical and policy standards that willing partners can adopt to facilitate AI-DSS integration and interoperability.

- **Invest in data, data sharing, and data governance.** The AI-DSS opportunity is wasted without data. This means elevating allied data generation; establishing common cybersecurity certificates and data sharing agreements (such as common data use agreements or AUKUS-like ITAR exemptions); and accelerating investment in cross-domain solutions for the efficient transfer of information to coalition networks.

- **Invest in NATO Maven.** NATO has the infrastructure, policy frameworks, and political will that are preconditions for coalition AI-DSS success. CDAO should treat Task Force Maven as both an operational asset and a learning laboratory, and use those lessons to accelerate adoption with critical Pacific partners, with AUKUS Pillar II as a potential coordination forum.

Supporting AI-DSS adoption across allies is mutually beneficial, improving partner capabilities, spurring cutting-edge AI development, and building durable security. Our recommendations are meant to close the gap between the potential advantages and our current reality.

Table of Contents

Introduction: The Drive for Military AI-Enabled Decision Support Systems (AI-DSS)

The U.S. military has long drawn on support from its allies and partners. Looking forward, any great-power conflict in the Indo-Pacific or Europe would almost certainly entail operations alongside allies and partners. But working collaboratively with other militaries is hard, for reasons ranging from differences in political goals to incompatible computer networks and data formats. Ideally, U.S. and partner forces aim to have interoperability—"the ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives"—despite these challenges.[1]

The hope is that AI, and specifically AI-enabled decision support systems (AI-DSS) that are adept at ingesting, analyzing, visualizing, and sharing vast and disparate data, can help coalitions achieve this ideal.[2]

This paper, the second in our series on the expansion of military AI-DSS, opens with a review of AI-DSS capabilities and surveys current examples, including the U.S.-developed Maven Smart System (MSS) and several international counterparts. We then examine four specific coalition applications: building a common operating picture, supporting targeting decisions, implementing foreign disclosure policies, and bridging language differences. From there, we examine the risks and hurdles specific to coalition contexts, including trust, sovereignty, data governance, and policy. We conclude with observations and recommendations for overcoming those barriers.

While this paper examines AI-DSS applications for military decisions, including targeting, it does not extensively cover how to balance automation with human judgment. The interaction between humans and AI is at the crux of important debates over AI-DSS, but a full analysis of how this varies by countries is beyond the scope of this analysis. Rather, we focus on a few specific AI-DSS applications unique to coalitions that could serve as case studies to inform future research on human judgment.

What Are AI-DSS and How Can They Help?

Military AI-DSS are software systems that ingest information, generate insights, and enable military decision-making through automation and tailored information sharing. They can take many forms and employ a variety of AI techniques but generally support six key functions, which we defined at length in a previous paper but restate briefly in Table 1.[3]

Table 1: Functions that define an AI-DSS

AI-DSS Function	Description	Examples
Ingest	Ingesting, connecting, correlating, and managing structured and unstructured information streams of a heterogeneous nature in (near) real time to maintain a continuously updated knowledge base.	• This data can include everything from traditional military sensors through to commercial data and even social media feeds. Modern data management and data architecture are most consequential for success, but AI techniques such as natural language processing and computer vision help users by providing an integrated, tailored view of all available information.
Generate	Generating insights and information from that knowledge base that is tailored to support nations or individual users and the role they play in decision-making.	• For a tactical air defender: Report airborne objects that might pose a threat together with coalition-force units available to intercept. • For a Corps-level fires officer: Report likely threats, relay engagement priorities, and suggest units best able to engage. • For a logistics planner: Report the coalition units most likely to run short of ammunition or other supplies, and the options to resupply them. • For a combatant commander: Help manage national caveat restrictions that constrain coalition force employment decisions.
Enable	Enabling users to easily create individualized dashboards,	• Users create displays that enable them to rapidly understand novel situations, develop options, and

	reports, charts, and control panels tailored specifically to their needs, decision process, and role.	assess them. ● Users design (or redesign) workflows to reflect the needs of the commander and the situation; for example, implementing different decision workflows according to national processes or rules of engagement. ● Allow watch-standers or national leaders to easily customize information displays to facilitate execution of their assignments.
Automate	Automating steps required to implement and execute a decision.	● At tactical levels, automate the creation and transmission of appropriately formatted messages or execution orders to coalition units, such as automating the transfer of target information and fires orders to appropriate artillery units. ● At operational and strategic levels, automate the generation of reports such as Situation Updates, Mission Reports, Fragmentary Orders (FRAGOs), and similar documents necessary for implementing and executing a decision.
Share	Sharing its knowledge base (in whole or part) with other authorized users, based on user permissions or bandwidth constraints, to enable a common understanding of the operational environment.	● Smart filtering, redacting, and/or editing of information to be shared based on classification, need-to-know of the recipient, and/or official release guidance. ● Smart prioritization of information to share with users that suffer bandwidth limitations. ● Sharing smart automated summaries of essential information elements with all relevant parties.

Interface	Interfacing and interacting directly with existing information systems and combat systems to allow direct transfer and exchange of relevant data, eliminating the need for slow and error-prone manual re-entry of information.	• As an illustration of such capability, Army MSS can interface directly with Advanced Field Artillery Tactical Data System (AFATDS, the system used by Army and Marine Corps to command and control artillery fires) to obtain information about various fires units and send target assignments and fire orders. Or it can interface with logistics systems such as Military Logistics Network Planning System (MLNPS) to automatically provide updates that trigger planning/replanning of logistics operations.
Source: Adapted from Igor Mikolic-Torreira and Emelia Probasco, “Beyond Targeting: The Untapped Role of AI in Military Decision-Making,” Center for Security and Emerging Technology, July 2026, https://doi.org/10.51593/20250012.		

International AI-DSS Adoption

Military AI-DSS tools are still new, but they are spreading quickly. While each system we list below has substantial differences, at their core they leverage data, software, and AI to gather, parse, and use intelligence to support military decisions. As more militaries adopt these systems, more coalitions will face the opportunity—and challenge—of operating with AI-DSS. A growing diversity of systems will compound challenges further, as we will discuss later. Examples of current, international, and coalition military AI-DSS are listed in Table 2:

Table 2. International and Coalition AI-DSS Examples[4]

Country	AI-DSS Name	Description
Australia[5]	AthenaAI; Land 156; SitaWare LAND 200[6]; Palantir (February 2026 contract)[7]	● $4M contract for AthenaAI's "automated decision support tool." ● $46M for Leidos Australia's Land 156, a counter-drone technology that combines data from numerous sensors, builds a threat picture, and handles cueing and targeting. ● Undisclosed amount for Danish firm Systematic's SitaWare LAND 200 for military planning and intelligence integration.[8] ● $7.6M to Palantir (for which system is undisclosed; note, however, that Palantir is the prime contractor for the U.S. system MSS; see U.S. row below).
Israel	Gospel[9]; Lavender[10]	● Gospel supported the management of target databases following the October 7, 2023 Hamas attack, analyzing data from satellite imagery, social media, captured communications, and other sources to propose targeting options. ● Lavender has been used to support militant identification.
NATO	NATO Maven	● The NATO version of the MSS platform—similar to the U.S. version, but with different data and tailored workflows within the platform.
Ukraine	Delta System[11]	● Integrates and maps data from multiple sensors and intelligence sources (both commercial and military). ● Used in exercises with NATO and once described by a senior Ukrainian official as "Google for the military."

United States	Maven Smart System (MSS)	• The best-known American AI-DSS, which integrates multiple intelligence sources into a tailorable graphic interface and includes workflow management and analytic tools. • Tens of thousands of users across U.S. combatant commands. • Palantir is the prime contractor.
United States (CENTCOM)	Maven Rel; Maven Green	• Two CENTCOM-developed MSS variants: Maven Rel (CENTCOM-funded) supports regional partners and allies. Maven Green (CDAO-funded) supports humanitarian relief coordination with non-governmental organizations within CENTCOM's area of responsibility (AOR).

Source: Authors' analysis.

Maven Smart System

The best-known American AI-DSS is the Maven Smart System (MSS). Between 2021 and early 2026, it went from an experiment at one military unit to an estimated 50,000 licenses across the U.S. Department of War, also recognized as the U.S. Department of Defense.[12] MSS is a flexible platform embodying all of the AI-DSS features listed earlier. It organizes and has the potential to analyze disparate intelligence sources, as well as military guidance and tactical and logistical information on blue forces. Its key components include compute infrastructure, data and data streams, graphic user interfaces, workflow management modules, and algorithms and models (including computer vision, natural language processing, and generative AI).[13] Overall, the system is highly tailorable to different military use cases provided the right data is available. In other words, AI is important to MSS, but data is essential.

The press covered MSS extensively in the context of Operation Epic Fury.[14] Palantir also advertises the underlying software for MSS (called Gotham and Foundry) as being "operationally deployed in some of the world's most hostile threat environments for both international and national security across all Five Eyes nations and coalition partners, NATO members, and some of the world's largest listed companies."[15]

In addition to MSS, several offshoots of the original system exist. While we cover MSS and NATO Maven here, we do not have sufficient information on Maven Rel or Maven Green to explore those two systems fully. Moreover, the speed at which MSS is being copied and iterated upon across the U.S. military means this list is likely already out of date.

MSS is by no means the only AI-DSS in use today, even within the United States. It is, however, the most mature, the most publicly studied and verifiable, and—through its growing family of offshoots—now the most rapidly diffusing across allied militaries and into active conflicts. Moreover, it is the system with which the authors are most familiar. For these reasons, this paper extrapolates from MSS as an exemplar of AI-DSS.

NATO's Task Force Maven

NATO's Supreme Headquarters Allied Powers Europe (SHAPE), the strategic-level headquarters of NATO's Allied Command Operations, announced the acquisition of MSS in March of 2025, relaying that it was "the most expeditious in NATO's history, taking only six months from outlining the requirement to acquiring the system."[16] NATO Maven is already spreading within the alliance.[17] Task Force Maven—the team charged with leading adoption—has reported $6M in annual savings from Maven's use in support of NATO training requirements.[18] NATO Maven has also improved process efficiency in the targeting cycle by validating targeting nominations against NATO guidance and standards, and by supporting the proper translation and formatting of targeting packages. As one member of the team put it, "MSS is addressing task overload from email" and acting in an editorial capacity by catching issues with human-generated content.[19]

Allied Country MSS Acquisition

MSS and one of its major commercial architects, Palantir, have gained traction within the militaries of alliance members. At least ten NATO countries were reportedly in talks to use MSS or another related Palantir product by October 2025.[20] Examples include:

NATO announced the acquisition of MSS in March of 2025, saying it was "the most expeditious in NATO's history, taking only six months from outlining the requirement to acquiring the system."

- **The United Kingdom (UK)** announced a partnership with Palantir for AI-DSS in September 2025, with a contract valued up to £750 million over five years.[21]

- **Canada's** Defence Department reportedly signed a $20M contract with Palantir in 2020, although public investigations claim the number to be closer to $46M over five years.[22]

- **Poland** signed a letter of intent for Palantir services and may have a contract in place in 2026.[23]

Other countries have expressed more mixed reactions to MSS:

- **Denmark** has been slow to adopt AI-DSS, even though the Palantir Gotham system is used by Danish law enforcement.[24] Denmark is also reportedly considering terminating its contract with Palantir, either as a consequence of security concerns or in response to heightened tensions with the United States over Greenland.[25]

- **France** is explicitly seeking to develop its own "sovereign system that will essentially be the equivalent of Maven," ready for operation in late 2027. France has also been building the Asgard Supercomputer, with reportedly over 1,000 NVIDIA GPUs available for classified tasks.[26]

- **Germany** has publicly rejected Palantir and announced plans to adopt European company solutions.[27]

- **Japan** has been slower to acquire the technology, despite intentions to use AI for decision support, but reported plans to exercise Maven with the United States and other Indo-Pacific allies in late 2026.[28]

- **The Netherlands** has committed to trying out MSS, but officials have voiced skepticism. Public pushback against Palantir recently resulted in the largest Dutch pension fund divesting from Palantir shares, linked to concerns about social responsibility.[29]

- **Switzerland** publicly rejected a partnership with Palantir for AI-DSS, citing concerns that Palantir would share Swiss data with U.S. intelligence.[30]

These mixed reactions reflect the tension between military interest in MSS's technical capabilities and political concerns over foreign commercial reliance, vendor lock-in, and Palantir itself. Despite the mixed reactions, the evidence shows substantial allied interest in acquiring AI-DSS, and buying or at least learning from MSS.

How Might AI-DSS Enable Coalition Operations?

AI-DSS hold substantial promise for coalition operations, where the persistent challenges of fusing data across incompatible national systems, language barriers, and cross-partner classification workflows are uniquely acute. The subsequent sections examine four specific applications of AI-DSS for allied and partner operations: establishing a common operational picture, supporting targeting decisions, implementing information-sharing policies through the foreign disclosure process, and bridging language differences.

Establishing a Coalition Common Operational Picture

A common operating picture (COP) is a continuously updated, geographic view of the battlespace. A typical COP shows the positions of all friendly, neutral, and enemy forces along with their key identifying information. Sharing this picture across a coalition is the most fundamental data exchange needed for informed decision-making and synchronized operations.

From the Field: When There's No Common Picture

In Afghanistan, coalition partners lacked a common network to share critical data before 2010, instead relying on segmented national networks and "swivel chair command and control" — turning to talk or pass notes physically rather than communicating electronically.[31] The inability to reliably communicate digitally had a detrimental impact on personnel safety, and it took years before the Afghan Mission Network provided a workable solution, instigating a shift from a "need-to-know" to a "need-to-share" culture.[32]

The 2004 Indian Ocean Tsunami response faced similar failures. A lack of network interoperability challenged communications and the digital exchange of information before the United States and other partners eventually began using the U.S. military's unclassified All Partners Access Network (APAN). Even then, necessary satellite imagery was difficult to disseminate to partners.[33]

The Challenge of Establishing and Maintaining a COP

Achieving a shared COP has proven difficult for three reasons. First, maintaining a comprehensive picture of all military and civilian assets across a geographic area is inherently hard. Second, coalition partners often lack the systems to ingest, display, and manipulate COP data, and where compatible systems exist, they still produce inconsistent results. Third, information-sharing policies and security constraints frequently delay or block the flow of critical data to allies.

NATO illustrates these challenges: Despite clear data-sharing rules, it has never fielded a NATO-wide COP system, and only the recent Federated Mission Networking (similar to the U.S. Mission Partner Network) provides a standard means of exchanging NATO classified COP information.[34] In Afghanistan, both General David Petraeus and General Stanley McChrystal decried the toll that information-sharing shortfalls were taking on achieving a common operational picture for years before a workable solution emerged.[35]

How AI-DSS Can Help Coalition COPs

AI-DSS could support COPs in two important ways:

Relevant AI-DSS Functions
Ingest
Share
Interface

- **COP data-sharing management.** Sharing live data streams such as satellite feeds, drone imagery, and internet data is inherently complex. New sources must be rapidly integrated as they come online; old ones must be retired. Unlike individualized reports, which disclosure officers can label with explicit handling instructions, a COP data stream is continuous, and information cannot be cleared piecemeal.

  AI-DSS can be built to integrate data and algorithms flexibly; for example, adding new drone sensor feeds and then updating the data fusion algorithms to account for the new source. An example of this is MSS' recent integration of a French company's computer vision algorithms and a German company's drone control and data system.[36] This means coalition data from nation states, nonprofit organizations, or intergovernmental organizations could be added more rapidly to improve an operational picture. It also means that access to data streams from military sensors could be granted to coalition members more flexibly.*

- **Managing complex information sharing.** AI-DSS could (and should) support data governance and data provenance—a method for knowing the origin of a dataset and its history of transformation, ownership, access, and usage patterns over time. Such provenance could help ensure proper and rapid information sharing, enforce standards and rules across partners, and retroactively assess data or decision errors in operations, while also facilitating transparency and traceability needed to monitor compliance with international humanitarian law (IHL) and the law of armed conflict (LOAC).

AI-DSS are already showing promise in addressing the challenges of building a COP for shared awareness. Before 2024, the XVIII Airborne Corps' Scarlet Dragon exercises using MSS demonstrated the capability to connect and share a COP with new partners in minutes and days, not years. U.S. Central Command developed Maven Rel and Maven Green in 2025 to support COP sharing with partners in the Middle East. NATO Maven has since demonstrated the same ability to enable a NATO Headquarters COP.

Despite these successes and apparent advantages, COP challenges remain. For example, nations may have competing intelligence sources, differences in communications latency, or worry about inadvertent declassification of information through the compilation of data from disparate sources. We address these and other challenges later in this paper.

Aiding and Improving Targeting Decisions in Coalitions

Targeting is a multi-step process that historically involves many people and a lot of data on enemies, civilians, neutral, and friendly forces.[37] Coalition targeting—where nations work together to identify, prioritize, and divide up target lists for deliberate and dynamic strikes—shares many features with national processes; however, the differences between national approaches and standards make it harder to operate

---

* While AI-DSS can implement user-based access to limit the accessibility of information to certain personnel, the true work of protecting classified information is done at the computer network level. For example, classified American data resident in MSS is not directly connected to NATO Maven. Instead, data is passed from a classified American network to the Mission Partner Network on which NATO-Maven resides via a cross-domain solution (CDS) that acts as a traffic cop, filtering out any unauthorized information.

rapidly and in synchronization.[38]

The Challenges of Coalition Targeting

Three challenges with coalition targeting stand out for their potential to be addressed with AI-DSS solutions:

- **The challenge of managing capabilities and national caveats.** Nations and non-governmental organizations participating in a coalition set terms of reference, known as national caveats, which "describe the mission, command relationships, organization, logistics, accounting procedures, coordination and liaison, and responsibilities of the military units and personnel assigned or detailed to the multinational force."[39] Countries also usually retain "national command" of their forces, meaning that any targeting order must be issued by designated national personnel.[*] Any strike planning must therefore account for a partner nation's distinct obligations under international law as well as the domestic policy and rules of engagement (ROE). As the number of nations in a coalition expands, managing these national caveats and procedures can become both onerous and time-consuming. In the past, targeting package information would be managed via emails and Excel spreadsheets—methods that are easy to execute but prone to error and a nightmare to keep synchronized across partners as a conflict evolves. Complications from old methods of managing caveats and ROE (when those ROE are shared and not classified by a partner nation) have even led to dangerous force protection scenarios in the midst of a conflict.[40]

From the Field: National Caveats

In Afghanistan, managing national caveats—which are the rules which dictate where, when, and how a nation's forces can be employed—required "enormous spreadsheets" and resulted in both strategic weaknesses and near-fatal incidents in the field. The patchwork of restrictions created substantial downstream effects on coalition targeting, as planners had to manually track each nation's terms before any force could be assigned or tasked.

[*] In other words, they will not relinquish control of their forces to a foreign military commander.

- **The challenge of communicating and planning as a coalition.** In addition to national caveats, generating targeting plans within coalitions often requires procedures and documentation that are unique to the coalition. In other words, the process a country normally follows will be different when working in a coalition. What's more, in multilingual coalitions the language used to promulgate orders may not be the native language of the operators.

- **The challenge of achieving consensus, or at least facilitating debate, for target selection and engagement.** Target selection may require agreement from some or all coalition members. For example, every target required unanimous approval of the 19-nation coalition in Operation Allied Force in Kosovo.[41] Even where unanimous approval is not required, coalitions will debate questions of military necessity, proportionality, and the potential for civilian harm, all reflecting differing national interpretations of IHL, such as in Operation Enduring Freedom.[42] These debates, shaped by both alliance and domestic politics, are to be expected, as militaries must judiciously apply force and consider their unique context as well as the short- and long-term consequences of lethal actions.

How AI-DSS Can Support Coalition Targeting

MSS has already demonstrated its utility in supporting the United States targeting process, dramatically reducing the number of soldiers required to execute the full targeting cycle.[43] For coalition targeting, AI-DSS offer a slightly different advantage in that they will help manage coalition-specific information and communication requirements. As a result, AI-DSS could help:

Relevant AI-DSS Functions
Ingest
Generate
Enable
Share

Manage and navigate caveats. AI-DSS hold the potential to address this challenge not so much through AI inference, but by creating a centralized repository of national caveats as well as information on available weaponry and platforms—allowing planners to spend less time searching for information and more time exercising judgment about how to allocate and assign forces. Beyond centralizing relevant information, planner visualizations could incorporate data on national caveats, with logic or LLMs used to alert operators when policy changes might affect targeting activities. This all assumes that sufficient caveat information and data on coalition platforms are available in digital format and shared appropriately with decision-makers.*

Relevant AI-DSS Functions
Generate
Automate
Share

Support compliance with coalition-specific communications standards and processes. In the example of NATO Maven, representatives reported that AI is being experimented with in an editorial role—reviewing targeting packages to ensure proper formatting, clearing up potential translation issues (see below), and validating proposals against NATO-specific guidance.[44] This has the potential to address targeting validation issues that have plagued past coalition operations. For example, during Operation Allied Force in Kosovo, 64% of targets required levels of approval higher than the commanding general.[45] In some instances, concerns about target quality led to missions being canceled once they had begun.[46] As a result of quality concerns and a tedious review process, over 150 targets were still waiting for approval at the end of the operation.[47]

Relevant AI-DSS Functions
Automate
Share

Support commander's judgment. AI-DSS have the potential to both speed up the targeting process for coalitions and improve the quality of decisions. Where countries and commanders wish to consider all available information on a target, or coalition partners' determinations of the appropriateness of the target, AI-DSS can serve to aggregate information for the commander's consideration and share a nation's final determination on a particular target. It is important to caveat that AI-DSS necessarily reflect the unique contexts, data, and problem sets that shaped their design, including the national origin of their source code, and may embed biases that do not always translate perfectly to a coalition setting.

Implementing Information Sharing Policies: The Foreign Disclosure Process

Information sharing in military operations can include:

- Indications and warning reports from intelligence agencies.
- Mission reports and status reports from units in the field.

---

* This assumes a scenario where national caveat information is readily sharable with members of a coalition. On occasion, members of a coalition may have hidden national caveats, which only become visible after an order which may violate a caveat occurs, see: Alexandra Novosseloff, "No Caveats, Please? Breaking a Myth in UN Peace Operations" (Global Peace Operations Review, September 2016).

- Imagery from both government and commercial sources.
- Electronic sensor information.
- News media, social media, and open-source reporting.
- Video from intelligence, surveillance, and reconnaissance (ISR) platforms, commercial platforms, and social media.
- Official government policies and memoranda.

From the Field: When Sharing Is the Problem

In Afghanistan, NATO's ISAF headquarters was often unable to share information with its own tactical personnel because of complex disclosure rules.[48] Italian forces working alongside the United States could not access relevant intelligence.[49] British personnel found themselves excluded from U.S. intelligence even when the UK government was the original source of the information.[50]

Ukraine also illustrated a new wrinkle: commercial companies—Amazon, Cisco, Microsoft, Palantir, and Starlink—contributed data and IT services, raising unresolved questions about how information shared with or through commercial actors flows within a coalition.[51]

Sharing this information gives coalition members critical context for determining how, where, and when to employ forces. But choosing what information to share with which ally or partner is a political and strategic decision based on national interests and mutual trust. Those decisions cascade down the military chain of command and affect the ability of military forces to exchange information and operate safely at the tactical level.

The failure to share data effectively has tangible consequences for coalition readiness and can, in some cases, explicitly prevent forces from completing missions.[*]

---

[*] For example, in Afghanistan NATO International Security Assistance Force partners found it difficult to share information with some non-NATO organizations who provided critical support, degrading the effectiveness of the overall mission, see: Michael Hanna, David Granzow, Bjorn Bolte, and Andrew Alvarado, "NATO Intelligence and Information Sharing: Improving NATO Strategy for Stabilization and Reconstruction Operations," *Connections: The Quarterly Journal* 16, no. 4 (Fall 2017): 11, https://isij.eu/article/nato-intelligence-and-information-sharing-improving-nato-strategy-stabilization-and.

Oversharing data, on the other hand, can put sensitive intelligence sources and methods at risk. Balancing these competing interests—between sharing with partners and protecting sources—makes information sharing difficult. NATO has well-established information-sharing policies and mechanisms that ease coalition operations, but those took decades to fully establish.

Ad hoc partnerships, especially in large coalitions, can pose substantial challenges for intelligence sharing, especially at the outset. Crises can help accelerate some actions, such as during the 2022 Russian invasion of Ukraine, but not entirely eliminate the friction.[*]

The Challenges with Information Sharing

Government policies, domestic laws, and international agreements shape the releasability of information to allies and partners.[†] In some alliances, disclosure rules are largely settled, as in NATO.[‡] In other cases, information disclosure requests must navigate the changeable and competing interests of intelligence agencies, operational warfighters, and domestic politics and law. Confusion about who has the authority to make disclosure decisions, and how to reach them in an emergency, compounds the problem. This network of overlapping policies, unclear approval chains, and rapid

[*] For example, in the run-up to the Russian invasion of Ukraine, the U.S. intelligence community made the unusual decision to declassify and publicly release intelligence on Russian troop movements and invasion plans—a move officials later said was designed to build a coalition, undercut the adversary's narrative, and enable partners, and one that has allegedly expanded U.S. willingness to share intelligence more broadly with NATO and allied partners going forward; Mark Pomerleau, "Authorized Strategic Intelligence Disclosures Are Likely Here to Stay, U.S. Officials Say," *DefenseScoop*, April 28, 2023, https://defensescoop.com/2023/04/28/authorized-strategic-intelligence-disclosures-are-likely-here-to-stay-us-officials-say/.

[†] These rules and processes must include high-level national security guidance establishing the legal and policy basis for foreign disclosure (National Security Decision Memorandum 119 and its associated documents); export-related laws, regulations, and policies including the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR); and DoW policies such as DoDD 5230.11 (Disclosure of Classified Military Information to Foreign Governments and International Organizations), DoDD 5530.3 (International Agreements), and DoDD 5230.20 (Visits and Assignments of Foreign Nationals).

[‡] Even where information disclosure is not uniform within an alliance, AI-DSS should be able to support these differences, though uniformity greatly simplifies the efforts.

changes in a conflict makes foreign disclosure complex, time-consuming, and error-prone.

Faced with this complexity, disclosure officers typically err on the side of over-sanitizing, and as told in official guidance:

"Whenever possible completely remove entire volumes, chapters, sections, or paragraphs from the document. If more exact sanitizing is required, remove sentences, words, and graphics from the document. ***Exact sanitizing may result in a more precise document, but is labor-intensive and requires an extensive knowledge of the information being reviewed."***[52]

This guidance is even more understandable given the asymmetry in accountability that foreign disclosure officers face: significant penalties for releasing or under-classifying information, but few immediate consequences for over-classification or unnecessary withholding, even though the latter can immediately affect operating forces.[53]

Managing these constraints is difficult even in the best conditions, and harder still at the volumes typical of modern conflict. Historically, much of this work was done by phone, email, official messages, chat rooms, and Excel files.[54] Furthermore, attempting to change needlessly restrictive classification designations can be arduous and lead to friction between allies.[55]

How AI-DSS Can Support Coalition Information Sharing

AI-DSS could help information sharing in three ways:

Relevant AI-DSS Functions
Automate
Share

Implementing straightforward guidance. In some cases, foreign disclosure guidance is relatively simple. In those instances, LLMs are well-positioned to act as an initial drafter of a sanitized intelligence report. In more complex scenarios, where guidance may be unclear, they could serve as a thought partner to disclosure officers wrestling with interpretation questions.[*] Take, for example, the simple test pictured in Figure 1, which we completed using Anthropic's Claude, where writing the prompt was the only meaningful time cost.

[*] They could even collect data on choices made by individual disclosure officers to help refine policies and guidance.

Figure 1. Using Generative AI for Foreign Disclosure Assistance

You are a foriegn disclosure officer assistant. Your goal is to help review raw intelligence and produce sanitized reports according to instructions. Sanitize the following report for countries x, y, and z:
Two Chinese JU-20s were detected by sensor ABC at 19N 116E at 0630Z

Use as your disclosure guidance:
* Country X disclosure guidance:
  * Detections of aircraft by sensor ABC can be disclosed with position, time, and aircraft identification but the sensor cannot be disclosed.
* Country Y disclosure guidance says:
  * Detections of aircraft by sensor ABC can be disclosed with time and identification, but only broad area geographic location can be shared and the sensor cannot be disclosed.
* Country Z disclosure guidance says:
  * Detections of aircraft by sensor ABC can be disclosed with time, location, and sensor, but the identification of the aircraft cannot be disclosed.

Show less

Country X Release

Two Chinese J-20s were detected at 19N 116E at 0630Z.

> **Sanitization notes:** Sensor ABC removed per disclosure guidance. Position, time, and aircraft identification retained.

Country Y Release

Two Chinese J-20s were detected in the South China Sea region at 0630Z.

> **Sanitization notes:** Sensor ABC removed per disclosure guidance. Precise coordinates (19N 116E) generalized to broad geographic area. Time and aircraft identification retained.

Country Z Release

Two aircraft were detected by sensor ABC at 19N 116E at 0630Z.

> **Sanitization notes:** Aircraft type (J-20) and nationality (Chinese) removed per disclosure guidance. Sensor, precise location, and time retained.

Source: https://claude.ai/share/4773a0a6-5de8-411a-8f86-2d5da85e18a9.

The head of Air Force Special Operations Command reported to Congress that AI has already been used to help with disclosure in Operation Epic Fury, and Palantir has also advertised a system for automated disclosure that leverages an LLM.[56]

Relevant AI-DSS Functions
Automate
Share

Managing policy changes. Foreign disclosure personnel must also contend with regular changes to the guidance itself—driven by new policies, shifts in the mission or commander's intent, or the addition or removal of partners from the coalition. These changes must be applied rapidly and can involve re-marking of previously disclosed information.[57] AI-DSS can help ensure timely dissemination and accurate tracking of new disclosure guidance, and assist with re-marking previously disclosed information.

Relevant AI-DSS Functions
Generate
Automate

Supporting policy interpretation. Servicemembers struggle to interpret and apply disclosure guidelines properly, especially when it frequently changes. Notably, an entire appendix of the Army's 2023 guidance on information sharing for multinational operations is dedicated to common misinterpretations of guidance, especially the tendency to refuse to release information when it can in fact be shared.[58] AI-DSS may help to address misinterpretations of guidance. For example, servicemembers seeking to share information in multinational operations can test their rationale for sharing or not sharing information with LLMs, similar to the example above (Figure 1). An LLM-enabled workflow that consults relevant disclosure guidance could help servicemembers make more accurate and consistent sharing decisions.

Bridging Language Differences

We have emphasized information sharing throughout this paper, and nothing may be more fundamental to information sharing than language. Coalition forces rely on language to effectively conduct everything from command and control to logistics and intelligence processing. Beyond intra-coalition communication, forces must also understand the languages of the operational environment itself. The ISAF mission in Afghanistan, for example, illustrated that effective intelligence collection and local operations depended on communicating in Dari and Pashto—two languages the coalition never had in adequate supply.[59]

The Challenges of Language

In longstanding alliances like NATO, established standards govern language proficiency.[61] In ad-hoc coalitions, language differences must be addressed in other ways, usually through liaison officers, contracted interpreters, and efforts to avoid complex plans that would stress language gaps.

> **From the Field: When Words Fail**
>
> During Operation Unified Assistance, the 2004 tsunami response, translation barriers contributed to the near-collision of a U.S. HH-60 Seahawk and an Indonesian Puma helicopter, caused by a U.S. pilot's mispronunciation of an Indonesian town. Even in a non-combat context with strong political will and a shared humanitarian mission, language differences created dangerous operational friction.[60]

Even where language standards or linguists exist, confusion and misunderstanding can arise from differences in pronunciation and accent; the use of jargon, acronyms, or idioms; and the wide variation in English proficiency. At minimum, such problems slow decision-making; in extreme cases, they can give rise to misunderstandings that cause a partner nation to operate out of synchronization, potentially causing unnecessary casualties and putting the operation itself at risk.

How AI-DSS Can Help Break Language Barriers

Relevant AI-DSS Functions
Enable
Automate
Share

Augment translations and improve communication. Advanced machine-learning tools have made remarkable strides in translation, particularly between major languages. Translation between English and less common languages remains less accurate. Furthermore, regardless of language, idiomatic expressions can be problematic to translate properly. Not all of these shortfalls are unique to machines; there are fewer human translators available for low-resource language translation as well.

While machine translation remains imperfect, the formalized structure of military communications may actually help. Military language is dense with jargon and specialized terminology, yet highly structured and standardized. These very characteristics—the ones that make military English sound foreign to civilians and confuse general-purpose translators—may make it easier to fine-tune AI systems specifically for military translation. The specialized vocabulary and rigid conventions create predictable patterns that advanced AI can learn to recognize and translate accurately.

AI-DSS could, therefore, make it possible to imagine a future in which incoming intelligence and warning reports or mission/status reports would not only be automatically sanitized for disclosure, but also append an automated translation as required. Or perhaps even voice communications could be live-translated in real time at each end. The former is feasible now: AI can already sanitize intelligence and append automated translations. The latter is not yet practical today (it might be in a few years).

Challenges to Scaling AI-DSS for Coalition Operations

A long literature already explores the challenges of coalition interoperability when it comes to technology.[62] In 2020, three years after the founding of Project Maven and over two years before the launch of ChatGPT, the veteran and academic Dr. Erik Lin-Greenberg theorized how these past challenges might manifest as coalitions try to adopt AI-DSS.[63] Many of those predictions are now bearing out:

Political constraints on data sharing and standardization still prevent nations from sharing information effectively. Whereas prior challenges with intelligence sharing concerned finished intelligence, AI-DSS benefit from raw intelligence—in other words, data directly from sensors that is continuously shared. This raw intelligence sharing challenges several longstanding national and political concerns:

- the risk of inadvertently sharing information in ongoing data feeds
- the risk of "classification by compilation," or the potential for lower-classification data to be pieced together in a way that reveals more highly classified information.[64]
- the risk that data is not strictly segregated and information intended for only one partner becomes available to many.[65]
- the risk of violating national "data sovereignty" requirements.[66]

A separate but similar challenge involves humanitarian non-governmental organizations, which share data to protect their staffs when operating in war zones—for example, through a voluntary Humanitarian Notification System.[67] Notwithstanding this mechanism, they must ensure their humanitarian data is not used for military purposes.[68] Though this is a longstanding concern for NGOs, sharing raw feeds poses new concerns about the potential to mix NGO data with military data for offensive operations.[69]

Finally, whereas each of these risks concerns sharing information with an AI-DSS, a separate but related concern arises when data is shared to train AI models. Intelligence sharing has commonly followed the "third party rule"—intelligence shared with one nation may not be shared with a third party unless permission to share is explicit.[70] Nations have not yet settled how this rule applies to algorithms trained on intelligence from multiple nations.

Nations must still reconcile data and security standards, which can be a long and complicated process that delays AI-DSS adoption. A recent industry survey of U.S. and U.K. security professionals confirms this hurdle, citing differing security classifications, a lack of common data standards, and inconsistent authorization models as primary barriers to collaboration.[71] AUKUS is illustrative: Despite reforms to streamline defense trade and encourage trilateral innovation since 2021, the United States remains concerned about Australian cybersecurity and industrial security standards, issues which are yet to be harmonized through regulatory cooperation.[72]

Nations differ in their trust of AI tools, a gap likely to generate frustration and friction in coalition operations. Varying levels of trust in AI across nations further complicate data sharing and joint decision-making.[73] In particular, differing national perspectives on the appropriate balance between human judgment and AI-DSS input, which itself shifts across a human-machine teaming relationship, is likely to be a central obstacle. Surveys show sharp differences in public confidence: only 13% in Japan and 17% in South Korea trust AI, compared to 25% in the United States and 43% in Turkey.[74] Even terminology regarding "trustworthy AI" differs across cultures, suggesting future disagreements within coalitions.[75]

Within that larger conversation are concerns about:

- The lawfulness of AI applications.
- What constitutes responsibility and accountability or qualifies as "appropriate levels of judgment and care" by military commanders.
- The standards of explainability and traceability for verification, assessment and validation.
- The reliability minimums for "safety, security and robustness."
- The ability to ensure the systems operate as intended and can still be governed should they "demonstrate unintended behavior."
- The mitigation of unintended bias in the development or use of the system.[76]

Not all nations have AI tools, and tension will arise between the haves and the have-nots. Some nations lack the infrastructure, data, or training to fully or even partially leverage AI.[77] Each nation will face at least temporary inequalities in AI use, depending on data digitization, the availability of AI infrastructure in austere or emergent situations, and the emergence of new systems. For the foreseeable future, coalition operations with AI-DSS will have to rely on incomplete or in-progress data and AI.

This “haves and have-nots” dynamic is spurring nations to act. At least ten nations have announced contracts or experiments with Palantir for the services that enabled MSS.[78] Our discussions with Task Force Maven suggest these nations are growing more concerned about falling into the “have-not” category—a fear sharpened by their exposure to MSS capabilities. As these inequalities play out, coalition effectiveness could be hampered by differing levels of adoption, suggesting modernization support could be required for those experiencing deficiencies in areas like infrastructure and training.

Differing technical interoperability standards, especially for networks and security, will slow coalition adoption. Lin-Greenberg noted that divergent accreditation standards, security requirements, and computer networks would also hinder coalitions.[79] AUKUS, launched in 2021, once again illustrates this issue: Despite its ambition, the United States, the United Kingdom, and Australia have struggled to reconcile national technical standards, preventing teams from using shared digital platforms.[80]

Ten years after a “15-star” memorandum requesting a coalition partners network, the Mission Partner Environment (MPE) and its corresponding network now constitute the primary U.S. mechanism for information sharing with coalition partners.[81] MPE, however, is not sufficient for all needs. For example, Taiwan’s ambiguous diplomatic status under the One China policy prevents Taiwan’s formal integration into MPE, leading it to announce the creation of a separate, Taiwan-specific tactical mission network.[82]

Even with partner networks, operational exercises have shown that militaries still struggle to transfer information effectively. During the 2024 Warfighter and Avenger Triad exercises, intelligence flowing over U.S. networks (SIPRNet) could not reach the exercise’s MPE network without a soldier manually transferring it—inviting errors in communication, potential synchronization issues, and an unnecessary slowing in operations.[83] Autonomous methods of transferring data between networks have been developed (Cross Domain Solutions (CDS) managed by the Defense Information Systems Agency (DISA)), though they are technically difficult and time-consuming to establish.[84] Representatives from U.S. European Command and NATO identified CDS as a leading bottleneck to the broader adoption of MSS by European allies and partners.[85]

AI-DSS cannot eliminate or render frictionless differences in targeting policies or rules of engagement.

AI-DSS may help illuminate and track policy differences between coalition nations, when they are shared at least.[86] User interfaces and workflows may even be tuned to support different oversight processes and standards. But AI-DSS cannot eliminate national policy differences that govern targeting.

Moreover, where one coalition member may assert they are ready to act at "the speed of AI," others may not be so comfortable. International perceptions of what constitutes "meaningful human control"[87] or "appropriate human judgment"[88] are unsettled. The controversy surrounding the speed of MSS and the targeting of Israel's Lavender and Gospel systems illustrates that concurrence on AI targeting is unlikely anytime soon.[89] The Lavender and Gospel systems prompted concerns among UN experts of "lowered human due diligence to avoid or minimize civilian casualties."[90] More recently, the strike on a girls' school in Minab, Iran, during Operation Epic Fury has prompted international media concern and U.S. congressional inquiries that reveal ongoing disagreement about the proper role of AI in decision-making.[91]

New Challenges

Beyond the hurdles Lin-Greenberg and others foresaw, several new challenges are emerging:

Commercial technology providers are facing political headwinds that complicate state adoption. Following a disagreement over contract language in early 2026, the Pentagon labeled the AI company Anthropic a supply chain risk and ordered Claude's removal from all military platforms, including MSS.[92] In the dispute, Anthropic refused to budge from its preferred stipulation that Claude would not be used for "fully autonomous weapons" or "mass surveillance," whereas the Pentagon insisted that it be free to deploy Claude for "all lawful uses."[93] Meanwhile, European governments and media voiced discomfort with Palantir, citing its close affiliation with the United States and comments by senior company leaders, even as European financial institutions expanded their investment in the company.[94]

The Anthropic dispute and European anxiety about Palantir raise two new issues. First, U.S. military partners must consider this: If the U.S. military will not accept usage constraints from its own domestic AI vendors, what assurances can partners realistically expect about how their algorithms or data will be handled inside a shared system? Second, can militaries worldwide depend on commercial AI providers, especially those with substantial ties to another sovereign nation?[95] As one Chatham House report put it: "the fact that Anthropic—one of the jewels in the crown of U.S. AI—can be served notice in this way is a hammer blow to the trustworthiness of U.S. technology at a time when many countries feel exposed by their deep U.S. tech dependencies and are looking for alternatives."[96]

The elevation of "AI sovereignty" as a priority has made states slow to accept workable solutions that are not considered sovereign.

Calls for "sovereign AI" have notably increased since 2025. Though the term has no agreed definition, it reflects a desire for national independence in AI. These sovereignty concerns echoed throughout our research and conversations with allies and partners.[97] The impulse is strategically rational, but for most U.S. partners it runs headlong into industrial, workforce, and market constraints that make genuine AI self-sufficiency difficult to achieve. For most allies, even wealthy ones, the domestic defense market is too small to sustain the investment required by cutting-edge AI-DSS.

This creates a dilemma: Adopt U.S. systems and accept dependency, or build alternatives and accept capability gaps. The Trump Administration's sudden June 2026 directive to suspend foreign access to Anthropic's Mythos and Fable models is an example of the type of risks allies must weigh.[98] Most allies are navigating both paths, recognizing that total sovereign control over technology supply chains is nearly impossible.[99]

Australia illustrates the tension well. Although AI-DSS are a priority sovereign capability area, Australia's small defense market means many relevant companies may look to scale or be acquired in the United States once they reach a certain size.[100] A small AI workforce split between commercial and defense applications compounds the pressure.[101] Countries in similar positions to Australia, including European allies, may have little choice but to look to international partners.[102] At the same time, there is evidence of considerable efforts on the part of allies to build sovereign AI infrastructure, such as France's Asgard supercomputer.[103]

Compute is a related bottleneck. National restrictions on compute—covering preferences for cloud, edge, or on-premises solutions—can confound collective efforts. Gaining agreement on how to build compute infrastructure, or compute interoperability where different providers are preferred, will be required for coalition AI-DSS. Even with agreement, allies must compete for compute resources with private companies racing to scale their own infrastructure.

The difficulty of building consensus around compute is already playing out in NATO. The Alliance only recently launched its Allied software for Cloud and Edge (ACE) program in July 2025 as a High Visibility Project, meaning NATO has designated it a priority which does not require full consensus and states may choose to opt in (22 nations signed a letter of intent to join in 2024 but only 12 committed to develop and roll out the initiative in 2025).[104] Even so, procurement contracts aren't expected to be awarded until late 2026, with full rollout targeted for 2030.[105]

The drive for sovereign and independent military solutions has the potential to diminish interoperability and exacerbate the "haves and have-nots" tension identified earlier.

NATO and MSS

Considering the hurdles with data sharing, security standards, and operational procedures, AI-DSS adoption across coalitions may seem hopeless. NATO's progress with MSS offers reasons for optimism. Instead of the typically long timelines, NATO is making rapid progress. Security approval to operate MSS on NATO networks, which can take up to 18 months on U.S. networks, took only six months to reach interim accreditation.[106] Even budgetary hurdles that would have otherwise taken years to clear are being overcome through the actions of a subset of nations eager to incorporate MSS.[107] So while AI-DSS adoption is challenging for all the reasons discussed above, the challenges are clearly not insurmountable.

Why has NATO moved so quickly with NATO Maven? A full answer is beyond this paper's scope, but based on conversations with Task Force Maven at NATO SHAPE Headquarters, as well as with some NATO and U.S. military members, we have several hypotheses.

First, over more than 75 years, NATO has established the underlying infrastructure needed to make AI-DSS successful for coalition operations. Intelligence sharing agreements, networking protocols, security standards, and established military doctrine and practices are already in place. These established processes can at times become sclerotic, but they have nonetheless seeded the field for AI-DSS adoption.

Second, demonstrations are inspiring action and addressing concerns. Task Force Maven representatives report that live demonstrations and hands-on experience are effectively winning over skeptics within the alliance. Using the tool demystifies its applications and demonstrates how responsible AI approaches can be applied.[108]

Finally, geopolitical and technological anxiety may sharpen NATO's sense of urgency. Russian aggression; demonstrations of AI-DSS in conflicts in Ukraine, Israel, and the United States; constant headline-grabbing news from AI companies; and the actual as well as threatened diminishment of U.S. military support to NATO may all contribute.[109]

Despite early progress, politics, data ownership, infrastructure, and interoperability issues may still complicate further scaling.[110]

Recommendations

We have examined AI-DSS' potential to improve common awareness, information sharing, and targeting for coalition operations. We have also identified challenges that would inhibit scaling. Based on this analysis, our recommendations to U.S. and international policymakers interested in pursuing the advantages of AI-DSS for coalition operations are:

Address AI trust issues by building justified confidence in, and understanding of, AI-DSS among coalition partners.

Coalition partners will not use what they do not trust. Mistrust of AI systems (MSS or otherwise) is most often rooted in a lack of information and experience. When allies gain direct visibility into how AI-DSS function—through NATO's Task Force Maven outreach, CDAO public talks, or hands-on exercises—they become more willing to prototype or experiment.[111] **Building justified confidence in these new tools must therefore begin with engagement and transparency about their nature and capabilities. This will require sustained, deliberate effort: engagement in international fora, public outreach, and above all, demonstrations and exercises.**

Demonstrations appear to be an especially effective engagement tool in the case of NATO. Task Force Maven's efforts appear to be producing shifts in acceptance among allied audiences.[112] Showing responsible adoption working in realistic use cases goes further in assuring coalition partners than abstract assurances about AI safety and reliability.

International fora offer a complementary avenue to demystify AI-DSS and upskill coalition leaders. Multilateral mechanisms to engage on AI issues are in flux, but where opportunities exist—either via general events like the Munich Security Conference and the Shangri-La Dialogue, or more focused fora like the U.S. Political Declaration on Responsible Military Use of AI and Autonomy—more transparent discussions of AI-DSS applications and requirements can help make coalition partners more AI-ready for future contingencies.

Trust must be built through exercises and real-world operations designed to test AI-assisted decision-making across alliance seams. Doing so will expose new interoperability challenges, doctrinal differences, and the dynamics of human-AI teaming. The XVIII Airborne Corps' Scarlet Dragon exercises with MSS and AUKUS's Maritime Big Play offer instructive models. Both event series treat technologies as variables to be tested and iterated upon, alongside operational goals. Replicating and expanding that approach would accelerate both the practical integration of AI-DSS and the alliance-level confidence necessary to employ them under operational conditions.

Where feasible, exercises, showcases, and operations should be treated as opportunities to demystify AI-DSS rather than solely as opportunities to impress or deter adversaries. Greater transparency about incidents of civilian harm that may or may not involve AI-DSS, such as the strike on the girls' school at Minab, Iran, could go a long way in calibrating confidence in these systems for future coalition operations.

Presume AI sovereignty and prepare for "haves and have-nots."

The sovereign AI movement reflects durable political, economic, and security interests. Interoperability challenges will persist across networks, compute environments, data ontologies, security standards, policy guidelines, standard operating procedures, and doctrinal rules. **CDAO could help to account for these foreseeable differences by defining technical and policy standards that willing partners can adopt and by working with partner nations early to identify where different systems will and won't work together.**

Finally, the United States should build AI-DSS that are ready to accept and incorporate coalition innovations. Ensuring third-party applications can integrate within MSS or other AI-DSS will position coalition forces to accept new algorithms, data feeds, and workflows regardless of their source. For example, Ukraine is rapidly creating new sensors and algorithms that are likely to be useful to allied forces, and they have already recognized the utility of sharing their battlefield data.[113] NATO Maven has found other European-developed technologies that are useful to NATO tasks and appealing for MSS integration.[114] Palantir, meanwhile, has advertised third-party application integration for MSS and highlighted successful tests with solutions from France, Germany, and the United Kingdom.[115]

Invest in data, data sharing, and data governance mechanisms and standards.

In a coalition environment, the data problem is compounded at every layer—by classification barriers, incompatible formats and ontologies, asymmetric collection capabilities among partners, and the political sensitivities that surround intelligence sharing even among close allies. **Nations hoping to benefit from AI-DSS in operations must address data issues in parallel with, or even ahead of, AI-DSS development.**

Three specific opportunities warrant leadership's attention in the short term:

- Investing more in cross-domain solutions (CDS) capable of transferring and censoring data efficiently without compromising security requirements. Without CDS, the benefit of AI-DSS is dramatically reduced, as it forces coalitions to resort to "swivel chair" command and control, emails, chats, and hand-entered data.[116]

- Building trust and establishing standard data-use agreements for NGOs and international organizations, which may contribute information important to relief operations and civilian protection.

- Expanding the AUKUS ITAR exemption approach to other nations by allowing more partners to obtain licenses and approvals for certain transfers of data and technology under reciprocal export control regimes to facilitate coalition sharing.[117]

- Building toward common, international cybersecurity standards to address data security concerns in advance of AI-DSS integration; for example, urging AUKUS partners to adopt the U.S. Cybersecurity Maturity Model Certification (CMMC) standard.[118]

Invest in NATO Maven.

The recent success of the NATO Maven team may be *the* opportunity to mature AI-DSS for allied operations. NATO already has the infrastructure, policy, and funding that are preconditions for successful coalition adoption of AI-DSS. Scaling adoption will still be challenging, but it may be the only near-term opportunity to accelerate learning for allied AI-DSS. **CDAO should seize the opportunity to gather lessons from Task Force Maven and, where feasible, use those lessons to build out adoption of AI-DSS (MSS or others as available) by other critical partners in the Pacific area of operations, especially Australia, Japan, and the United Kingdom. AUKUS Pillar II's AI and autonomy workstream could be a suitable forum, as Japan periodically coordinates with the AUKUS partners.**

Conclusion

The history of coalition operations is, in part, a history of interoperability efforts that were technically ambitious but institutionally constrained. The coordination failures in Afghanistan, from the patchwork of national caveats that required “enormous spreadsheets” to manage to the years it took to build the Afghan Mission Network, illustrate how slowly even well-resourced coalitions close the gap between technical possibility and operational reality.[119] The 2004 Indian Ocean Tsunami response showed that, even in a humanitarian context with no adversary and strong political will, information sharing can break down because of classification, network incompatibility, and disclosure policy—all issues that still hold today. Even though the war in Ukraine has demonstrated the potential of commercial technology to fill gaps, it also illustrates the persistent drag of political constraints on what partners can share and when.

Each of these cases reflects a pattern that has persisted across decades of coalition operations: The technical solutions that emerge are real improvements, but they are bounded by policy and trust constraints. MSS represents the latest iteration of this effort—an attempt to move beyond the historical patchwork of workarounds toward something more durable that can operate at the speed of modern conflict. Whether it succeeds where previous frameworks have fallen short will depend less on the sophistication of its architecture than on resolving the funding, bureaucratic, policy, and ultimately human issues that have constrained every prior solution.

Supporting AI-DSS across allies and partners is mutually beneficial for improving the military capabilities of allies; encouraging the development of new, cutting-edge AI solutions; building security across NATO; creating efficiencies in operations; and likely saving costs in the long run. Our recommendations are meant to help close the gaps that stand between these potential advantages and our current reality.

Authors

Emelia Probasco is a senior fellow at CSET.

Sophie Mayo is a graduate research assistant at CSET.

Lauren Kahn is a senior research analyst at CSET.

Acknowledgments

The authors extend their sincere appreciation to our collaborators at the Johns Hopkins Applied Physics Laboratory: Alan Brown, Christine Fox, and Annette Matheny.

We also thank the many individuals at the National Geospatial-Intelligence Agency, the Chief Digital and Artificial Intelligence Office, the Defense Innovation Unit, NATO–Supreme Headquarters Allied Powers Europe, Security Assistance Group–Ukraine, U.S. Army Europe and Africa, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, U.S. Transportation Command, and Army Futures Command, who lent their expertise and perspectives to help inspire and refine our findings.

We are grateful as well to the company representatives from Anthropic, Google, MORSE Corp, OpenAI, Palantir, and Scale AI, who contributed their research, perspectives, experiences, and insights, and to the subject-matter experts who informed this work: Ellen Lord, Margaret Palmieri, Radha Iyengar Plumb, Jack Shanahan, and Mike Siegl.

Our thanks also go to our expert reviewers: Brian Babcock-Lumish, Kyle Crichton, Julie George, Klaudia Klonowska, Igor Mikolic-Torreira, and Stephen Tankel; and to our key contributors and editorial support: Christa Bennett, Owen Daniels, Shelton Fitch, Danny Hague, and Aashka Vyas.

Finally, our sincere thanks to CSET's financial supporters, especially the Smith Richardson Foundation and U.S. Army Futures Command, without whom this work would not be possible.

Any errors or omissions are entirely the fault of the authors.

Document Identifier: doi: 10.51593/20250011

Endnotes

[1] Center for Army Lessons Learned (CALL), *Commander and Staff Guide to Multinational Interoperability,* CALL Publication No. 20-12 (Leavenworth, KS: Center for Army Lessons Learned, 2020), https://api.army.mil/e2/c/downloads/2023/01/31/3dadfaa2/20-12.pdf; Department of War, *Interoperability of Information Technology, Including National Security Systems*, *DoD Instruction 8330.01* (Washington, DC: Office of the DoW Chief Information Officer, September 27, 2022), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/833001p.pdf.

[2] John R. Boyd, *A Discourse on Winning and Losing*, ed. Grant T. Hammond (Maxwell AFB, AL: Air University Press, 2018), https://www.airuniversity.af.edu/AUPress/Display/Article/1528758/a-discourse-on-winning-and-losing/.

[3] For a more thorough examination of AI-DSS, see Igor Mikolic-Torreira and Emelia Probasco, "Beyond Targeting: The Untapped Role of AI in Military Decision-Making," July 2026, https://doi.org/10.51593/20250012; and Mohsen Soori, Fooad Karimi Ghaleh Jough, Roza Dastres et al., "AI-Based Decision Support Systems in Industry 4.0, a Review," *Journal of Economy and Technology* 4, no. 4 (2026): 206–225, https://doi.org/10.1016/j.ject.2024.08.005; Amine Abdelmouttalib and Yassin Tabaa, "Artificial Intelligence in Decision Support Systems: Applications in Strategic Business Planning," *Journal of Innovative Research and Business Studies* 1 (2025): https://journals.imist.ma/index.php/IRABS/article/view/557; Ebrahim Aly, Emiliya Suprun, Hasan Hüseyin Turan, and Sondoss Elsawah, "MBSE for Robust Decision Support Systems: A Resilient, Mission-Centric Reference Model," *Digital Engineering* 6 (2025): 100044, https://doi.org/10.1016/j.dte.2025.100044; Attila Kovari, "AI for Decision Support: Balancing Accuracy, Transparency, and Trust Across Sectors" *Information* 15, no. 11 (2024): 725, https://doi.org/10.3390/info15110725; plus numerous commercial "advertisements" of AI-DSS systems describe them performing these six functions (usually explicitly, sometimes implicitly) or non-military equivalents (e.g., in the case of financial-sector AI-DSS tools).

[4] There is also reporting on France's Artemis.AI platform, though it does not appear to support operational decision-making at this time and focuses instead on intelligence exploitation. Sources, including Vivienne Machi, "France Approves Final Phase of Artemis Big-Data Processing Platform," *Defense News*, July 11, 2022, https://www.defensenews.com/global/europe/2022/07/11/france-approves-final-

phase-of-artemis-big-data-processing-platform/; Emelia Probasco, Sam Bresnick, and Cole McFaul, "China's Military AI Wish List," (Center for Security and Emerging Technology, February 2026), https://cset.georgetown.edu/publication/chinas-military-ai-wish-list/; in 2025 the Australian firm AthenaAI was acquired by a U.S. firm, Sightline Intelligence, see: Sightline Intelligence, "News and Events," 2025, https://sightlineintelligence.com/sightline-and-athena-ai-a-powerful-partnership-for-the-future-of-ai-powered-defense/; The Hon. Pat Conroy MP, "Investing in Innovation to Boost Defence Capability," Australian Government Department of Defence, September 27, 2022, https://www.minister.defence.gov.au/media-releases/2022-09-27/investing-innovation-boost-defence-capability; "Australia Down-Selects SitaWare for Critical C2 Elements of the Australian Army," Systematic, July 27, 2023, https://systematic.com/int/industries/defence/news-knowledge/news/2023_australia-down-selects-sitaware-for-critical-c2-elements-of-the-australian-army/; The Hon. Pat Conroy MP, "Albanese Government Ramps Up Investment in Counter-Drone Capabilities for ADF," Australian Government Department of Defence, August 27, 2025, https://www.minister.defence.gov.au/media-releases/2025-08-27/albanese-government-ramps-up-investment-counter-drone-capabilities-adf.

[5] This was outlined in the 2024 Defence Industry Development Strategy, see SDIP 6, p.5: Australian Government Department of Defence, *2024 Defence Industry Development Strategy* (Canberra: Department of Defence, February 2024), https://www.defence.gov.au/about/strategic-planning/defence-industry-development-strategy.

[6] The Hon. Pat Conroy MP, "Investing in Innovation"; "SitaWare Deployed to Army Captains Course," *Australian Defence Magazine*, November 21, 2024, https://www.australiandefence.com.au/news/news/sitaware-deployed-to-army-captains-course; Systematic, "Australia Down-Selects SitaWare"; The Hon. Pat Conroy MP, "Albanese Government Ramps Up Investment in Counter-Drone Capabilities for the ADF," Australian Government Department of Defence, August 27, 2025, https://www.minister.defence.gov.au/media-releases/2025-08-27/albanese-government-ramps-up-investment-counter-drone-capabilities-adf; Julian Kerr, "SitaWare Selected as Army's New BMS," *Australian Defence Magazine,* July 25, 2023, https://www.australiandefence.com.au/defence/land/sitaware-selected-as-army-s-new-bms.

[7] Author interviews; and Robert Dougherty,"Palantir Secures $7.6M Defence Contract to Supply ICT System Platform," *Defence Connect*, February 17, 2026,

https://www.defenceconnect.com.au/industry/17697-palantir-secures-7-6-million-defence-contract-to-supply-ict-system-platform.

[8] Kirra Davey, "Leidos Selected as Land 156 Systems Integrator," *Australian Defence Magazine*, August 27, 2025, https://www.australiandefence.com.au/defence/land/leidos-selected-as-land-156-systems-integrator.

[9] Elizabeth Dwoskin, "Israel Built an 'AI Factory' for War. It Unleashed It in Gaza.," *The Washington Post,* December 29, 2024, https://www.washingtonpost.com/technology/2024/12/29/ai-israel-war-gaza-idf/.

[10] Dwoskin, "Israel Built an 'AI Factory' for War."

[11] "Battlefield Innovation: Ukraine's DELTA System Paves the Way for Allied Interoperability at CWIX24," NATO Allied Command Transformation, July 12, 2024, https://www.act.nato.int/article/delta-system-cwix/; Kateryna Bondar, "Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare" (Center for Strategic and International Studies, March 2025), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250306_Bondar_Autonomy_AI.pdf?VersionId=E2h8uqROea77udoc_og82HWsrfgfJRTZ; the Delta system also incorporates intelligence from allies, citizen reports, open-source intelligence, electronic warfare data, and acoustic detection systems, see: Kateryna Bondar, "Does Ukraine Already Have Functional CJADC2 Technology?," (Center for Strategic and International Studies, December 2024): 10, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-12/241211_Bondar_Ukraine%20CJADC2.pdf?VersionId=bxzcRKK.lmDJVz6xMtzeWwsmE2jkhcH5; NATO ACT, "Battlefield Innovation"; Katie Livingstone, "Ukraine Opens Battlefield AI Data to Allies in World-First Move," *Military Times*, March 13, 2026, https://www.militarytimes.com/flashpoints/ukraine/2026/03/13/ukraine-opens-battlefield-ai-data-to-allies-in-world-first-move/.

[12] Author interviews; while this number has not been verified independently, National Geospatial Intelligence Agency Chief Admiral Whitworth reported 20,000 active users publicly in May 2025, see: Frank Whitworth, "VADM Whitworth Delivers Keynote at 2025 GEOINT Symposium," National Geospatial-Intelligence Agency, May 21, 2025, https://www.nga.mil/news/VADM_Whitworth_Delivers_Keynote_at_2025_GEOINT_Sym.html.

[13] Palantir, "Multi-Domain AI: The Future of Command and Control | CDAO at AIPCon 9," YouTube video, May 2026, https://www.youtube.com/watch?v=yrtDgoqWmgM.

[14] Jon Harper, "Centcom Commander Touts Use of AI in Fight Against Iran During Operation Epic Fury," *DefenseScoop*, March 11, 2026, https://defensescoop.com/2026/03/11/us-military-using-ai-against-iran-operation-epic-fury-adm-cooper/.

[15] Palantir Technologies UK, Limited, "Palantir Platform: Gotham—Service Definition Document," prepared for G-Cloud 14 Framework, November 26, 2024, https://assets.applytosupply.digitalmarketplace.service.gov.uk/g-cloud-14/documents/92736/801146272055049-service-definition-document-2024-11-26-1253.pdf.

[16] "NATO Acquires AI-Enabled Warfighting System," news release, Supreme Headquarters Allied Powers Europe (SHAPE), April 14, 2025, https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-.

[17] NATO Allied Command Transformation ACT, "Artificial intelligence is becoming part of how NATO trains, adapts, and prepares for the future fight," LinkedIn post, (2026) https://www.linkedin.com/posts/nato-act_nato-wearenato-ai-activity-7462126168620621824-tQoX?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAExBnQBUmiSFR0ULP51aXuw-0gDsm69dTw; Task Force Maven NATO, "MSS NATO is in operators' hands. We want yours there too," LinkedIn post, (2026) https://www.linkedin.com/posts/task-force-maven-shape-aco-nato_dsnw-activity-7452024757463433216-4_jM?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAExBnQBUmiSFR0ULP51aXuw-0gDsm69dTw.

[18] Author interviews; see also NATO Allied Command Transformation, "AI in Audacious Training: JWC Advances a NATO Allied Command Transformation Beacon Project," March 15, 2026, https://www.act.nato.int/article/ai-audacious-training/.

[19]Author interviews.

[20] Katrina Manson, *Project Maven: A Marine Colonel, His Team, and the Dawn of AI Warfare* (New York: W. W. Norton & Company, 2026), audiobook, 10:30.

[21] Ministry of Defence and the Rt Hon. John Healey MP, "New Strategic Partnership to Unlock Billions and Boost Military AI and Innovation," September 18, 2025, https://www.gov.uk/government/news/new-strategic-partnership-to-unlock-billions-and-boost-military-ai-and-innovation.

[22] Murad Hemmadi, "The Defence Department Had a $14M Contract with Palantir for Data Management Software,' *The Logic,* September 18, 2025, https://thelogic.co/news/palantir-department-of-national-defence-contract-canada/; J.P Alegre, "Canada Spent $46.8 Million on Secret Palantir Contract for Special Forces, Records Show," *The Deep Dive*, June 2, 2026, https://thedeepdive.ca/canada-spent-46-8-million-on-secret-palantir-contract-for-special-forces-records-show/.

[23]Palantir Technologies, "Palantir is committed to Poland and proud to deepen our partnership with the Ministry of Defense," LinkedIn post, (October 27, 2025), https://www.linkedin.com/posts/palantir-technologies_palantir-is-committed-to-poland-and-proud-activity-7388560500533661696-Oriv/; "Poland Signs Intent Letter with Controversial U.S. Firm Palantir on AI and Cyber," Polskie Radio, October 29, 2025, https://www.polskieradio.pl/395/7784/artykul/3600454,poland-signs-intent-letter-with-controversial-us-firm-palantir-on-ai-and-cyber.

[24] Ian Johnston and Laura Pitel, "German States Rethink Reliance on Palantir Technology," *Financial Times,* March 10, 2023, https://www.ft.com/content/790ee3ae-f0d6-4378-9093-fac553c33576.

[25] Peter Christian Bech-Nielsen, "Denmark to Build Homegrown Palantir Alternatives for Surveillance and Warfare," *Radar,* May 7, 2026.

[26] Rudy Ruitenberg, "France Readies AI-Powered Combat Data Management Similar to U.S. 'Maven,'" *Defense News,* April 16 2026, https://www.defensenews.com/global/europe/2026/04/16/france-readies-ai-powered-combat-data-management-similar-to-us-maven/; Sylvain Biget, "La France Frappe Fort Avec Asgard, Le Supercalculateur Militaire Le Plus Puissant d'Europe," *Futura Sciences,* September 8, 2025, https://www.futura-sciences.com/tech/actualites/guerre-futur-france-frappe-fort-asgard-supercalculateur-militaire-plus-puissant-europe-125341/.

[27] Stefan Krempl, "Digital Sovereignty: BfV Buys European Palantir Alternative," *Heise Online,* May 13, 2026, https://www.heise.de/en/news/Digital-Sovereignty-BfV-Buys-European-Palantir-Alternative-11293717.html; Anna Desmarais, "Why Are European

Governments Reevaluating Their Agreements With U.S. Defense Tech Contractor Palantir?," *Euronews,* June 5, 2026, https://www.euronews.com/next/2026/06/05/why-are-european-governments-reevaluating-their-agreements-with-us-defence-tech-contractor.

[28] NSBT Japan, "The Ministry of Defense Sets Its First AI Policy and Seven Priority Areas," *Asian Military Review*, July 31, 2024, https://www.asianmilitaryreview.com/2024/07/the-ministry-of-defense-sets-its-first-ai-policy-and-seven-priority-areas-nsbt/; "Maven Smart System," Missile Defense Advocacy Alliance, August 30, 2024, https://www.missiledefenseadvocacy.org/maven-smart-system/; Resistance in Japan has been impeded by reluctance in corners of the academic and R&D community towards developing defense technology, notwithstanding the Japanese Government's shift away from a pacifist defense posture in recent years, see: Motohiro Tsuchiya, "Overcoming the Long Shadow of the Past: Defense AI in Japan," in *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, ed. Heiko Borchert, Torben Schütz, and Joseph Verbovszky, Contributions to Security and Defense Studies (Cham: Springer, 2024), 487–504, https://link.springer.com/chapter/10.1007/978-3-031-58649-1_22; Mari Yamaguchi, "Pacifist Japan Has Slowly Transformed From Exclusively Self-Defense to a Military Buildup," Associated Press, December 31, 2025, https://apnews.com/article/japan-military-buildup-defense-constitution-us-china-4986b7e36b9bb86355898c6d762084e7.

[29] Author interviews and "Largest Dutch Pension Fund Cuts Ties with Controversial Tech Firm Palantir," *NL Times*, April 2, 2026, https://nltimes.nl/2026/04/02/largest-dutch-pension-fund-cuts-ties-controversial-tech-firm-palantir.

[30] Adrienne Fichter, Marguerite Meyer, Lorenz Naegeli, Balz Oertli, and Jennifer Steiner, "How Tenaciously Palantir Courted Switzerland," trans. Priscilla Imboden, *Republik*, February 18, 2026, https://www.republik.ch/2026/02/18/how-tenaciously-palantir-courted-switzerland.

[31] Chad C. Serena, Isaac R. Porche III, Joel B. Predd, Jan Osburg, and Bradley Lossing, "Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network, RR-302-A," (RAND Corporation, 2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR302/RAND_RR302.pdf; Donna Miles, "New Afghan Network Supports Coalition Sharing," American Forces Press Service, March 8, 2011, https://www.dvidshub.net/news/513773/new-afghan-network-supports-coalition-

sharing; Erik Lin-Greenberg, "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making," *Texas National Security Review*, 3, no. 2 (Spring 2020): 56–76, https://tnsr.org/2020/03/allies-and-artificial-intelligence-obstacles-to-operations-and-decision-making/.

[32] Martin M. Westphal and Thomas C. Lang, "Conducting Operations in a Mission Partner Environment," *Joint Force Quarterly* 74, (3rd Quarter 2014): 45, https://ndupress.ndu.edu/Media/News/Article/577527/conducting-operations-in-a-mission-partner-environment/; Serena et al., "Lessons Learned from the Afghan Mission Network."

[33] Eric J. Shaw, *Operation Unified Assistance: 2004 Sumatran Earthquake and Tsunami Humanitarian Relief*, JMO Contemporary Operations Case Study (Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2013), 17; Curatola, "Lessons from 'A Team of Teams,'" 12–13. Though valuable, APAN was narrowly suited to humanitarian operations because it was unclassified and was also decommissioned in 2025, see: Partners Access Network (APAN), "After 28 years of providing unclassified mapping," LinkedIn post, (December 2025), https://www.linkedin.com/feed/update/urn:li:activity:7384014075518910464/; see also Cordula Droege, "Keeping Civilians Off-Limits in Present and Future Wars," *Digital Front Lines*, FP Analytics, August 20, 2023, https://digitalfrontlines.io/2023/08/20/keeping-civilians-off-limits-in-present-and-future-wars/; David J. Dorsett, "Tsunami! Information Sharing in the Wake of Destruction," *Joint Force* Quarterly, no. 39 (4th Quarter 2005): 17.

[34] NATO Allied Command Transformation, "Federated Mission Networking," accessed July 7, 2026, https://www.act.nato.int/activities/federated-mission-networking/; while NATO countries can all share COP-like data via JTIDS, that network primarily connects combat systems supporting tactical operations, not DSS systems that support operational or strategic-level decision-making. We address the U.S. Mission Partner Environment and Mission Partner Network later in the paper.

[35] Serena et al., "Lessons Learned from the Afghan Mission Network."

[36] Palantir, "Maven Smart System: Innovating for the Alliance," Palantir Blog, March 5, 2026, https://blog.palantir.com/maven-smart-system-innovating-for-the-alliance-5ebc31709eea.

[37] Joint Chiefs of Staff, *Joint Targeting*, Joint Publication 3-60 (Washington, DC: Joint Chiefs of Staff, September 28, 2018),

https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Joint_Staff/21-F-0520_JP_3-60_9-28-2018.pdf.

[38] North Atlantic Treaty Organization, *Allied Joint Doctrine for Joint Targeting*, NATO Standard AJP-3.9, Edition B, Version 1 (Brussels: NATO Standardization Office, 2021), 1-15–1-19, https://assets.publishing.service.gov.uk/media/618e7da28fa8f5037ffaa03f/AJP-3.9_EDB_V1_E.pdf; Merel A.C. Ekelhof, "The Distributed Conduct of War: Reframing Debates on Autonomous Weapons, Human Control and Legal Compliance in Targeting" (PhD diss., Vrije Universiteit Amsterdam, 2019), 180–81, https://research.vu.nl/files/90547665/complete%20dissertation.pdf.

[39] Stephen M. Saideman and David P. Auerswald, "Comparing Caveats: Understanding the Sources of National Restrictions upon NATO's Mission in Afghanistan," *International Studies Quarterly* 56, no. 1 (March 2012): 67–84, https://nwc.ndu.edu/Portals/71/Images/Publications/Comparing%20Caveats.pdf; Multinational Planning Augmentation Team (MPAT) Secretariat, *Multinational Force Standing Operating Procedures*, version 3.4, (Camp H. M. Smith, HI: Headquarters, U.S. Pacific Command, February 14, 2025), https://www.pacom.mil/Portals/55/Documents/J7/MNF%20SOP%20Ver%203.4_14%20FEB%2025_vbf.pdf.

[40] Annie Shiel, "The Sum of All Parts: Reducing Civilian Harm in Multinational Coalition Operations" (Center for Civilians in Conflict, January 2019), https://civiliansinconflict.org/publications/research/the-sum-of-all-parts/.

[41] John Peters, Stuart Johnson, Nora Bensahel, Timothy Liston, and Traci Williams, European Contributions to Operation Allied Force: Implications for Transatlantic Cooperation (RAND, 2001), 25; Chance Smith, "The Continued Evolution of Air Force Targeting," *Air & Space Operations Review* 4, no. 2 (Winter 2025): 45, https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-4_Number-2/Smith.pdf; Richard A. Hand, "Who Should Call the Shots? Resolving Friction in the Targeting Process" (School of Advanced AirPower Studies, Air University, 2001), 56; Elaine M. Grossman, "Fellow Military Leaders May Prove to Be Clark's Toughest Hurdle," *Inside the Pentagon,* September 17, 2003, https://insidedefense.com/share/32976; Richard K. Betts, "Compromised Command," *Foreign Affairs* 80, no. 4 (July/August 2001), https://www.foreignaffairs.com/reviews/compromised-command.

[42] Donald P. Wright, James R. Bird, Steven E. Clay, Peter W. Connors, Scott C. Farquhar, Lynne Chandler Garcia, and Dennis F. Van Wey, *A Different Kind of War: The United States Army in Operation Enduring Freedom, October 2001–September 2005* (Fort Leavenworth, KS: Combat Studies Institute Press, US Army Combined Arms Center, 2010), https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/DifferentKindofWar.pdf.

[43] Emelia Probasco, "Building the Tech Coalition" (Center for Security and Emerging Technology, August 2024), https://cset.georgetown.edu/publication/building-the-tech-coalition/.

[44] Author interviews.

[45] United States Government Accounting Office, *Kosovo Air Operations: Need to Maintain Alliance Cohesion Resulted in Doctrinal Departures*, GAO-01-784 (Washington, DC: GAO, July 27, 2001), 8–9.

[46] GAO, *Kosovo Air Operations,* 8–9.

[47] GAO, *Kosovo Air Operations,* 8–9.

[48] Lin-Greenberg, "Allies and Artificial Intelligence."

[49] Brian F. Neumann, Lisa Mundey, and Jon Mikolashek, *Operation Enduring Freedom: The United States Army in Afghanistan, March 2002–April 2005*, CMH Pub 70-83-1 (Washington, DC: U.S. Army Center of Military History, 2013): 47, https://history.army.mil/Portals/143/Images/Publications/Publication%20By%20Title%20Images/O%20titles%20PDF/operation-enduring-freedom-1.pdf.

[50] Neumann et al., *Operation Enduring Freedom*.

[51] James Black, Pauline Paille, Charlotte Kleberg, Conlan Ellis, and Maxime Sommerfeld Antoniou, "Russia's War in Ukraine" (RAND Europe, 2024), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA3400/RRA3400-1/RAND_RRA3400-1.pdf: 24; Christine H. Fox and Emelia Probasco, "Volunteer Force: U.S. Tech Companies and Their Contributions in Ukraine" (Center for Security and Emerging Technology, May 2023), https://cset.georgetown.edu/publication/volunteer-force/; Sam Bresnick, Ngor Luong, and Kathleen Curlee, "Which Ties Will Bind?" (Center for Strategic and Emerging Technology, February 2024), https://cset.georgetown.edu/publication/which-ties-will-bind/; Vera Bergengruen,

"How Tech Giants Turned Ukraine Into an AI War Lab," *Time,* February 2024, https://time.com/6691662/ai-ukraine-war-palantir/.

[52] U.S. Marine Corps, Basic *Foreign Disclosure Pocket Guide,* (Foreign Disclosure & Export Solutions Corporation, 2008), https://www.aviation.marines.mil/Portals/11/Documents/Foreign%20Disclosure%20Guide.pdf.

[53]Though it can immediately affect operating forces, see: Byman, *Improving U.S. Intelligence Sharing with Allies and Partners.*

[54]Amy Walker and Kathryn Bailey, "Army Corps Leveraging Multinational Exercises to Advance Data-Driven Operations," The United States Army, June 1, 2023, https://www.army.mil/article/267157/army_corps_leveraging_multinational_exercises_to_advance_data_driven_operations; James P. Micciche and Jahara Matisek, "Connecting the Force: Building U.S. Military Interoperability for the Modern Battlefield," Small Wars Journal, February 13, 2025, https://smallwarsjournal.com/2025/02/13/connecting-the-force-building-us-military-interoperability-for-the-modern-battlefield/; Robert Deitz, "Multinational Intelligence Sharing and Interoperability," MI Professional Bulletin, April 28, 2025, https://mipb.ikn.army.mil/issues/continuous-transformation-2025/multinational-intelligence-sharing/. Substantial efforts have been made to better facilitate information exchanges but none have achieved widespread success for reasons we will discuss later.

[55] Sometimes, information sharing classifications cannot be changed to account for allies, despite a determination that this should occur. In other instances, an ally might have an intelligence sharing agreement with the United States but not with another U.S. ally in a coalition; in this case the two U.S. allies cannot be placed in the same data sharing network, see: U.S. Government Accountability Office, *Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework*, GAO-25-106454 (Washington, DC: Government Accountability Office, 2025), https://files.gao.gov/reports/GAO-25-106454/index.html.

[56] Committee on Armed Services, U.S. Senate, "Open/Closed: To Receive Testimony on the United States Special Operations Command," May 12, 2026 https://www.armed-services.senate.gov/imo/media/doc/05-12-2026_etc_transcript.pdf; Palantir, "AI's Role in Reimagining the Classification System," Palantir Blog, February 22, 2024, https://blog.palantir.com/ais-role-in-reimagining-the-classification-system-2d7878c71217.

[57] U.S. Department of the Army, *ATP 3-16.02: Write for Release*, Army Techniques Publication 3-16.02 (Washington, DC: Department of the Army, September 2023), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39403-ATP_3-16.02-000-WEB-1.pdf.

[58] U.S. Department of the Army, *ATP 3-16.02: Write for Release.*

[59] Matthew Mosk, Brian Ross, and Joseph Rhee, "Exclusive: Whistleblower Claims Many U.S. Interpreters Can't Speak Afghan Languages," ABC News, September 7, 2010, https://abcnews.com/Blotter/afghanistan-whistleblower-claims-us-interpreters-speak-afghan-languages/story?id=11578169.

[60] The operation involved India, Australia, Japan, Malaysia, Korea, New Zealand, Singapore, Germany, France, Pakistan, and the United Kingdom; Jim Garamone, "More Ships, Helicopters Arrive to Aid Tsunami Victims," Defense Visual Information Distribution Service, May 2005, https://www.dvidshub.net/news/536237/more-ships-helicopters-arrive-aid-tsunami-victims#:~:text=Navy%20helicopters%20continue%20to%20airlift,nations%20from%20Indonesia%20to%20Somalia; Curatola, "Lessons from 'A Team of Teams'"; Shaw, "Operation Unified Assistance," 18.

[61] Bureau for International Language Coordination, "NATO STANAG 6001," ed. 5, 2019.

[62] James Igoe Walsh, "Findings and Implications," in *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2010), http://www.jstor.org.proxy.library.georgetown.edu/stable/10.7312/wals15410.9.

[63] Lin-Greenberg, "Allies and Artificial Intelligence."

[64] Center for Development of Security Excellence, "Derivative Classification Student Guide," July 2021, https://www.cdse.edu/Portals/124/Documents/student-guides/IF103-guide.pdf.

[65] Author interviews.

[66] Everfox, "CYBER360: Defending the Digital Battlespace," 2026, https://45276492.fs1.hubspotusercontent-na1.net/hubfs/45276492/2026_CYBER360_Files/Everfox_CYBER360_Defending_the_Digital_Battlespace_0.4%201.pdf; Mobile World Live, "AI Survey Report 2026," 2026,

https://assets.mobileworldlive.com/wp-content/uploads/2026/02/19111314/Mobile-World-Live-AI-Survey-Report-2026.pdf.

[67] Norwegian Refugee Council, “Explainer: Humanitarian Notification Systems (HNS)," April 12, 2024, https://www.nrc.no/globalassets/pdf/reports/protection-of-civilians-and-access/nrc-notifications-explainer.pdf.

[68] Norwegian Refugee Council, “Explainer: Humanitarian Notification Systems (HNS).”

[69] Norwegian Refugee Council, “Explainer: Humanitarian Notification Systems (HNS)”; Safia K. Southey, “The Cost of Aid: When Humanitarian Data Collection Becomes a Method of Warfare,” *Opinio Juris*, November 6, 2025, https://opiniojuris.org/2025/11/06/the-cost-of-aid-when-humanitarian-data-collection-becomes-a-method-of-warfare/.

[70] Scarlet Kim, Diana Lee, Asaf Lubin, and Paulina Perlin, “Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements,” *Lawfare*, April 23, 2018, https://www.lawfaremedia.org/article/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing.

[71] Everfox, “CYBER360.”

[72] William Greenwalt and Tom Corben, “AUKUS Enablers? Assessing Defence Trade Control Reforms in Australia and the United States,” United States Studies Centre, August 2024, 34–35, https://www.ussc.edu.au/aukus-assessing-defence-trade-control-reforms-in-australia-and-the-united-states.

[73] Lauren Kahn, Emelia S. Probasco, and Ronnie Kinoshita, “AI Safety and Automation Bias” (Center for Security and Emerging Technology, November 2024), https://cset.georgetown.edu/publication/ai-safety-and-automation-bias/.

[74] Kate Iida, Sulamaan Rahim, Chris Hutber et al., “Government AI Readiness Index 2025,” Oxford Insights, January 2026, https://oxfordinsights.com/wp-content/uploads/2026/01/2025-Government-AI-Readiness-Index-Report_01_26.pdf.

[75] Emelia Probasco and Kathleen Curlee, “The Inigo Montoya Problem for Trustworthy AI (International Version): Comparing National Guidance Documents” (Center for Security and Emerging Technology, October 2023), https://cset.georgetown.edu/publication/the-inigo-montoya-problem-for-trustworthy-ai-international-version/; Lin-Greenberg, “Allies and Artificial Intelligence.”

[76] "Summary of the NATO Artificial Intelligence Strategy," NATO, October 2021, 2026, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/10/22/summary-of-the-nato-artificial-intelligence-strategy.

[77] Lin-Greenberg, "Allies and Artificial Intelligence."

[78] Tamara Rozouvan, "NATO Agrees [to] Sole-Source Procurement of Palantir's Maven," *Janes*, April 23, 2025, https://www.janes.com/defence-intelligence-insights/defence-news/c4isr/nato-agrees-sole-source-procurement-of-palantirs-maven.

[79] Lin-Greenberg, "Allies and Artificial Intelligence"

[80] Clara Riedenstein, William Echikson, and Lance Landrum, "Defend in the Cloud: Boost NATO Data Resilience," Center for European Policy Analysis, April 2025, https://cepa.org/comprehensive-reports/defend-in-the-cloud-boost-nato-data-resilience/.

[81] The "15 stars" refers to signatories, which included the deputy commanders of U.S. Special Operations Command and the Africa, Central, European, and Pacific Commands. Robert B. Sims, "The Mission Partner Environment: Challenges to Multinational Information Sharing" (research report, Air War College, Air University, February 15, 2016); Sandra I. Erwin, "U.S. Central Command Leads Push to Connect Allies in Common Network," *National Defense*, September 2015, https://www.nationaldefensemagazine.org/articles/2015/9/1/2015september-us-central-command-leads-push-to-connect-allies-in-common-network-updated; Lauren C. Williams, "US Army's Pacific Corps Will Invite More Allies to Join Groundbreaking Comms Platform," *Defense One*, October 25, 2023, https://www.defenseone.com/defense-systems/2023/10/us-armys-pacific-corps-will-invite-more-allies-join-groundbreaking-comms-platform/391529/; U.S. Army Mission Command Center of Excellence, *Commander and Staff Guide to the Mission Partner Environment*, No. 25-1004 (April 2025), https://api.army.mil/e2/c/downloads/2025/04/29/59b51ef8/no-25-1004-commander-and-staff-guide-to-mission-partner-environment-apr-25.pdf; and U.S. Department of War, DoD Instruction 8110.01, *Mission Partner Environment Information Sharing Capability Implementation for the DoD*, June 30, 2021, https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/811001p.pdf.

[82] "Taiwan to Build Integrated Defense Network With U.S. Tactical Mission Network $1.0B Sale," *Army Recognition Group*, December 19, 2025,

https://www.armyrecognition.com/news/army-news/2025/taiwan-to-build-integrated-defense-network-with-u-s-tactical-mission-network-1-0b-sale.

[83] Robert Deitz, “Multinational Intelligence Sharing and Interoperability,” *MI Professional Bulletin*, April 28, 2025, https://mipb.ikn.army.mil/issues/continuous-transformation-2025/multinational-intelligence-sharing/.

[84] Gregory M. Kausner, “Policy Change to Identify Missile Defense Agency as the Implementing Agency for Stand-Alone Cross Domain Solution FMS Cases,” DSCA Policy Memorandum 19-13, December 20, 2019, https://samm.dsca.mil/policy-memoranda/dsca-19-13; “Cross Domain Enterprise Service (CDES),” DOD Cyber Exchange Public, accessed April 27, 2026, https://www.cyber.mil/cdes/; Alexander Schellong, “Cross Domain Solutions – Quo Vadis,” *Cyber Defense Magazine*, March 28, 2020, https://www.cyberdefensemagazine.com/cross-domain-solutions-quo-vadis-2/.

[85] Author interviews.

[86] Novosseloff, “No Caveats, Please?”

[87] “‘Politically Unacceptable, Morally Repugnant’: UN Chief Calls for Global Ban on ‘Killer Robots’ | UN News,” May 14, 2005, https://news.un.org/en/story/2025/05/1163256.

[88] DoD Directive 3000.09, “Autonomy in Weapon Systems,” January 25, 2023.

[89] Yuval Abraham, “‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza,” *+972 Magazine*, April 3, 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/; Harry Davies, Bethan McKernan, and Dan Sabbagh, “‘The Gospel’: How Israel Uses AI to Select Bombing Targets in Gaza,” *The Guardian*, December 1, 2023, https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets.

[90] Balakrishnan Rajagopal, Francesca Albanese, Reem Alsalem et al., “Gaza: UN Experts Deplore Use of Purported AI to Commit ‘Domicide’ in Gaza, Call for Reparative Approach to Rebuilding,” press release, Office of the United Nations High Commissioner for Human Rights, April 15, 2024, https://www.ohchr.org/en/press-releases/2024/04/gaza-un-experts-deplore-use-purported-ai-commit-domicide-gaza-call.

[91] Anna Lansford, "Gillibrand Demands Bipartisan Investigation Into Deadly Bombing of Iranian Elementary School," press release, Office of Senator Kirsten Gillibrand, April 7, 2026, https://www.gillibrand.senate.gov/news/press/release/gillibrand-demands-bipartisan-investigation-into-deadly-bombing-of-iranian-elementary-school/.

[92] The supply chain risk designation is still being disputed. Commands and contractors were originally given six months to transition away from using Anthropic products in March. The status of the transition is unknown to the authors. Matt Mande and Gregory C. Allen, "What Is Maven Smart System, and What Does It Do?," *Center for Strategic and International Studies*, June 2, 2026, https://www.csis.org/analysis/what-maven-smart-system-and-what-does-it-do; Dario Amodei, "Statement from Dario Amodei on Our Discussions with the Department of War," Anthropic, February 2026, https://www.anthropic.com/news/statement-department-of-war.

[93] Amrith Ramkumar, Keach Hagey and Vera Bergengruen, "Pentagon Used Anthropic's Claude in Maduro Venezuela Raid," *The Wall Street Journal*, February 15, 2026, https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17; Bobby Allyn, "Pentagon Labels AI Company Anthropic a Supply Chain Risk," *NPR*, March 6, 2026, https://www.npr.org/2026/03/06/g-s1-112713/pentagon-labels-ai-company-anthropic-a-supply-chain-risk.

[94] Joana Soares, "The Palantir Paradox: Can European Sovereignty Be Built on Controversial U.S. Tech?" *EU Perspectives*, May 17, 2026, https://euperspectives.eu/2026/05/the-palantir-paradox-can-european-sovereignty-be-built-on-controversial-us-tech/; Sebastiaan Brommersma, Casper Rouffaer, and Salsabil Fayed, "European Funders Bet Big on Tech Giant Palantir Despite Concerns over Human Rights and Democracy," *Follow the Money*, March 19, 2026.

[95] Author interviews; and Vladimír Šucha, "Europe's AI Sovereignty Just Became a Security Emergency," *Euractiv*, April 1, 2026, https://www.euractiv.com/opinion/europes-ai-sovereignty-just-became-a-security-emergency/.

[96] James Ball, "Anthropic-Pentagon Dispute Reverberates in European Capitals," *Tech Policy Press*, March 19, 2026, https://www.techpolicy.press/anthropic-pentagon-dispute-reverberates-in-european-capitals/; "Anthropic's Feud with the Pentagon Reveals the Limits of AI Governance," Chatham House, March 4, 2026,

https://www.chathamhouse.org/2026/03/anthropics-feud-pentagon-reveals-limits-ai-governance.

[97] Author interviews.

[98] "Statement on the U.S. Government Directive to Suspend Access to Fable 5 and Mythos 5," Anthropic, June 12, 2026, https://www.anthropic.com/news/fable-mythos-access.

[99] Richard Marles, "Securing Australia's Sovereignty," statement, Australian Government Department of Defence, February 9, 2023, https://www.minister.defence.gov.au/statements/2023-02-09/securing-australias-sovereignty.

[100] The Australian Government's 2024 and 2026 Defence Industry Development Strategies indicated a focus on cultivating sovereign technologies, including battlespace awareness and management systems which utilize AI, see: Australian Government Department of Defence, *Defence Industry Development Strategy* (February 29, 2024), SDIP 6, https://www.defence.gov.au/about/strategic-planning/defence-industry-development-strategy; and Australian Government Department of Defence, *DIDS26 Detailed Sovereign Defence Industrial Priorities Annex A* (July 2026), SDIP 6, https://www.defence.gov.au/sites/default/files/2026-07/DIDS26-SDIP-Annex.pdf.

[101] Peter Layton, "Evolution Not Revolution: Defence AI in Australia," in *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, ed. Heiko Borchert, Torben Schütz, and Joseph Verbovszky (Springer, 2024), 599, https://doi.org/10.1007/978-3-031-58649-1_26.

[102] Layton, "Evolution Not Revolution: Defence AI in Australia."

[103] Pablo Chavez, Vivek Chilukuri, and Ruby Scanlon, "Sovereign AI Index" (CNAS Reports, April 2026), https://interactives.cnas.org/reports/sovereign-ai-index/.

[104] "NATO Cloud Conference Advances Innovation and IT Security across the Alliance," NATO, January 23, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/01/23/nato-cloud-conference-advances-innovation-and-it-security-across-the-alliance.

[105] "Allies Enhance NATO's Digital Posture," NATO, July 23, 2025, accessed April 24, 2026, https://www.nato.int/en/news-and-events/articles/news/2025/07/23/allies-enhance-natos-digital-posture.

[106] While six months is still very slow when compared to the release of new frontier models, relative to military approval processes it is fast. In a related CSET study, one firm reported full approval timelines of up to 36 months. "NATO Acquires AI-Enabled Warfighting System," NATO Communications and Information Agency, April 14, 2025, https://www.ncia.nato.int/newsroom/news/nato-acquires-aienabled-warfighting-system; and Katherine Carroll, "Outpaced: AI and Policy's Role in Transforming Cybersecurity Compliance," August 2026, https://doi.org/10.51593/20250028.

[107] "NATO Cloud Conference Advances Innovation and IT Security across the Alliance," NATO, January 23, 2025, https://www.nato.int/en/news-and-events/articles/news/2025/01/23/nato-cloud-conference-advances-innovation-and-it-security-across-the-alliance.

[108] Author interviews; and Palantir, "Multi-Domain AI: The Future of Command and Control | CDAO at AIPCon 9," YouTube video, May 2026, https://www.youtube.com/watch?v=yrtDgoqWmgM.

[109] Sydney J. Freedberg Jr., "NATO Picks Palantir's Maven AI for Military Planning, Amid Trans-Atlantic Tension," *Breaking Defense*, April 14, 2025, https://breakingdefense.com/2025/04/nato-picks-palantirs-maven-ai-for-military-planning-amid-trans-atlantic-tension/.

[110]Author interviews.

[111] See, for example, Palantir, "Multi-Domain AI."

[112] Task Force Maven NATO, LinkedIn profile, accessed June 2026, https://www.linkedin.com/company/task-force-maven-shape-aco-nato.

[113] Katie Livingstone, "Ukraine Opens Battlefield AI Data to Allies in World-First Move," *Defense News,* June 6, 2026, https://www.defensenews.com/flashpoints/ukraine/2026/03/13/ukraine-opens-battlefield-ai-data-to-allies-in-world-first-move/.

[114] Task Force Maven NATO, "This was a busy and productive week for Task Force MAVEN," Linkedin post, May 2026, https://www.linkedin.com/posts/task-force-maven-shape-aco-nato_nato-maven-itec-activity-7450881752925032449-

OPtv?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAExBnQBUmiSFR0ULP51aXuw-0gDsm69dTw.

[115] Palantir, “Maven Smart System: Innovating for the Alliance,” Medium, March 9, 2026, http://blog.palantir.com/maven-smart-system-innovating-for-the-alliance-5ebc31709eea.

[116] Investments in establishing and exercising current CDS already appear to be paying off. At the 2024 Project Convergence Capstone exercise, Army leaders reported a new high-water mark in data exchange between U.S. networks, but only after reprogramming the CDS in the midst of the event. Discussions with U.S. military operators in Europe indicated CDS remain a bottleneck for implementing MSS with partners and allies.

[117] Exemptions for Defense Trade and Cooperation among Australia, the United Kingdom, and the United States, 22 C.F.R. § 126.7 (2026), https://www.ecfr.gov/current/title-22/part-126/section-126.7; and “International Traffic in Arms Regulations: Exemption for Defense Trade and Cooperation Among Australia, the United Kingdom, and the United States,” Federal Register, December 30, 2025.

[118] Greenwalt and Corben, “AUKUS Enablers?”

[119] Shiel, “The Sum of All Parts,” 11.