August 2021

Military AI Cooperation Toolbox

Modernizing Defense Science and Technology Partnerships for the Digital Age

CSET Issue Brief

AUTHOR
Zoe Stanley-Lockman

Executive Summary

The United States looks at leadership in artificial intelligence (AI) as critical to both advancing its strategic position in the international system and sustaining its military advantage into the future. The U.S. network of allies and partners is an asymmetric asset in service of these aims, as affirmed in national security and defense policy aimed at preparing the United States for the current era of strategic competition.

Most notably, key initiatives announced in the Department of Defense (DOD) AI Strategy and recommendations from the National Security Commission on Artificial Intelligence indicate the importance of international engagement for AI safety, security, interoperability, and alignment with democratic values.[1]

In short, there is a consensus that strengthening alliances and partnerships is important not just because the United States acts in coalitions, but also because China and Russia often act alone. AI and other emerging technologies are at the heart of competition with these near-peer competitors because of how technological acceleration drives military advancements, spurs economic growth, and shapes governance models in the 21st century. The United States can neither meet the challenges China poses, nor reap the benefits that come with shaping a democratic trajectory for AI, without deepening cooperation with its allies and partners.

Within this context, this report focuses on the imperative to safeguard the advantage of the United States and its network of partners and allies, relative to potential adversaries, through robust military relationships based on interoperable forces and cutting-edge technologies. DOD already has several tools at its disposal to deepen science and technology (S&T) cooperation with its allies and international security partners. But to capitalize on their full potential for AI, the department needs to re-envision and better integrate them.

To this end, the analysis here frames the existing defense S&T agreements, military S&T exchanges, and elements of multilateral institutions as a **military AI cooperation toolbox.** This effort goes

beyond solely pooling resources for AI-enabled capability development, to also include policy alignment; the testing, evaluation, validation, and verification (TEVV) pipeline; research and development (R&D), personnel exchanges; data sharing; and standardization. Rather than proposing new agreements, the aim here is to answer how DOD can leverage its existing mechanisms of S&T cooperation to support military cooperation in the digital age, making sure that relevant resources and frameworks do not go untapped in the quest for AI leadership and future coalition success.

While challenges, including the sensitivity around data exchanges and differing policy views on technology policy, should be acknowledged, they can also be motivating forces for cooperation to alleviate these barriers over time. In other words, the existing tools can help create more buy-in for longer term gains in political trust, cohesion, and interoperability, so that cooperation helps meet the shared challenges of digital authoritarianism and technology-driven changes to the international security environment.

The key findings are:

- TEVV is an important, but underrepresented, feature of military AI cooperation. A range of activities could factor into cooperative TEVV pipelines for AI, including joint tests, trials, experimentation, training, exercises, and modelling and simulation.
- Using defense S&T agreements to cooperate on shared R&D priorities can help build good will for other forms of AI cooperation, including alignment with democratic values.
- Military AI cooperation is not a purely technical endeavor. Technical, human, and procedural measures that foster policy and personnel connections are equally important to advancing interoperable AI adoption.
- Allies and partners in the Indo-Pacific region are under-represented in the main agreements and institutions covered in the existing military AI cooperation toolbox.

While some aspects of military AI cooperation may require new investments, mechanisms, and agreements, that should not preclude the many ways that existing tools can be put to new use. The military AI cooperation toolbox is attractive precisely because it can be activated in the near term, meeting the urgency of building interoperability and advancing AI with allies and partners as early as possible.

Table of Contents

Introduction

In the current era of strategic competition, the United States is sizing and shaping its efforts to secure leadership in artificial intelligence (AI) and maintain technological superiority. As affirmed in the 2018 Department of Defense Artificial Intelligence (DOD AI) Strategy, the network of U.S. allies and partners offers an "asymmetric strategic advantage that no competitor or rival can match."[2] Safeguarding existing partnerships and alliances is important for the United States to maintain its strategic position, prevail on future battlefields, and safeguard the international order.[3] Efforts to include allies and partners in these strategic goals are therefore just as important to advancing technological leadership in support of democratic values as they are to ensuring future military effectiveness.

For the DOD, a lot of groundwork for enhanced military-to-military cooperation is already in place, and does not require lengthy new negotiations or costly pooled resources. But to effectively use the existing tools, the department needs to re-envision their utility for AI cooperation and better integrate them in support of democratic values.

To be sure, the stakes of AI competition extend beyond the military realm. A whole-of-government, or even whole-of-society, approach is necessary to involve more robust diplomatic engagement and the array of actors relevant to securing democratic AI leadership. The focus on DOD here is intended to give concrete, detailed views on one key aspect of that broader international engagement, following the established view that strengthening alliances and partnerships is crucial to maintaining the U.S. strategic position.

The emphasis on U.S. alliances and partnerships as pertinent to AI strategy is already embedded in defense policy objectives. Namely, the Joint Artificial Intelligence Center (JAIC) has built on the DOD AI Strategy with three pillars of international AI engagement: "shaping norms around democratic values, ensuring data interoperability and working to create pipelines to enable the secure transfer of technology."[4] In its recommendations to the

executive branch and Congress, the National Security Commission on Artificial Intelligence (NSCAI) has also expanded on how to achieve this aim through a "coalition of coalitions" approach to technology cooperation.[5] Following these recommendations, the 2021 National AI Initiative directs the United States to "support opportunities for international cooperation with strategic allies, as appropriate, on the research and development, assessment, and resources for trustworthy artificial intelligence systems."[6] The tools presented in this paper can be used to match these stated priorities with concrete pathways for cooperation.

By zeroing in on military-to-military relations, the aim is to focus on a new generation of international defense cooperation that includes AI-enabled capabilities. Throughout the report, cooperation is defined more broadly than joint development and procurement. The more prominent focus on testing, evaluation, validation, and verification (TEVV), research and development (R&D), policy alignment, personnel exchanges, data sharing, and standardization is briefly summarized in Table 1 in the Appendix. As the table suggests, DOD has significant clout that it can mobilize in each of these priority areas. If used, DOD can help ensure that AI cooperation with partners and allies aligns with democratic values and simultaneously fortifies military effectiveness in a new age of digital cooperation.

Before analyzing the tools themselves, it is worth briefly touching on interoperability as a cross-cutting theme within this military AI cooperation toolbox. Interoperability means that forces can operate together because they can understand each other.[7] The technical, human, and procedural dimensions of interoperability are all important to ensuring coalition success as well as effective deterrence against competitors such as Russia and China.[8] The challenge, however, is that the gap in military capabilities only continues to expand as allies and partners are dedicating fewer resources to military digitalization relative to DOD.[9] Moreover, if AI-assisted decision-making capacities are based on different doctrinal, legal, and policy assumptions, then coalitions risk fielding systems that partners cannot use.[10] In addition to the tactical consequences of not being able to communicate and operate

alongside one another, the lack of interoperability can also result in decreased political trust between countries.

To prevent this breakdown in trust from occurring, cooperation that prioritizes near-term wins could also help build good will for more ambitious interoperability efforts down the road. Although allies and partners are not investing in AI-enabled capabilities to the same degree, most countries agree that AI is a factor that will shape their future operating environment, at the very least because of threats they will have to defend against. Moreover, preventing resource gaps from widening and ensuring robustness in systems that safeguard democratic citizenries and militaries from new forms of attack are goals that can motivate cooperation. With this in mind, military cooperation that helps build "algorithmic resilience" and countermeasures is important to assure the integrity of the information used in military decision-making.[11] In particular, political leaders need to trust the integrity of information so that disagreement does not slow decision-making down, or even weaken political cohesion between alliances.[12] Integrating AI at least into the defensive posture is an important aspect of interoperability and cooperation efforts.

To find cooperative wins, it is necessary to understand which implementation pathways DOD has at its disposal. To this end, the tools explored here fit into three broad categories through which the United States can lead cooperation and learn from its allies and partners. These categories are (1) international defense science and technology (S&T) cooperation agreements, (2) the global military S&T network, and (3) multilateral alliances and partnerships. Together, the military AI cooperation toolbox that they constitute offers a range of options to advance AI with both treaty allies and other partners. While treaty allies have stronger security guarantees and a higher level of political trust, the other partners importantly form a much broader network of friendly countries that have more varied cooperation avenues.

The rest of this report expands on this military AI toolbox. The first two sections on S&T cooperation agreements and personnel exchanges include analysis of the respective advantages and limitations of each tool, as applied to AI cooperation. The third

section on multilateral alliances and partnerships explores how each format offers its own pathways for AI cooperation. Lastly, key findings focus on the technical, policy, and region-specific prospects for AI cooperation. More specifically, these relate to the prospects of collaborative TEVV and R&D for AI, human and policy connections to foster a more conducive climate for AI adoption, and the under-representation of Indo-Pacific allies and partners in the existing military AI cooperation toolbox. While not exhaustive, the toolbox nevertheless offers net benefits for the United States to ensure that it does not tackle critical 21st century challenges alone.

International Defense Science and Technology Cooperation Agreements

The first set of tools examined in this report is the range of international defense S&T cooperation agreements that DOD has already negotiated and approved. Together, they offer policymakers and practitioners different options to advance U.S. goals of interoperability and military effectiveness, as well as starting points to begin the work announced in the DOD AI Strategy and the National AI Initiative.[13] The first two tools discussed below—International Test and Evaluation (IT&E) agreements and Reciprocal Defense Procurement and Acquisition Memoranda of Understanding (RDP MoUs)—may be used to stimulate military AI cooperation. The third tool is the less structured agreements that are bilateral or minilateral, meaning they involve a small number of countries outside the framework of multilateral institutions. These other bilateral military AI agreements and cooperative S&T blueprints are relevant because they already apply to DOD technology priorities, or can readily orient toward them.

International Test and Evaluation Agreements

- **Bilateral IT&E agreements:** Australia, Canada, Denmark, Finland, France, Germany, Italy, the Netherlands, Norway, Sweden, and the U.K.[14]
- **Multilateral IT&E agreements:** Multinational Test and Evaluation Program (MTEP) with Australia, Canada, New Zealand, the U.K., and the United States; initiated negotiations in FY2018 for a multinational Transatlantic MTEP with France, Germany, Italy, the U.K., and the United States.

IT&E agreements can help the United States work with select allies to advance procedures and methods, standards and other criteria related to testing. TEVV is critical to assuring AI will perform as expected in safety- and mission-critical systems. Current TEVV methods, however, will not work for all AI techniques, especially deep learning, because the systems are only validated and verified

relative to the specific context in which they are assessed. This does not ensure that the system will perform as expected if deployed in new or unknown environments. These concerns also extend to the security of AI systems, as they will need to be tested against adversarial attacks and other failure modes. Further, as they continue to learn, existing accreditations and certifications will not necessarily account for new behavior that AI systems pick up in inferences. As such, there is a growing consensus that DOD's TEVV infrastructure and environments, methods, and talent must all evolve.[15]

IT&E Agreements: Advantages

International cooperation is critical for evolving and upgrading TEVV to accommodate advances in emerging technologies, and IT&E agreements are integral to this this effort. For one, rather than having to pool resources, these agreements allow countries to use each other's test facilities on a "fee-for-service" and "cost-to-test" basis.[16] This means countries can access and transfer testing tools and be reimbursed on a per-use basis, or can test jointly if desired.[17] It is worth noting that the mechanism that allows this financial flexibility—Reciprocal Use of Test Facilities Project Arrangements—is not available under any other international agreement.[18] Furthermore, increasing the diversity of testing environments can also enhance AI system reliability and robustness: if a system performs predictably in an unfamiliar testing environment, it can demonstrate to allies that the AI is not just fit for U.S. TEVV processes. In other words, internationalizing the TEVV process fuses the technical and political elements of trustworthy and reliably AI—building trust between humans and intelligent machines, as well as between the allies and partners.

Using IT&E agreements to develop an international testing-as-a-service business model could be an easier, or at least faster, alternative to joint test beds. Experts have suggested that the United States should develop international joint test beds with partners and allies.[19] Joint test beds may be the optimal technological choice because they could build state-of-the-art methods and software into the design of facilities with virtual, blended, and live environments. But the idea of pooling resources

quickly comes up against political realities, including challenges to political coordination and budget commitments. Options below this threshold can be used more immediately. At the very least, using IT&E agreements in the short term could also offer valuable insights into allies' willingness and ability to exchange data needed for AI testing, or offer pathways for cooperation on burgeoning testing methods. For AI, international testing-as-a-service could equally be an interim solution until other test beds are up and running, or an alternative if other countries may not have the resources to develop their own testing capabilities.

Applying IT&E agreements to AI can also borrow from other international testing precedents. The Foreign Comparative Testing program has a small amount of funding each year to test technologies from allies and partners, particularly if it helps reduce duplication of testing costs or fills a gap. Foreign Comparative Testing is a helpful example to show why building international TEVV relationships benefits interoperability, with 280 projects over the past 40 years resulting in follow-on procurement.[20]

Outside of the United States, there are other initiatives from which the DOD can also learn. For instance, the U.K. offers synthetic training for air-to-air refueling, which analysts have suggested they use to "provide training as a service to European nations operating similar platforms."[21] Separately, the European Defence Agency also has a Defence Test and Evaluation Database and a mandate to harmonize and standardize between the more than 100 TEVV facilities across Europe.[22] As simulated environments and synthetic training become more prevalent, then increased testing collaboration could be used to benefit AI robustness. Treating AI testing as a payable service could likewise work in international cooperation, especially as IT&E agreements already include the mechanism to do so.

Just as important as the tests themselves, IT&E agreements also offer a structure for personnel connections to be included in TEVV cooperation. Under IT&E agreements, DOD can assign military or civilian employees to work in foreign facilities for cooperative projects.[23] Such personnel exchanges offer an opportunity to establish IT&E working groups that can focus on the policy,

procedural, and technical aspects of AI TEVV, with a particular emphasis on AI safety and security.

Policy-wise, IT&E working groups could focus on operationalizing safe and ethical AI principles via testing, and also work toward testing standards for AI. Relatedly, process-oriented groups could seek alignment on continuous, integrated testing methodologies.[24] As the recently updated DOD Instruction on T&E notes, integrated testing requires greater collaboration between stakeholders involved in different steps of testing processes, so that planning and execution are not sequential functions and so that data can be shared more effectively.[25] To facilitate interoperability, partners and allies can be counted among these stakeholders. Aligning software testing procedures helps integrate safety and interoperability requirements into early stages of development, which pays later dividends in streamlining "integration, developmental and operational T&E, interoperability certification, and faster delivery to the field."[26] Using IT&E working groups to collapse the barriers between these phases, which are often large, sequential milestones, is important because AI systems will need to be tested continuously over the course of their lifecycle.[27] Indeed, IT&E agreements may also prove useful to this end because the template for Reciprocal Use of Testing Facilities Project Arrangements has an option to include various test periods over multiple years.

On the technical side, working groups could focus on priorities like documentation practices and new testing methods that make AI systems more robust to cyber and physical attacks. Documenting the provenance of data and models would help ensure that allies and partners understand their strengths and limitations before using them.

Such efforts can be particularly valuable when partners need to understand how other partners' capabilities work, and also in cases where they are using similar inputs (e.g., data lakes and warehouses, software libraries) to create new models. Attackers can compromise AI systems through a range of motivated attacks, including data poisoning and adversarial machine learning, among others.[28] Adversarial machine learning—a form of spoofing that is

invisible to the human eye but leads to AI models misclassifying results, sometimes with even higher confidence—has garnered particular attention.[29] To protect against these attacks, it is important for testing to include adversarial examples in environments that are representative of physical and real-world conditions. For data poisoning, it may be difficult for testers to identify misclassifications because the attacker contaminates data prior to the testing phase (e.g., during training), and because life-long learning systems will need to be continuously tested.[30] The security risks of each kind of attack need to be accounted for in testing, and thus could be its own working group.

Another way to cooperatively tackle AI security challenges is to use IT&E agreements for threat modelling. IT&E cooperation could model threats that focus specifically on the levels of risk and attacks that exploit vulnerabilities of operating in coalitions. Threat modelling would take place over the whole AI lifecycle—not just testing—but countries could use data from previous tests to improve future testing capabilities. If testing data is structured and exchanged via IT&E agreements, then partners and allies could also institute a data-driven approach to identify and prioritize common attack vectors, as well as identify which failure is most likely in given scenarios.[31] Down the road, this data-driven approach to threat modelling could also include reinforcement learning as a validation and verification technique, and new classifiers could be used to "detect suspicious or anomalous AI behavior."[32] The use of testing data to train future classifiers could be instructive for cooperative AI development. Using IT&E personnel exchanges and working groups to set up this kind of data-driven threat modelling framework for testing would focus on the policy, procedural, and technical aspects of this new approach to AI security.

Together, these ideas for AI testing working groups are mutually reinforcing. To continue with the safety and security theme, algorithmic resilience is not purely technical. To also bring operational stakeholders into testing procedures, red teaming could also be used to ensure the safety and security of AI systems, which may be put to use in adversarial operational environments.[33] This kind of red teaming already happens for cyber, offering a useful starting point for threat mitigation at the nexus of AI and cyber

issues. In sum, IT&E agreements could be used to make headway establishing best practices—and eventually testing standards—for the technical and procedural dimensions of interoperability, as well as AI safety and security.

IT&E Agreements: Limitations

The most obvious weakness of IT&E agreements is that the United States does not have IT&E agreements with allies in the Indo-Pacific region. The only Indo-Pacific countries that the United States can engage in these flexible testing arrangements with are Australia and New Zealand, via the MTEP between Five Eyes countries. Japan, South Korea, and India would need separate mechanisms or newly negotiated agreements to use IT&E provisions like pay-per-use tests or exchanges of testing data.[34] While a multilateral Euro-Atlantic agreement is currently being negotiated, there are no announcements for an Indo-Pacific equivalent.

Further, finding the right talent to populate working groups for collaborative TEVV may be a challenge. If collaborative testing arrangements become more expensive, then EU countries may be inclined to dedicate joint investments to intra-European infrastructure as part of a greater "strategic autonomy" or "technological sovereignty" agenda. Lastly, partners and allies may hesitate to share testing data if it means disclosing or revealing the vulnerabilities of their systems.[35]

These limitations notwithstanding, as TEVV becomes an important part of the AI pipeline, IT&E agreements are overall well suited for increased AI cooperation between democratic countries. Although these agreements are only available to a small number of close allies and partners, the benefit is that these countries already have experience in navigating political sensitivities and other barriers from previous collaborations. Moreover, the IT&E agreements themselves provide the necessary mechanisms to legally share data. Rather than limiting the utility of these tools, it may just make it more important for countries to pre-select their own baselines for what parts of TEVV they are most willing to exchange data on. As

explored elsewhere in this report, this may also extend to trial and experimentation activities.

Reciprocal Defense Procurement and Acquisition Memoranda of Understanding

- **RDP MOU partners and allies:** Austria, Belgium, Canada, Czech Republic, Denmark, Egypt, Estonia, Finland, France, Germany, Greece, Israel, Italy, Japan, Latvia, Luxembourg, Netherlands, Norway, Poland, Portugal, Slovenia, Spain, Sweden, Switzerland, Turkey, and the U.K.
- **Reciprocal Government Quality Assurance MoUs:** Czech Republic, Finland, South Korea, Poland, Romania, and Slovakia.[36]

RDP MOUs are bilateral agreements that aim to improve interoperability and facilitate cooperative R&D, co-production, and cooperative logistics support. Each of these areas is necessary to build political trust between countries for technology cooperation, but especially for AI because interoperability is dependent on countries' willingness and ability to share sensitive data and align software processes. RDP MOUs can help jumpstart such AI interoperability efforts because they are structured to level the playing field between countries.[37] The reciprocity that this creates could help countries advance the state of the art in shared AI research priorities and better coordinate on adoption pathways. With political trust, AI advancement, and adoption in mind, this section offers four ways that specific mechanisms of RDP MOUs can benefit military AI cooperation. Depending on the level of cooperation desired, the implementation of these four areas could be carried out independent from one another, or in tandem.

RDP MOUs: Advantages

First, these memoranda can be used to create AI development alternatives that will not require countries to share large swaths of highly sensitive data.[38] While the name of these agreements spells out their focus on procurement and acquisition, it is the clauses on cooperative R&D that are more relevant to the question of data

sharing.[39] More specifically, DOD can use RDP MOUs to collaboratively invest in in techniques that help preserve privacy, improve safety and security, and reduce the amount of data needed for AI development.[40]

A few of these privacy-preserving techniques deserve mention here. For example, federated learning allows for training to take place on devices rather than transferring data to a centralized network. Another technique is homomorphic encryption, which allows calculations on encrypted data without decrypting it. Both may offer workaround options to sharing or revealing sensitive data for joint capabilities.[41] For their part, synthetic datasets allow algorithms to train on data that has the same structure as data collected from sensors, without having to reveal the real characteristics of the data. Synthetic training environments may also provide useful data that can be used for testing—especially because AI-enabled systems will require more use of virtual and blended environments, not just intermittent tests for a small number of high-end systems.[42]

Cooperative R&D on privacy-preserving techniques could also supplement other research on making AI models leaner. Lowering compute requirements could spin into more cooperative opportunities, particularly because militaries do not necessarily have sufficiently sized datasets for training.[43] Among others, advancing research in these areas could pay dividends in later stages of cooperation. Over time, mainstreaming these techniques through cooperation could also help make them more affordable and make data more representative of what coalition partners should expect in operations.

Second, and relatedly, RDP MOUs also include the option to draw up subordinate Data Exchange Annexes for partners to exchange classified R&D information in specified technology areas. RDP MOU Data Exchange Annexes delineate precisely what technical data can be exchanged, often in the form of lists of weapons systems and subsystems that may be subject to future cooperation. These annexes are attractive because they allow users to calibrate the level of data exchanged depending on its level of sensitivity, meaning that DOD can take political realities

into account when sharing data. One example that gives a sense of how these RDP MOU annexes can be used is the U.S.-Israeli Data Exchange Annex from 1970, which shows how they can be used for basic research, including on less sensitive projects.[44] This publicly available precedent shows how they may be of use to broadly develop the "respective technology bases of the two countries, not necessarily in relation to specific operational requirements."[45] In other words, Data Exchange Annexes can be used for the general advancement of military-relevant technology and broadly defined goals.

As a more specific precedent that could be useful in the digital age, the U.S.-Israeli agreement allowed for information and data exchanges for "software development methodologies."[46] This example suggests that early cooperation efforts can focus on the software fundamentals at the policy, procedural, and technical levels prior to getting into questions about sharing more sensitive sensor data. This is important because it could allow the DOD to create buy-in for more effective data sharing by starting with alignment on software methodologies and processes (e.g., agile development, DevSecOps). This cooperation underscores all algorithmic adoption, be it for AI or non-AI systems, and thus could benefit other military digitalization efforts that are more focused on network-centric warfare than explicit AI adoption. Another area where the U.S.-Israeli annex shows promise for countries to calibrate how much sensitive data they are willing to share is projects that "include technology assessments and forecasting, development of advanced technologies, testing of new technologies (including techniques, facilities, and instrumentation)."[47] By connecting R&D to other cooperative activities in this report—including the TEVV pipeline and technology forecasting—this point shows how RDP MOUs can cohere with other tools at DOD's disposal if properly integrated for AI.

Third, at a higher level, RDP MOUs could be helpful to align policies on AI adoption because the memoranda already require national armaments directors to meet on a regular basis and coordinate on new acquisition methods.[48] These consultations could facilitate adoption and interoperability, with a specific focus on the

processes that relate to acquiring and integrating AI into capability development. This dovetails with the NSCAI recommendation to implement AI cooperation and standards "through the [NATO] Conference of National Armaments Directors and associated subgroups and informed by international normative and technical standards bodies."[49] At the bilateral level, RDP MOUs create such subgroups. Countries with RDP MOUs could likewise set up bilateral armaments committees below the director level that focus specifically on AI-enabled and autonomous system capability development. While not a prerequisite to engage in armaments cooperation, this framework can help promote collaborative innovation at cost, especially if countries start with different base levels of technological advancement.

Lastly, other annexes of RDP MOUs could also be used to tie R&D to emerging best practices on risk management and quality control mechanisms for AI. The language in the annexes themselves focuses mostly on quality assurance and standardization. Standardization is central to military cooperation because it creates common frameworks for armed forces to communicate and interoperate, and also forms a basis for operators to trust the systems they are using together. But because AI standards are not yet defined, other quality assurance frameworks—including ones that could eventually culminate in standards—are needed to create this interoperability and trust. As such, cooperative activities that use RDP MOU frameworks could focus on best procedural practices like benchmarks, federation agreements, audit trails, stage-gated development processes, certification and accreditation recommendations, and reporting requirements.

As a brief aside, this focus on quality assurance is relevant not only because standards are not yet available to implement, but also because the United States has other quality assurance agreements that are less comprehensive than RDP MOUs with other countries, including South Korea.[50] These are called Reciprocal Quality Assurance MOUs, which are far less comprehensive than RDP MOUs. Still, if the DOD chooses to set up other AI-related project arrangements with allies like South Korea, then the Reciprocal Quality Assurance MOU could be useful for quality-assurance support. Used as such, they could help frontload interoperability

efforts into the early stages of cooperation, and equally focus on AI safety, security, and reliability in lieu of current standards.

RDP MOUs: Limitations

The limitations of RDP MOUs mostly relate to the data pipeline, which speaks to the broader context in which AI cooperation will take place. The option to draw up Data Exchange Annexes is not sufficient to guarantee that they will actually be implemented. Even if used for on basic research and software methodologies, data exchanges are still limited by the countries' willingness to trust one another.

While effective collaboration will depend on allies' ability to resolve these data pipeline challenges, or at least alleviate associated privacy and security concerns, the techniques described above are not necessarily suited for short-term wins because they are still relatively immature and costly. For instance, the associated compute expenses for federated learning are exorbitant—estimated to be tenfold relative to learning on centralized data—and could risk cancelling out any cost rationalization gained by pooling resources.[51] Higher costs do not mean that federated learning is impracticable, but rather that it would be more valuable for narrowly targeted priorities, as opposed to being a silver bullet for privacy-preserving AI. With these important caveats in mind, the long-term promise of machine-learning techniques that can reinforce privacy and make inroads to partners' comfort levels in exchanging data does make R&D in these areas more urgent. Until then, these techniques may be more attractive as workaround solutions for niche, cooperative R&D areas until breakthroughs help reduce these barriers.

Another important factor is that data rights may limit military-to-military cooperation when owned by the private sector. This is because provisions of RDP MOUs create opportunities for governments to exchange the data they themselves own, however most defense contracts give contractors the data rights. This has been cited an obstacle to U.S. military adoption, even before considering the challenges of international cooperation. As such, the ability of these legacy agreements to permit data exchanges

between countries will often be dependent on industry's willingness to share data they own.[52] RDP MOUs stipulate that governments can "seek appropriate agreement with their industries that in the interest of standardization and armaments cooperation, proprietary rights in defense-relevant information and data can be transferred by appropriate arrangements and on fair and reasonable terms, between the industries of the two countries."[53] While data exchanges between contractors in different countries could indeed be useful to fulfil aims of cooperation, the feasibility to do so is not automatic because it depends on the data owners, not just governments.[54]

While much of this section has focused on utilizing RDP MOUs for collaborative R&D, 'procurement' is also in the title of these agreements. It is, however, unclear what benefits the agreements extend to joint procurement in the digital age, especially given the carveouts for national preferences which limit their utility for foreign participants competing in U.S. procurement. Moreover, countries with their own established national sovereignty preferences, like France, may still choose to not exercise their RDP MOUs with the United States in favor of their own suppliers. As such, procurement may be a backburner priority in relation to the other benefits of RDP MOUs for military AI cooperation.

Bilateral Military AI Agreements and Cooperative S&T Blueprints

Whereas the two tools above consist of structured opportunities for military AI cooperation, a host of other initiatives offer additional useful ways forward on military AI cooperation. The selection here focuses on bilateral AI agreements that create linkages to foreign national security innovation bases, as well as pathways that do not yet orient toward AI but could with only minor adjustments.

Bilateral Military AI Cooperation Agreements

DOD already has many project arrangements that create *ad hoc* cooperation opportunities with defense technology communities in other countries, but only a small number of recent initiatives target new forms of military AI cooperation.[55] This section focuses on two such formats, one with Singapore and the other with the U.K.

Military AI collaboration is already taking place. The JAIC technology collaboration with the Singapore Defence Science and Technology Agency, agreed in June 2019, is different from other AI-related project arrangements in that it names a specific area of cooperation, and is not necessarily service-specific.[56] This collaboration focuses on the mutual operational interest of humanitarian assistance and disaster relief, a relatively non-controversial area.[57] This echoes calls from several analysts to begin international military AI cooperation with lower stakes and the possibility to scale into larger initiatives.[58]

The centralization of AI efforts in the JAIC may portend an eventual hub-and-spokes model for cooperation. This is because its location and reporting structure in the Office of the Secretary of Defense (OSD) could promote coordination with the military departments to either work across combatant commands or cut across operational domains. Further, the coordinating role played by the JAIC could make the cooperation more visible and easier to assess as a blueprint for other countries. On this note, it could be seen as a pilot not just for U.S.-Singaporean collaboration, but also as an inspiration for similar efforts with partners in the Indo-Pacific region, which are under-represented in the toolbox here.

With the U.K., the Bilateral Academic Research Initiative (BARI), launched in 2018, focuses on creating academic collaborations. More specifically, this collaboration could take the form of grants and fellowships on AI research. With the inaugural pilot program selected to focus on human-machine teaming, DOD and the U.K. Ministry of Defence will respectively sponsor up to $3 million and £1.5 million for the multidisciplinary, academic team to conduct the "high-risk basic research as a bilateral academic collaboration."[59] Notably, while the allies with the same level of intelligence access as the U.K. are numbered, the broader academic and scientific focus of the BARI pilot could be replicable for basic and applied research with many more countries willing and able to co-fund these ventures.

The flexibility of these forms of collaboration is overall a strength. That said, for both examples here, the military AI collaboration projects fit into existing, overarching frameworks of cooperation, as

declared by the heads of state or defense minister counterparts.[60] Without these broader frameworks, similar working-level relationships may be seen as *ad hoc*.

Cooperative S&T Blueprints

Whereas the above bilateral cooperation agreements are already oriented toward AI, the defense technology cooperation tools discussed below could be integrated into the toolbox for AI, but have not yet done so.

One example of such S&T blueprints is the Allied Prototyping Initiative. Launched in 2019 by the Office of the Under Secretary of Defense for Research and Engineering (OUSD/R&E), the Initiative funds a small number of cooperative operational prototypes related to the top DOD modernization priorities. Under the Initiative, the United States can identify transition pathways for operational capabilities in the five- to seven-year horizon, including future co-development with the U.S. national security innovation ecosystem.[61] So far, the program has funded prototypes for high-speed propulsion technologies with Norway and hypersonic vehicles with Australia.[62] But given its focus on DOD technology modernization priorities, the Initiative can also oversee prototyping related to AI and machine learning, autonomy, microelectronics, and fully networked command, control, and communications.[63]

Building on existing international cooperation agreements such as IT&E agreements, future Allied Prototyping Initiative project arrangements can help further identify the extent of TEVV and technology transition funding focused on AI-enabled and autonomous systems. In fact, it may be better suited for this task than the longer-standing, counterpart program, Foreign Comparative Testing.

Another small, regional agreement that can serve as a blueprint for AI cooperation is the Polar Research, Development, Testing, and Evaluation arrangement between the United States, Canada, Denmark, Finland, New Zealand, Norway, and Sweden.[64] Just as this agreement is based on a "shared desire for strong cooperative relationships that preserve safe, stable and secure Polar regions,"

other minilateral arrangements—such as the Quad—could use this as a blueprint to align R&D and TEVV priorities with a free, open, secure, and prosperous Indo-Pacific.[65]

While notable, these programs are small and limited in scope. Their utility depends largely on the willingness to emulate existing cooperation avenues to new ends, rather than focusing on more familiar areas with more established track records. Prototyping cooperation, for example, may be easier for countries to use for hardware and platforms, in contrast to other forms of trials and experimentation that enter into AI TEVV processes.

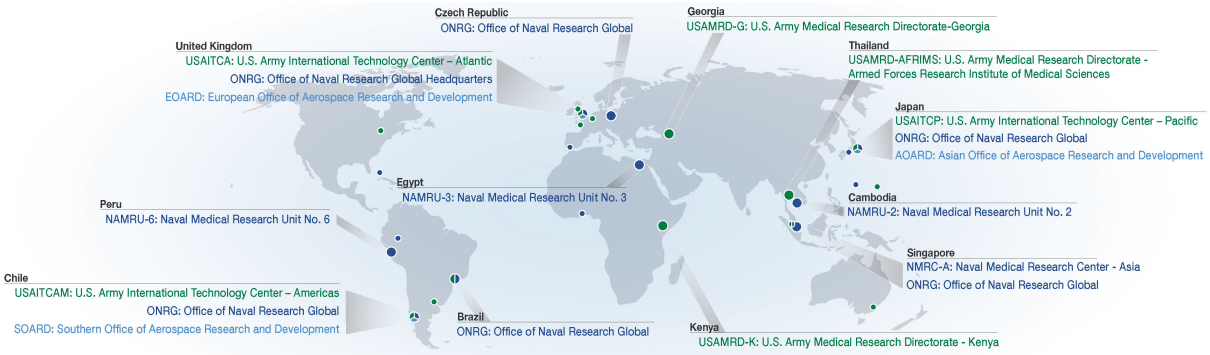
Global Military Science and Technology Network

This second category of tools focuses on talent linkages between the United States and its allies and partners, which are mainly facilitated by the individual military departments (*i.e.*, Departments of the Air Force, Army, and Navy). Overall, increased access to the global technology base is an important counterweight to the increasingly isolated innovation ecosystems of rivals, particularly given that there are more AI hubs in allied and partner countries than not.[66] Given the multidisciplinary, general-purpose nature of AI, connections with the global talent base will be important for the United States to improve technology monitoring and scouting. The convergence of different research disciplines entails increasing complexity for future technological advancements. Together, these trends make it unlikely for the United States to have fully independent leadership in all of the emerging and combinative research areas. In this vein, leveraging the global military S&T network and engaging in global technology monitoring and forecasting also offers other entry points for DOD to better track and incorporate AI research from abroad.

U.S. Military Global S&T Presence

Military S&T assignments overseas, grants, and cooperative workshops can help the United States harness the strengths from foreign innovation bases. Each of the military departments has its own foreign S&T research centers and laboratories, which can be leveraged for AI and other emerging-technology priorities.[67] These are, namely, the international detachments of the Air Force Office of Scientific Research, Army Combat Capabilities Development Command and Army International Technology Centers, and the Office of Naval Research. As Figure 1 illustrates, they reach both the most-trusted allies, as well as other countries with which DOD does not have formalized reciprocal R&D, testing, and procurement agreements.[68]

Figure 1: International S&T Detachments from the Departments of the Air Force, Navy, and Army



Source: Department of Defense Research & Engineering Enterprise.[69]

U.S. Military Global S&T Presence: Advantages

In engaging the international S&T community, the military departments are able to stay up to date on trends and developments across the global S&T landscape. They can also scout for new technologies and "socialize new S&T ideas or findings" with the U.S. research community.[70] This global reach in foreign technology bases offers opportunities to the United States to both foster military research networks and to match foreign products and services with domestic U.S. military customers. In addition to placing small investments and connecting foreign-based researchers with the U.S. military, these international detachments also administer international testing and support initiatives.

With the diffusion of technology, meeting researchers where they are helps reinforce technology partnerships both with leading hubs in like-minded countries, and in underserved areas. Most of the time, DOD personnel overseas have regional mandates, which means that science advisors and envoys can connect with researchers in even more countries than the map indicates.[71] Moreover, science advisors do not need to already work in military laboratories in order to qualify for postings in embassies overseas.

Through short-term visits, conferences, and small research grants, there are many activities to track. The reputation of organizations like the Office of Naval Research, in addition to the stability of funding from the U.S. government, help their brand when

represented overseas. As such, research grants and networking can increase understanding of the global pipeline for "future friendly capabilities."[72]

U.S. Military Global S&T Presence: Limitations

While other tools described in this report provide helpful frameworks to exchange on policies and institutional procedures, these global networks are not intended for policy use because the exchange officers are not liaisons or official government representatives.[73] These military-funded outfits nonetheless have the resources to conduct scientific diplomacy, especially increasing awareness of new innovators and institutions. Yet while they could complement their State Department counterparts, it is unclear how coordinated these different kinds of scientific diplomats would be.

Generally speaking, the individuals who take on these roles get to shape the direction of the research based on their own experience and own networks. The flexibility works well to meet the diversity and breadth of global S&T communities, but at the same time, there is no structured process for engagement. The results are therefore highly dependent on the individuals themselves. Indeed, these scientific networks have been looking at AI and adjacent research areas for decades, including in areas and applications relevant to DOD priorities. There are, however, few feedback loops for the knowledge these individuals have to filter upward and for their results to inform strategic thinking about technological evolution around the globe. This has consequences for the ability of DOD stakeholders to act on the information, as picked up in the next section.

Technology Monitoring and Forecasting

Global military S&T networks also provide valuable information about the state of research in different research hubs, including tracking for breakthrough developments beyond U.S. shores.

Technology Monitoring and Forecasting: Advantages

As AI investments become clearer, coordination between these networks can help not only to increase availability and integration of technology for the U.S. military, but also to improve technology monitoring and forecasting of technology-driven changes in the international system. As the NSCAI recommends, global monitoring of emerging technologies in near-real time is critical to the United States monitoring technology progression, from basic research to prototyping to fielding.[74] By extension, this has implications for the ability of DOD to leverage innovations from the global economic system and assess cooperation prospects with foreign researchers.

Here, each of the activities that the international military S&T detachments undertake is a potentially useful datapoint for global technology awareness. In this vein, the information they collect may be valuable to insert into technology roadmaps and U.S. strategy so that the United States is at least aware of, and possibly can capitalize on, as broad a range of innovation assets as possible. Making sure that the global technology awareness these detachments help provide is actionable, however, is a task that requires more coordination.

Technology Monitoring and Forecasting: Limitations

At present, these S&T partnerships in the military departments are underleveraged. One reason that their work often goes unnoticed is that it is difficult to advertise the successes of basic research in relation to more tangible gains that can be measured in more applied and advanced stages of technology development. A more fundamental challenge, however, is that these vast networks do not have databases or directories where they log their activities. Even if researchers wanted to share information about their work, they may not know who they should communicate with across the different offices and military services. Without an overarching structure, their research can be duplicative, difficult to measure, and almost impossible to act on.

This lack of a unified structure undermines the ability of these networks to gather all their discrete datapoints, which could otherwise culminate in a unique tracking system for global technology trends. Tracking global technology trends was intended to be one of the three main components around which the OUSD/R&E was organized.[75] Although OSD is best positioned to use the information garnered from these global networks for strategic foresight, at present, the international detachments are organized to work better among themselves rather than through OSD.

Addressing this disconnect, the NSCAI has recommended that DOD reconceive the Strategic Intelligence Analysis Cell, in part for OUSD/R&E to better fulfil its global technology tracking responsibilities and lead an interagency technology scouting community of practice.[76] The NSCAI includes international security partners in this community of practice.[77] If Congress adopts this NSCAI recommendation, there is also room to include the international S&T detachments of the military departments here. Without the Strategic Intelligence Analysis Cell or equivalents reporting directly to the Under Secretary of Defense for Research and Engineering, the extent of coordination between the three military departments is *ad hoc*, depending more on co-location of scientific directors and advisors in the overseas offices.

Currently, the actionability of technology trends largely remains limited to the respective priorities of each military service, focused more on relationships with customers and researchers than with strategic decision-making bodies. Although beyond the scope of this study, improving the actionability of global technology awareness will also entail more interagency collaboration, including with the State Department and the National Institute of Standards and Technology.

Military S&T Exchanges

Together with the policy, procedural, and technical-oriented personnel and working groups described in relation to IT&E agreements, exchange programs are also key to building mutual understanding and capacity between countries interested in

military adoption of AI. Forms of secondments between innovation-centric organizations, be they between innovation units or strategic-level exchanges, can help internationalize the talent pipeline of experts.

Military S&T Exchanges: Advantages

Exchange programs that include civilian policy experts or military officers from different allied countries exemplify collaboration and can create momentum for more joint activities. Recent examples include secondments of personnel, such as a U.K. liaison officer in the Defense Innovation Unit and a Dutch foreign exchange officer in the JAIC.[78] Reported plans for the Defense Innovation Unit to host an Indian military officer show that these exchanges can also include non-treaty allies.[79] Making use of the range of less formal exchanges, networks of liaison officers, and short-term exchanges can help ensure that policy priorities match the more technical side of AI-related talent exchanges. In addition to these exchanges, the multilateral institutions explored in the following section also have entire dedicated structures through which personnel cooperate.

Service-level exchange groups are another option. The Air Force Trilateral Strategic Steering Group (TSSG) between the United States, France, and the U.K. is an example of this. Senior personnel (typically colonels/wing commanders) in the offices of the Chiefs of Air Force of the three allies "cross-pollinate ideas and concepts that directly influence the employment of airpower" through annual exchanges.[80] Since its establishment in 2013, the TSSG has become a forum to exchange views and seek interoperability initiatives, more recently focusing on AI and airpower. As previous participants have noted, such minilateral arrangements are easier and less hierarchical than treaty-based exchanges, meaning that they rely on "initiative and creativity" to be more "innovative in [their] approach," even if that means sacrificing organizational authority that other empowered entities have.[81] For emerging areas of cooperation such as AI, this flexibility can be used to garner will for other joint investments. As such they are complementary to other formal arrangements. It is conceivable to imagine the TSSG or similar formats to come up with mutually beneficial ideas, and then use other agreements to implement them.[82] While the

feedback mechanisms are not as formal as reporting structures in alliances, as discussed with regards to NATO below, their location in the offices of the service chiefs can be used to elevate the benefits of the S&T agreements described above.

Relatedly, the military departments also manage international Engineer and Scientist Exchange Programs (ESEPs) to cooperate on specific, longer-term projects. ESEPs allow individuals from friendly countries to cooperate on shared technical modernization priorities and understand each other's R&D processes. They are not intended for technical training or technical data transfers.[83] As such, assessing their applicability to some of the multidisciplinary research areas that are important to AI, including social sciences, may be of use. Importantly for Indo-Pacific relations, forthcoming ESEPs with India and Taiwan will also facilitate exchanges between government scientists.[84] When finalized, that will make them the only tool surveyed here that explicitly allows for military S&T talent exchanges with these key partners.

Separate from government-to-government exchanges, international cooperation could indirectly borrow and benefit from government-to-industry exchanges as well. One important example is the Training with Industry and Tours with Industry programs, which the U.S. military departments independently run to allow active-duty personnel to serve a "tour" inside U.S. companies. The exposure to multinational companies like Microsoft and Amazon can inform the ways that personnel think about the procedural, organizational, and cultural aspects of technology adoption, as much as the technology itself.[85] While domestically focused today, international components could conceivably learn best practices from the experiences of individuals who have completed the programs. Already, recommendations to improve the DOD talent pipeline emphasize exchanges as the basis for international components of "digital corps."[86] Building on this, relationships with multinational companies whose AI research centers are based in allied and partner countries may also be of use.

Military S&T Exchanges: Limitations

For exchanges that include civilian policy experts and military officers, there is a tradeoff between structured agreements and flexible exchanges. The TSSG format is exemplary of this tradeoff. On the one hand, the role and connections between personnel and bodies typically include direct, actionable lines of effort in negotiated agreements and treaty-based alliances. This means that the reporting structures give them the authority to follow through on identified priorities within the hierarchy. On the other hand, other informal exchanges may help sidestep bureaucratic hurdles and allow greater flexibility in aligning AI policies and strategic priorities. This tradeoff does not necessarily have to be a liability, but recognizing the limitations of flexible exchanges is important to ensuring they are appropriately used.

Furthermore, sending key personnel abroad may pay dividends in gaining relevant expertise, but some countries may perceive it as undesirable. The number of technologically savvy experts who also have a solid grasp of technology policy priorities and broader strategic dynamics is limited, especially in comparison to the relatively larger international S&T networks of engineers and natural scientists involved in collaborative R&D programs. As such, while these exchanges are beneficial to aligning on policy, the domestic demand for their unique skills may make governments reluctant to second them to other countries.

Nevertheless, the examples above, in addition to the international institutions discussed below, do offer pathways for policy alignment and mutual understanding between partners and allies. And as more U.S. partners and allies stand up units dedicated to emerging technology and defense innovation, short-term assignments, as opposed to multi-year tours of duty, may be more appealing to those who need to keep limited AI expertise in-house.

Multilateral Alliances and Partnerships

While the aforementioned tools mostly offer pathways for militaries to cooperate on TEVV, R&D, policy alignment, and exchanges, these goals can also be accomplished through existing multilateral institutions with deep experience in military S&T cooperation. The main institutions here are NATO and Five Eyes, and, to a lesser extent, the newer JAIC AI Partnership for Defense (PfD). There are multiple pathways to enhance AI cooperation in these formats, and in fact advances from the agreements and exchanges above can be seen as individual increases that benefit broader alliances. The goal here is not to be exhaustive, but instead to spotlight the relevance of these institutions in two ways.

First is the possibility to harvest data from existing cooperative activities—such as exercises, training, and of course, operations—for AI experimentation. Within NATO and amongst the Five Eyes, the regularity of these activities makes them a natural starting point for fuller exploitation of the data. In fact, select multinational exercises incorporating dozens of unmanned systems have already set this groundwork by testing interoperability and developing tactics, techniques, and procedures. As such, the utility of this data is perhaps most obvious and immediate for interoperability between unmanned and autonomous systems and testing human-machine teaming in coalition environments.

Second is strengths that each of these institutions offer. Although numerous, this report only highlights the select areas of experimentation and military standardization for NATO and strategic challenges within Five Eyes. This is also where the PfD comes in, with its unique standing to align policy and procedural views on adoption of responsible AI amongst a broader group of democratic countries, which includes non-treaty allies.

North Atlantic Treaty Organization (NATO)

- **NATO Allies:** Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia,

Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, U.K., and the United States.[87]

As one of the primary formats through which the United States advances defense rationalization, standardization, and interoperability, it goes without saying that NATO is central to realizing the benefits of defense technology cooperation. While its organizational structures are beyond the scope of this report, it is worth briefly noting that several NATO organs have experience with the political, operational, process-oriented, and technical aspects of AI. These include the Conference of National Armaments Directors, Allied Command Transformation (ACT), the NATO Science & Technology Organization (STO), the NATO Consultation, Command and Control Board (C3B), the NATO Communications and Information Agency, and the NATO Standardization Office, as well as the newer NATO Innovation Advisory Board, Innovation Unit, and Data Policy Unit.[88]

Through these bodies, the United States supports various strands of work on AI to ensure that the alliance can anticipate AI-enabled threats and moderate the interoperability gap between allies pursuing different generations of military modernization. The alliance's high-level policy interest in emerging and disruptive technologies (EDTs), including AI, dates back to 2019 and builds on years of groundwork set by ACT and STO.[89]

Defense ministers endorsed the 2019 EDT "Roadmap" and 2021 EDT "Coherent Implementation Strategy," which have set the agenda to integrate and bolster NATO's work on AI.[90] This agenda includes other critical guiding documents, including the 2020 NATO White Paper on AI, the Data Exploitation Framework Policy, and the expected NATO AI Strategy.[91] In these documents, the NATO approach to EDTs is based on the motto "adopting and adapting."[92] This entails five complementary goals: "(1) better understand emerging disruptive technologies; (2) properly look at their implications for defense; (3) decide about their use; (4) mitigate their risks; and (5) exploit their advantages."[93] Together, these documents demonstrate how the alliance sees its role coordinating and facilitating AI adoption, as well as protecting against AI-driven changes to its operating environment.

NATO's longstanding technical and operational groundwork focuses on foundations for AI adoption, rather than development. That said, the announcement at the June 2021 Brussels summit that NATO will establish a defense innovation accelerator and innovation fund may facilitate both.[94] The groundwork on which these developments build includes AI ontologies and taxonomies, operational and materiel standards for data and man-machine teaming, interoperability initiatives, military data management studies and working groups, federated accreditation models for modelling and simulation (M&S) and validation and verification, pilot projects, cloud infrastructure, and more.[95] Through forums like the Conference of National Armaments Directors and NATO C3B, consultations also help align on acquisition and information sharing. With these building blocks, the multilateral alliance is an important venue to advance military AI aims. That said, it will be harder to come to consensus between all 30 Allies, and cooperation often takes place in initiatives between smaller groups of Allies outside of the NATO framework.[96]

One unique area where NATO has clout is military standardization. Broadly speaking, standardization is important not only to secure economic first-mover advantages and establish a level playing-field, but also to ensure that systems are safe, secure, and interoperable.[97] Even with its decreased funding in recent years, the NATO Standardization Office remains the largest military standardization body.[98] It therefore is a natural convening point to see which civilian standards can apply to the military realm, as well as identify niche areas where military AI standards require dedicated attention.

In NATO, standardization agreements (STANAGs) already cover several aspects of interoperability between communications and information systems, including for imagery formats, data storage interfaces, and data links.[99] Further, data security measures improved in STANAGs in 2017-8, with focus not just on labelling for confidentiality (classification level), but also integrity and availability. These are critical fundamentals for future AI developments, yet national implementation is more difficult than the process of agreeing on the standards themselves. The aforementioned RDP MOUs—many of which are in place with

NATO allies—could be used as bilateral support mechanisms that implement these NATO standards, so as to ensure that bilateral efforts support NATO priorities on data and EDTs.

As AI standardization efforts crystallize around data protocols and model documentation, the NATO Standardization Office will have to be careful to not duplicate civilian efforts that can apply to this dual-use, general purpose technology. Tying technical requirements to operational standards is a helpful place to start.[100] For instance, the NATO Standardization Office could focus on "the level of robustness required for a given operation," an imperative question that does not have civilian equivalents.[101] Technical standards defining thresholds for use in military operations could be even more specific, for instance requiring documentation for lighting conditions of training data which could impact the performance of systems in different environments.[102] Another example could be tying documentation to the acceptability of using an AI-enabled decision support system depending on the operational environment (e.g., urban versus rural, no people in a specified radius, desert versus mountain, coastal whitecap sea versus open waters, etc.).[103] Agreeing to quality control and standardization on these issues could help developers and operators understand the limits of training data and the transferability of AI-enabled systems for coalition operations.

NATO also recognizes that, in order to operate effectively, interoperable forces need to consider how their AI-enabled and autonomous systems integrate with one another at the technical, procedural, and human levels.[104] The rapid increase of U.S. allies and partners developing and operating multiple autonomous systems enhances the urgency of coordination and interoperability between the systems for military effectiveness.[105] Human-machine teaming makes this even more pressing because countries conceive of the relationships between operators and AI systems differently.[106] As such, the focus on AI adoption naturally means a focus on multilateral integration and interoperability.

Current experimentation efforts on unmanned and autonomous systems could both advance interoperable AI adoption and inspire future AI developments. NATO STO has led much of the technical

work, and is engaged in activities that could lead to more exploitable data for AI. One example is the maritime exercise held in September 2019 under the auspices of NATO's Maritime Unmanned Systems initiative.[107] With 800 personnel associated with allied militaries and the NATO Centre for Maritime Research and Experimentation, the exercised involved dozens of unmanned systems with the aim of building "technological and procedural interoperability" into operations.[108] Whether the data from these activities is structured and stored for future use is a separate question. Still, it is worth exploring how the data collected from such open-air and open-water exercises can feed into T&E procedures, which in turn can be used to test the performance of systems of systems.[109]

Relatedly, cybersecurity assessments can also be included in exercises.[110] This is important to both testing the protection of AI systems against failure modes, as well as a proof-point of more digital assessments that fit in line with different types of evaluations in real-world scenarios. In the future, as these exercises focus on the integration of various unmanned systems with different levels of autonomy, the data can also be used to document emergent behavior, so as to reduce unpredictable and undesirable behavior arising from multi-agent systems. In anticipation of this, building documentation practices early will be a necessary first step to ensure that testing personnel are familiar with multi-agent systems and the concept of emergent behavior. Considering human factors in multinational settings is another vital aspect of understanding system behavior in real-world contexts. All in all, seeing testing and training as complementary processes, NATO can continue to build on live exercises that are used for experimentation in concepts related to AI security, human-machine, and machine-machine teaming.

Finally, NATO experimentation can also converge with its existing M&S competencies. NATO is well suited to play a role here given its experience coordinating between national M&S structures both through the NATO STO M&S Group that focuses on standardization and common services, as well as the M&S Centre of Excellence with competencies in education, integration, and certification.[111] Moreover, concerns about emergent behavior

heighten the need for common M&S frameworks so that allies and partners—in and out of NATO—can better anticipate how their systems will interact during operations. To that end, M&S is increasingly important to test high-end capabilities and autonomous systems for which current testing regimes are insufficient, either because testing the systems in live ranges is impossible or too expensive. Militaries are already familiar with the need for simulated testing environments for high-end capabilities, including in coalition settings.[112] These competencies dovetail with the TEVV methods described above, including in relation to synthetic training environments.[113]

Five Eyes

- **Five Eyes countries:** Australia, Canada, New Zealand, U.K., and the United States.

Five Eyes should be noted for initiatives linking standardization and interoperability, including those that NATO has dedicated bodies working on. In addition to the aforementioned MTEP between Five Eyes countries, the Technical Cooperation Program (TTCP) international organization, as well as the ABCANZ Agreements for Standardization and Five Eyes Air Force Interoperability Council, create a helpful architecture for defense technology cooperation.[114]

In particular, the Five Eyes TTCP is a valuable venue for AI experimentation because of the high degree of political trust between the five anglophone allies. Further, the intelligence sharing agreements between the five allies may offer better avenues to exchange sensitive data, which TTCP can use.[115] Through TTCP, the Five Eyes cooperate on strategic challenges that lend themselves to the integration of AI and autonomy. Accordingly, the TTCP Autonomy Strategic Challenge and TTCP AI Strategic Challenge are the two most relevant examples here. As part of the TTCP Autonomy Strategic Challenge, engineers from the Five Eyes countries collaborated on command and control (C2) integration software as part of the "Wizard Series."[116] In November 2018, Australia hosted an exercise called *Autonomous Warrior*, which included the capstone "Wizard of Aus" C2 software trial.[117] The exercise included total of 450 personnel from the Five Eyes

countries and more than 100 engineers who worked on and tested the Allied Impact (AIM) C2 software system.[118] AIM includes multiple software components from Australia, Canada, the U.K., and the United States that aim to enable a single operator to control 17 different unmanned systems.[119] As a human-machine teaming assessment tool including a recommender system, the software from this exercise aims to improve coordination across assets from different countries.[120] The combination of developing C2 software *and* the ability to trial it during exercises is a useful format to encompass different stages of AI development.

TTCP is also sponsoring the three-year-long AI Strategic Challenge for research related to trustworthiness, international legal implications, and technology transition.[121] This helps combine the weight of signals intelligence sharing with exploration of AI applications for military cooperation. In some ways, this is a natural progression from the precedent of the Five Eyes sharing data for Project Maven.[122]

While the TTCP AI Strategic Challenge is in its earlier days, the AIM example from the Autonomy Strategic Challenge shows how TTCP strategic challenges can facilitate technical cooperation across the different stages of the technology lifecycle. By combining intelligence collection, data sharing, software development, and exercises and experimentation, Five Eyes countries have already begun integrating AI into their interoperability efforts, and can continue to do so through future strategic challenges.

With greater access to each others' facilities and assets than is the case for most other defense relationships, Five Eyes may also be a suitable format to operationalize standards, including those developed within NATO. All in all, the high level of cohesion, AI exploration through data sharing for Project Maven and the TTCP AI Strategic Challenge, and complementary agreements on standardization and interoperability may mean that Five Eyes is an effective venue for cooperation with fewer of the political trust-related caveats described relative to other partnerships.

AI Partnership for Defense (PfD)

- **PfD countries:** Australia, Canada, Denmark, Estonia, France, Finland, Germany, Israel, Japan, Norway, the Netherlands, Singapore, South Korea, Sweden, U.K., and the United States.

The JAIC supports international engagements across all levels discussed in this paper, including the MOU with the Singapore Defence Science and Technology Agency, talent exchanges, and coordinating activities with NATO. Yet its most prominent contribution to international engagement is the creation of the PfD, a forum for like-minded countries to share practices and coordinate on AI policy and adoption.

PfD merits attention as an avenue for cooperation precisely because it is not a formally negotiated agreement, and can therefore capture a broader selection of countries. As the PfD develops, the flexibility of the format will allow future participants and more concrete policy topics to exchange views. This makes it a notable complement to both the international defense S&T cooperation tools, in which key allies like Japan and South Korea are under-represented, as well as alliances, which do not include partner countries like Finland, Israel, Singapore and Sweden.

Thus far, PfD discussions have touched on interoperability in policies and processes, more than they have technical measures for data exchange and technology transfers. This is seen in the focus on responsible AI in the first two meetings.[123] Adding to these priorities, the third meeting also covered workforce issues.[124] These topics and measures are pertinent to AI adoption. Policy alignment may help spur "legal interoperability," which is needed to manage the different regulatory frameworks and data management abilities of the diverse group of countries.[125]

In sum, each of the institutions overviewed in this section has its own character and its own contributions to S&T cooperation. They are at once mutually reinforcing complements to the S&T agreements and the global military S&T networks, as well as their own unique frameworks for cooperation.

Key Findings

The military AI cooperation toolbox offers several immediate pathways for the DOD to engage allies and partners on democratic, safe, secure, ethical, and interoperable AI. This section highlights the key findings from this report, by focusing on TEVV, R&D, policy and personnel considerations, and the under-representation of allies and partners from the Indo-Pacific region.

TEVV is an important, but underrepresented, feature of military AI cooperation. A range of joint activities could factor into cooperative TEVV pipelines for AI, including tests, trials, experimentation, training, exercises, and M&S.

- IT&E agreements allow countries to use each other's testing services on a pay-per-use basis. Implementing an international testing-as-a-service business model could either be an interim solution or an alternative to co-developing joint test beds. Using these agreements for integrated, continuous testing would also be possible, as is consistent with current DOD software acquisition policy.

- Bilateral or multilateral exercises can help trial new AI-enabled capabilities in real-world conditions. Further, the data from these activities could be used for future validation and verification techniques, as well as for cooperative threat model frameworks.

- Coordination between different countries' independent M&S services could help improve the interoperability, security, and reliability of autonomous and AI-enabled systems. In addition to coordinating M&S through NATO, programs like Foreign Comparative Testing and the Allied Prototype Initiative could also direct attention to AI and convergent technologies.

- If implemented, joint research on new testing methods and the use of data from cooperative military activities could help cement common approaches to best practices, accreditations and certifications, and implementation of risk management frameworks for AI. In this way, military AI

cooperation efforts offer implicit avenues for eventual standardization.

Cooperating on shared R&D priorities can help support interoperability, ensure military effectiveness, and build good will for other forms of AI cooperation, including alignment with democratic values.

- R&D topics that could help alleviate the political sensitivities of exchanging data include privacy-preserving machine learning, federated learning, homomorphic encryption, and the usage of synthetic data. RDP MOUs and bilateral agreements include mechanisms that allow for cooperative investments in these areas.

- Multilateral institutions like NATO, Five Eyes and JAIC's PfD initiative can facilitate coordination of investments and activities in R&D.

- Collaboration on basic research has a number of benefits, including broadening the network of partner countries and sidestepping the requirement of exchanging sensitive military data. Military department-level investments can be particularly impactful in this area.

Opportunities for personnel connections that can help advance AI adoption are featured across the different agreements, exchanges and institutions that makeup the military AI cooperation toolbox. Yet they are often underutilized or ineffectively integrated.

- Working groups and exchanges between IT&E partners and allies could help build capacity for new testing procedures, and work together on the procedural aspects of validation and verification that ensure AI system responsibility over its entire lifecycle.

- Inside the U.S. military departments, ESEPs and science envoys and advisors already have a global presence that helps establish connections between foreign and U.S. researchers, socialize new ideas with the U.S. military S&T

community, and scout technologies. There is, however, no structured process for connecting these individuals and programs, or for logging, tracking, and analyzing their activities and research findings.

- If better integrated, global military research networks can buttress strategic technology monitoring and forecasting efforts.

Indo-Pacific allies and partners are underrepresented in the main agreements and institutions covered in the existing military AI cooperation toolbox.

- The U.S. military S&T cooperation architecture is heavily skewed toward European allies. At present, prospects for TEVV cooperation with Indo-Pacific allies, at least through IT&E agreements, seem limited.

- There are a number of pathways forward in the absence of more structured cooperation venues with Indo-Pacific allies. For example, the RDP MOU with Japan could provide structure for R&D projects. The less-comprehensive Reciprocal Quality Assurance MOU with South Korea could be used to implement best practices. Meanwhile, *ad hoc* arrangements like the collaboration between the JAIC and Singapore's Defence Science and Technology Agency could be a more flexible model to use with other Indo-Pacific Asian allies and partners, as well as personnel exchanges, including ESEPs with partners like Taiwan and India.

- Focusing on expanding and deepening military S&T connections, project arrangements, and participation in the PfD is a viable short-term approach. But more structured R&D and TEVV tools may be needed to facilitate military AI cooperation over the longer term. Moving forward, DOD should assess whether and how frameworks and lessons learned from cooperation with European allies can be applied to cooperation with Indo-Pacific allies and partners.

Conclusion

The Department of Defense has a number of tools at its disposal to either jumpstart new cooperative AI efforts with allies and partners, or filter existing efforts into more comprehensive frameworks. These frameworks emphasize areas like policy and process alignment, R&D, TEVV, personnel exchanges, data sharing mechanisms, and standardization. With international defense S&T cooperation agreements, military S&T exchanges, and multilateral formats all at hand, the menu of available options is broad.

Overall, political sensitivities and security concerns around exchanging data will likely remain a core obstacle for high-end AI cooperation. That said, it should not dissuade DOD and its allies and partners from acting on the realm of the possible. Only by kneading through these challenges in international security relationships can allies and partners proactively relieve some of the pressure. If the United States is serious about leveraging its asymmetric asset of a robust network of partners and allies that its strategic competitors lack, then cooperation on ways to maintain its technological edge and interoperable forces should be built into the front end of S&T development.

The will to do so is not in doubt. But the pathways to do so still need to be navigated. Moreover, the partners that the United States may look toward for closer AI cooperation will not necessarily overlap naturally with military partners for conventional military equipment cooperation. Cooperation is a goal that needs to be actively tended to over time, be it to advance solutions with the closest of allies or use those lessons with new partners to address shortfalls in DOD's cooperation network.

This paper does not mean to suggest that these existing cooperation pathways are the best or only avenues—just that their utility is largely untapped. For now, using existing tools to new ends can help ensure that, as the United States seeks to meet the current strategic moment, it does not do so alone.

Author

Zoe Stanley-Lockman is an analyst researching military innovation, emerging technologies, and defense cooperation. The views expressed herein are the author's alone and do not reflect those of any organization.

Acknowledgments

The author expresses gratitude, first and foremost, to Margarita Konaev and Igor Mikolic-Torreira for their tireless assistance and patience reading multiple drafts of this report. Thanks are also due to Edward Hunter Christie, Torben Schuetz, Simona Soare, and Andrea Gilli, whose comments have improved the quality of argumentation and information here. Analytical and editorial support from Lynne Weil, Matt Mahoney, Corey Cooper, Adrienne Thompson, and fellow analysts who provided comments has been invaluable, start to finish.

Document Identifier: doi: 10.51593/20200091

Appendix

Below are definitions of structured agreements, exchange programs, and institutions in the military AI toolbox. Not all collaborations analyzed in this report are formalized, structured agreements. Further, some agreements—like Defense Trade Cooperation Treaties, Security of Supply Arrangements, and project arrangements more broadly—are not listed here.[126]

International Defense S&T Agreements:

International Test & Evaluation Agreements: International Test and Evaluation Program (ITEP): "ITEP bilateral and multilateral agreements allow for Cooperative Test and Evaluation (CTE) Project Arrangements (PAs); Equipment and Material Transfers; Working Groups; and Reciprocal Use of Test and Facilities (RUTF) PAs. These projects benefit the United States and our allied partners by enabling access to environments and facilities to achieve coalition and joint force operational realism; sharing T&E technologies, data, and costs; and standardizing test and analytical procedures."[127]

Reciprocal Defense Procurement and Acquisition Memoranda of Understanding: Bilateral agreements to "enhance military readiness by promoting rationalization, standardization, and interoperability of military equipment" and "promote competitive opportunities for the signatories' defense industries and call for the reduction of certain barriers, such as buy-national laws and tariffs."[128]

Reciprocal Government Quality Assurance Agreements: Less comprehensive bilateral agreement than Reciprocal Defense Procurement and Acquisition Memorandum of Understanding that aims to ensure effective, efficient quality assurance services for the procurement of defense materials and services in accordance with established and documented laws, directives, regulations, and procedures.[129]

Bilateral Academic Research Initiative: "Pilot program that supports high-risk basic research as a bilateral academic

collaboration. BARI's inaugural year focuses on artificial intelligence and collaborative decision-making and sought proposals that build new frameworks for artificial intelligence agents to more truly team with human counterparts. BARI also aims to support academic teams from the United States and U.K. to combine unique skillsets and approaches and provide rapid advances in scientific areas of mutual potential interest to the U.S. DOD and U.K. Ministry of Defence."[130]

Allied Prototyping Initiative: Initiative that "identifies, develops and executes a small number of high impact operational prototyping projects in which the US and Partner Nations (PN) provide Research and Development (R&D) funding, share technology and industry participation to co-develop leap-ahead operational capabilities."[131]

Foreign Comparative Testing Program: "Test items and technologies of our foreign allies that have a high Technology Readiness Level (TRL) in order to satisfy valid defense requirements quickly and economically" with the objectives of improving capability and reducing expenditure through "Rapidly fielding quality military equipment; Eliminating unnecessary duplication of research, development, test and evaluation; Reducing life cycle or procurement costs; Enhancing standardization and interoperability; Promoting competition by qualifying alternative sources; Improving the U.S. military industrial base."[132]

Polar Research, Development, Testing, and Evaluation Agreement: International Cooperative Engagement Program for Polar Research (ICE-PPR) to improve defense and security capabilities in the Arctic—namely through standardization, rationalization, and interoperability—between Canada, Denmark, Finland, New Zealand, Norway, Sweden, and the United States. [133]

Military S&T Exchanges

Global military S&T network: US Army: International Technology Center – Atlantic (U.K.); US Army Medical Research Directorate (Georgia); US Army Medical Research Directorate – Armed Forces

Research Institute of Medical Sciences (Thailand); US Army International Technology Center – Pacific (Japan); US Army International Technology Center – Americas (Chile); US Army Medical Research Directorate (Kenya);

U.S. Navy: Office of Naval Research – Global Headquarters (U.K.), hub (Czech Republic), and science advisor (Italy); Office of Naval Research hub (Japan; Singapore); Naval Medical Research Center – Asia (Singapore; Unit No. 2 hub in Cambodia); Office of Naval Research hubs (Brazil; Chile), and science advisor (Bahrain) [NB: London HQ covers Middle East]; Naval Medical Research Unit (No. 3 Egypt; No. 6 Peru);

U.S. Air Force: European Office of Aerospace R&D (U.K.); Asian Office of Aerospace R&D (Japan); Southern Office of Aerospace R&D (Chile).[134] (See Figure 1.)

Engineer and Scientist Exchange Programs: Professional development exchange program between the United States and 16 countries (with MoUs) for exchanges between military/government scientists and engineers to address S&T challenges in alignment with service-level modernization priorities, learn about partners' R&D processes, and cooperate on technical interoperability; not a training program and not used for exchanging of technical data or software.[135]

Trilateral Strategic Steering Group: Group composed of senior officers from the French, U.K., and U.S. air forces in strategic posts close to service chiefs to increase trust, improve interoperability, and advocate for airpower; oversight of the 2013 Trilateral Strategic Initiative (date of charter).

Training with Industry/Tours with Industry:[1] Training with Industry (Departments of the Air Force, Army) and Tour with Industry (Department of the Navy) work-experience programs for warrant officers to work in industry; domestic but placements in

---

[1] Air Force program known in DOD as Training with Industry but formally called Education with Industry.

multinational companies relevant to global business operations and industrial procedures.

Multilateral Alliances and Partnerships (with sets of own tools).

NATO: Euro-Atlantic alliance of 30 nations that implements the 1949 North Atlantic Treaty, including collective defense; range of NATO bodies and detachments possible in International Staff and bodies. Relevant bodies include, but are not limited to: Conference of National Armaments Directors, Allied Command Transformation, the NATO Science & Technology Organization, the NATO Consultation, Command and Control Board, the NATO Communications and Information Agency, and the NATO Standardization Office, as well as the newer NATO Innovation Advisory Board, Innovation Unit, and Data Policy Unit.

Five Eyes Technical Cooperation Program: International organization set up between Australia, Canada, New Zealand, the U.K., and the United States (*i.e.*, Five Eyes countries) to set up three-year Strategic Challenges on S&T areas of mutual interest; part of broader cooperative architecture between the Five Eyes countries including ABCANZ Agreements for Standardization, the Five Eyes Interoperability Council, and intelligence sharing arrangements, among others.

AI Partnership for Defense: Grouping of 16 countries interested in AI cooperation (possibility to expand membership); established in 2020 and hosted by the JAIC "with a goal of creating potential frameworks and new tools for international data sharing, cooperative development, and strengthened interoperability."[136]

Table 1: Cross-tabulating international military S&T tools with AI cooperation areas

	Policy/ process alignment	**R&D**	**TEVV**	**Personnel exchanges/ connections**	**Data sharing/ standard-ization**
IT&E Agreements	Alignment of software testing policies and processes in working groups	Technical working groups for new testing methods	Access to allies' testing infrastructure	Assignment of employees to foreign testing facilities	Exchanges of testing data
RPD MoUs	Bilateral armaments	R&D options useful for	Inclusion of safety and	[See policy/ process	Use of Data Exchange

	directors committees from agreements can focus on software acquisition policy	investments in privacy-preserving and lean AI	security in cooperative R&D	alignment and other agreements like ESEPs]	Annexes to support R&D projects
Bilateral and other agreements	Cooperation on policy approaches to data governance and future exploitation of AI	Possible connections between foreign testing/prototyping funding with DOD technology modernization priorities	Not explicit; can link to R&D (e.g., in Polar RDT&E Agreement or bilateral agreements)	*Ad hoc* and short-term exchanges may be permitted; see other tools	Dependent on type of agreement; not explicit
U.S. military global S&T presence	Coordinated information gathering for global technology monitoring/ forecasting	Small investments in foreign S&T bases to better utilize innovation assets in friendly countries	Not explicit; see data sharing and standard-ization	Programs include Engineer & Scientist Exchange Programs, science envoys/ advisors	Grants and workshops could focus on data sharing, testing standards, etc.
NATO	NATO Defence Planning Process & also Conference of National Armaments Directors to implement and track digitalization efforts in agreed NATO strategies/ documents	Existing R&D structures, especially under NATO Science & Technology Organization, and forthcoming innovation fund and accelerator	Use of data from activities like exercises, experiments, modelling/ simulation, in testing; federated accreditation	Official detachments (NB: not exchanges) possible; Coordination of vast scientific networks	NATO Standardizatio n Office focus on military standards; NATO C3B & NCI Agency respectively for info. and data sharing
Five Eyes	High degree of political trust and doctrinal coordination facilitates adoption/ cooperation	Technical Cooperation Program strategic challenges can focus on development	Trialing collective C2 software in exercises to collect more data for operational use	Existing mechanisms covered under other foreign exchange agreements and tools	ABCANZ Agreements for Standard-ization; data sharing facilitated by intelligence and other agreements
PfD	Partnership to cohere around democratic military AI ethics and governance and shared adoption challenges	Too early to assess	Too early to assess	No specific mechanisms, but precedent of foreign exchange officer in JAIC as possible pathway	Possibility to focus future engagements on data exchange and technology transfers

Source: Author's analysis.

Endnotes

[1] U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, D.C.: U.S. Department of Defense, 2018), 8, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF; National Security Commission on Artificial Intelligence, *Final Report* (Washington, D.C.: National Security Commission on Artificial Intelligence, March 2021), 100–101, 163–167, 192, 234, 241–250, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[2] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge* (Washington, D.C.: U.S. Department of Defense, 2018), 8, https://DOD.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[3] U.S. Department of Defense, *Summary of the 2018 National Defense Strategy of The United States of America*, 8.

[4] Jackson Barnett, "Why the Pentagon can't go it alone on AI," *FedScoop*, April 24, 2020, https://www.fedscoop.com/experts-urge-us-nato-not-to-go-it-alone-on-developing-artificial-intelligence/.

[5] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations Memo* (Washington, D.C.: National Security Commission on Artificial Intelligence, October 2020), 222–224, https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Interim-Report-and-Third-Quarter-Recommendations.pdf.

[6] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116–283, § 5101.b.8 (2021).

[7] For a more formal definition, interoperability is the "ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together." See: Myron Hura et al., "Interoperability: A Continuing Challenge in Coalition Air Operations" (RAND Corporation, 2000), 8, https://www.rand.org/pubs/monograph_reports/MR1235.html.

[8] Per NATO doctrine: "Interoperability of formations and units of a joint and multinational force has three dimensions: technical (for example, hardware, systems); procedural (for example, doctrines, procedures); and human (for example, language, terminology and training)." See: North Atlantic Treaty Organization, *NATO Standard AJP-01: Allied Joint Doctrine Edition E Version 1* (Brussels: 2017), 1–2.

[9] The aim of this paper is to focus primarily on DOD's tools, and therefore the degree of other countries' respective digitalization efforts is beyond its scope. For information on other countries' efforts that synchronize investments in AI (and autonomy in weapons) with operational concept development, see examples including: Vice Chief of the Defence Force, "ADF Concept for Multi-Domain Strike," Australian Department of Defence, November 2020, https://www.defence.gov.au/VCDF/forceexploration/adf-concept-Multi-Domain-Strike.asp; U.K. Ministry of Defence, "Multi-Domain Integration (JCN 1/20)," December 2, 2020, https://www.gov.uk/government/publications/multi-domain-integration-jcn-120; Ingo Gerhartz, "German Air Force chief: The service is undergoing upgrades to meet future challenges," *Defense News*, January 11, 2021, https://www.defensenews.com/outlook/2021/01/11/german-air-force-chief-the-service-is-undergoing-upgrades-to-meet-future-challenges/; Franz-Stefan Gady, "Network-Centric Warfare: Can Europe be ready?," *The Wavell Room* (blog), December 21, 2020, https://wavellroom.com/2020/12/21/network-centric-warfare-europe-defence/; Directorate General of Armaments, "Big data et IA : la DGA présente le projet Artemis," French Ministry of Armed Forces (in French), October 8, 2018, https://www.defense.gouv.fr/dga/actualite/big-data-et-ia-la-dga-presente-le-projet-artemis; Daisuke Akimoto, "Japan's Emerging 'Multi-Domain Defense Force'," *The Diplomat*, March 18, 2020, https://thediplomat.com/2020/03/japans-emerging-multi-domain-defense-force/.

[10] Margarita Konaev, Tina Huang, and Husanjot Chahal, "Trusted Partners: Human-Machine Teaming and the Future of Military AI" (Center for Security and Emerging Technology, February 2021), 13, https://cset.georgetown.edu/research/trusted-partners/; Joanna van der Merwe, "NATO Leadership on Ethical AI is Key to Future Interoperability" (Center for European Policy Analysis, February 17, 2021), http://cepa.org/nato-leadership-on-ethical-ai-is-key-to-future-interoperability/.

[11] D.F. Reding and J. Eaton, *Science & Technology Trends 2020-2040: Exploring the S&T Edge* (Brussels: NATO Science & Technology Organization, 2020), 52; Tomáš Valášek, "How Artificial Intelligence Could Disrupt Alliances" (Carnegie Europe, August 31, 2017), https://carnegieeurope.eu/strategiceurope/72966.

[12] Valášek, "How Artificial Intelligence Could Disrupt Alliances," 2017.

[13] Two other key agreements–Defense Trade Cooperation treaties and Security of Supply arrangements–are largely beyond the scope of this report because their provisions do not lend themselves to AI specifics. Defense Trade Cooperation treaties, which the United States has with the U.K. and Australia (as well as an equivalent with Canada) are notably more comprehensive than RDP MoUs in terms of access to the U.S. defense market. Separately, Security of Supply arrangements are not expanded on as they do not necessarily lend themselves to AI cooperation. They are nevertheless important cooperation tools

during operations because they allow partners to prioritize delivery of urgent equipment, spare parts, and services. For reference, the United States has bilateral Security of Supply arrangements with Australia, Finland, Italy, the Netherlands, Norway, Spain, Sweden, and the U.K.–as well as an equivalent agreement with Canada.

[14] The text of the Canada-U.S. Testing and Evaluation Program (CANUSTEP) is one of the main agreements from which information on specific clauses of IT&E agreements was gathered. See: *Memorandum of Understanding Between The Department of Defense of the United States of America and the Department of National Defence of Canada for Test and Evaluation Program (TEP) Cooperation (Short Title: CANUSTEP)*, September 10, 2002, https://www.state.gov/wp-content/uploads/2019/04/02-910-Canada-Defense-9.10.2002.pdf.

[15] Michèle A. Flournoy, Avril Haines, and Gabrielle Chefitz, "Building Trust through Testing: Adapting DOD's Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems" (Center for Security and Emerging Technology, October 2020), https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf; Robert F. Behler, *Director, Operational Test and Evaluation FY 2019 Annual Report* (Washington, D.C.: U.S. Department of Defense, December 20, 2019), ii–iii, https://www.dote.osd.mil/Portals/97/pub/reports/FY2019/other/2019DOTEAnnualReport.pdf?ver=2020-01-30-115634-877.

[16] Behler, *Operational Test and Evaluation FY 2019 Annual Report*, 49-50.

[17] This language is taken from CANUSTEP, the scope of which also extends to "exchange of information on T&E policy, testing criteria, standards and procedures and other test-related or test-derived information including, but not limited to, doctrine, tactics and operational requirements." *CANUSTEP*, 10.

[18] *CANUSTEP*, 10.

[19] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations Memo*, 230.

[20] Office of the Secretary of Defense, "Department of Defense Fiscal Year (FY) 2021 Budget Estimates: Defense-Wide Justification Book Volume 3 of 5: Research, Development, Test & Evaluation, Defense-Wide," U.S. Department of Defense, February 2020, volume 3–109, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2021/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol3_OSD_RDTE_PB21_Justification_Book.pdf.

[21] Elizabeth Quintana, Henrik Heidenkamp and Michael Codner, "Europe's Air Transport and Air-to-Air Refuelling Capability: Examining the Collaborative

Imperative" (Royal United Services Institute, August 26, 2014), 2, 18, https://rusi.org/explore-our-research/publications/occasional-papers/europes-air-transport-and-air-air-refuelling-capability-examining-collaborative-imperative.

[22] Europe here refers to the 26 EDA countries, i.e., the European Union without Denmark. See: European Defence Agency, *Factsheet: Defence Test and Evaluation* (Brussels: January 26, 2021), https://eda.europa.eu/publications-and-data/latest-publications/factsheet-defence-test-and-evaluation-base.

[23] *CANUSTEP*, B–11.

[24] Integrated testing is part of the move from "waterfall" to "agile" acquisition models. "Waterfall" acquisition means completing the requirements definition, design, execution, testing, and release phases separately and sequentially. Waterfall and agile models are direct opposites, but are not the only models. See: Shelby S. Oakley, *Defense Acquisitions Annual Assessment: Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight* (Washington, D.C.: Government Accountability Office, June 2020), 18, https://www.gao.gov/assets/710/707359.pdf.

[25] Acting Under Secretary of Defense (Research and Engineering) and Director (Operational Test and Evaluation), *Test and Evaluation*, DODI 5000.89, November 19, 2020, 7, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODi/500089p.PDF.

[26] Acting Under Secretary of Defense (Research and Engineering) and Director (Operational Test and Evaluation), *Test and Evaluation*, 24.

[27] Zoe Stanley-Lockman, "From Closed to Open Systems: How the US Military Services Pursue Innovation," *Journal of Strategic Studies* 44, no. 4 (2021): 480–514.

[28] These are just two examples of intentionally motivated failures–and protecting against each type of failure is important to consider in testing. For a more complete overview, Microsoft has a taxonomy that includes 16 types of failure modes, and NIST has issued a draft report with its own taxonomy for adversarial machine learning as one of the 16 failure modes. See: Ram Shankar Siva Kumar, David O'Brien, Jeffrey Snover, Kendra Albert, and Salome Viljoen, "Failure Modes in Machine Learning," Microsoft, November 11, 2019, https://docs.microsoft.com/en-us/security/engineering/failure-modes-in-machine-learning and Elham Tabassi, Kevin J. Burns, Michael Hadjimichael, Andres D. Molina-Markham, and Julian T. Sexton, *Draft NISTIR 8269: A Taxonomy and Terminology of Adversarial Machine Learning* (Washington, D.C.:

National Institute of Standards and Technology, October 2019), https://doi.org/10.6028/NIST.IR.8269-draft.

[29] Adversarial machine learning introduces different security challenges in testing, including exploratory attacks and evasion attacks. See: Tabassi et al., *Draft NISTIR 8269*, 7; Kendra Albert, Maggie Delano, Jonathon Penney, Afsaneh Rigot, Ram Shankar, and Siva Kumar, "Ethical Testing in the Real World: Evaluating Physical Testing of Adversarial Machine Learning," arXiv preprint arxiv:2012.02048 (2020), https://arxiv.org/abs/2012.02048.

[30] Shankar et al., "Failure Modes in Machine Learning."

[31] Miles Brundage, Shahar Avin, Jasmine Wang, and Haydn Belfield et al., "Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims," arXiv preprint arXiv:2004.07213 (2020), 14–15, 22, https://arxiv.org/abs/2004.07213.

[32] As the authors explain, this use of reinforcement learning would be an empirical, not formal, validation and verification technique. Brundage et al., "Toward Trustworthy AI Development," 22.

[33] Brundage et al., "Toward Trustworthy AI Development," 14–15.

[34] If the United States and South Korea cooperate on a project under the government quality assurance agreement, then live tests can be reimbursed, but this is a limited exception. See *Annex II Regarding Reciprocal Government Quality Assurances to the Memorandum of Understanding between the Ministry of National Defense of the Republic of Korea and the Department of Defense of the United States of America signed June 8, 1988 on Defense Technological and Industrial Cooperation*, December 11, 2013, Article VII, https://www.acq.osd.mil/dpap/cpic/ic/docs/US-KR_GQA_Annex_II_-_Signed_13_Dec_11.pdf.

[35] The author thanks Simona Soare for her comments on this point.

[36] While not as comprehensive as RDP MOUs, Reciprocal Government Quality Assurance MoUs are still relevant for standardization and interoperability. Both types of agreements can be found at: Defense Pricing and Contracting, "Reciprocal Defense Procurement and Acquisition Policy Memoranda of Understanding," Office of the Under Secretary of Defense for Acquisition and Sustainment, last updated October 7, 2020, https://www.acq.osd.mil/dpap/cpic/ic/reciprocal_procurement_memoranda_of_understanding.html; U.S. Department of Defense, "Defense Federal Acquisition Regulation Supplement Subpart 225.872-1," updated February 24, 2021, https://www.acq.osd.mil/dpap/dars/dfars/html/current/225_8.htm#225.872-1.

[37] In terms of levelling the playing field, one of the main purposes RDP MOUs serve is to waive protectionist, buy-national requirements, meaning that foreign suppliers can compete in partner countries' bids. Nevertheless, provisions that allow for offsets and carveout projects are loopholes that keep barriers up for foreign participation in procurement.

[38] Eric Lin-Greenberg, "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making," *Texas National Security Review* 3, no. 2 (Spring 2020), 65; Simona Soare, "What if… the military AI of NATO and EU states is not interoperable?" in *What if…Not? The Cost of Inaction* (Paris: European Union Institute for Security Studies, January 2021), 18–22, https://www.iss.europa.eu/content/what-ifnot-cost-inaction.

[39] The RDP MOU with Australia is the only one that does not cover R&D. However, the United States and Australia have other relevant frameworks for cooperative R&D that compensate for this difference.

[40] One other area that is important is to track emergent behavior. See the section on NATO for more information.

[41] Zoe Stanley-Lockman, "Futureproofing transatlantic relations: The case for stronger technology cooperation," in *Turning the Tide: How to Rescue Transatlantic Relations* (Paris: European Union Institute for Security Studies, October 2020), 182, https://www.iss.europa.eu/content/turning-tide-how-rescue-transatlantic-relations.

[42] Although beyond the scope of this study, synthetic environments are also relevant to modelling and simulation (M&S) capabilities. See: Stanley-Lockman, "Futureproofing transatlantic relations," 182.

[43] See the section referencing zero- and few-shot learning in: Husanjot Chahal, Ryan Fedasiuk, and Carrick Flynn, "Messier than Oil: Assessing Data Advantage in Military AI" (Center for Security and Emerging Technology, July 2020), 10, https://cset.georgetown.edu/research/messier-than-oil-assessing-data-advantage-in-military-ai/.

[44] The U.S.-Israeli defense relationship should not be read as a template for other international partnerships. Rather, the point here is to see how the annex itself could be a template.

[45] Government of the United States of America and the Government of Israel, *Annex II (Research and Development) to the Memorandum of Understanding between the Government of Israel and the Government of the United States Concerning the Principles Governing Mutual Cooperation in Research and Development, Scientist and Engineer Exchange, and Procurement and Logistics*

Support of Defense Equipment, April 19, 1988, https://www.acq.osd.mil/dpap/Docs/mou-israel.pdf.

[46] Government of the United States of America and the Government of Israel, *Annex II*.

[47] Government of the United States of America and the Government of Israel, *Annex II*.

[48] The agreements were negotiated before the bifurcation of Acquisition, Technology, and Logistics into Acquisition and Sustainment on the one hand, and Research and Engineering on the other. Because these are "procurement and acquisition" memoranda, the acquisition side of house takes precedence, even though the text in this section focuses mostly on research.

[49] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations Memo*, 194–5.

[50] See also endnote 34.

[51] Craig S. Smith, "Episode 49: The Conundrum of AI Export Controls with Jason Matheny," *Eye on A.I.* (podcast), August 19, 2020.

[52] See, for instance, the debates on how the "right to repair" impacts U.S. national security: Federal Trade Commission, *Comment Submitted by Major Lucas Kunce and Captain Elle Ekman* (Washington, D.C.: Federal Trade Commission, September 15, 2019), https://www.regulations.gov/document/FTC-2019-0013-0074.

[53] This language comes from the US-Belgian RDP MOU, and is repeated in the other agreements. See: *Memorandum of Understanding between the Government of the Kingdom of Belgium and the Government of the United States of America Concerning the Principles Governing Mutual Cooperation in the Research, Development, Production, Procurement, and Logistic Support of Defense Equipment*, December 12, 1979, Article 1, no. 11, https://www.acq.osd.mil/dpap/Docs/mou-belgium.pdf.

[54] Though beyond the scope here, intellectual property rights are considered in RDP MOUs and export controls are not. For more on export controls, see also endnote 13 on Defense Trade Cooperation Treaties.

[55] These project arrangements are numerous and are not exhaustively covered in this report.

[56] U.S. Department of Defense, "JAIC and DSTA Forge Technology Collaboration," June 27, 2019,

https://www.defense.gov/Newsroom/Releases/Release/Article/1888859/jaic-and-dsta-forge-technology-collaboration/.

[57] Humanitarian assistance and disaster relief is sometimes referred to as low-hanging fruit given that it is less controversial than higher-end missions. Nevertheless, in practice, it is difficult to build firewalls between capabilities built specifically for humanitarian assistance and disaster relief and other ISR applications. Further, the policy and technical aspects of authorizing data transfers and the use of platforms outside of strictly defined operations still require close collaboration on legal, policy, and technical fronts. As such, even if it may be easier to agree that it is an important, shared security challenge, implementation itself should not be seen as a given.

[58] Andrea Gilli, "'NATO-Mation': Strategies for Leading in the Age of Artificial Intelligence" (NATO Defense College, December 2020), 41–44; Melissa Heikkilä, "NATO wants to set AI standards. If only its members agreed on the basics," *Politico*, March 29, 2021, https://www.politico.eu/article/nato-ai-artificial-intelligence-standards-priorities/.

[59] More specifically: "This project aims to develop a novel architecture for complex group decision making that integrates, in an unprecedented way, the strengths of human and AI team members while compensating for their respective weaknesses." See: Basic Research Directorate, "BARI: Bilateral Academic Research Initiative," U.S. Department of Defense, accessed June 29, 2021, https://basicresearch.defense.gov/Pilots/BARI-Bilateral-Academic-Research-Initiative/; U.S. Department of Defense, "DOD Announces BARI Award for US-UK Collaboration on Human-Machine Teaming," September 25, 2018, https://www.defense.gov/Newsroom/Releases/Release/Article/1644263/DOD-announces-bari-award-for-us-uk-collaboration-on-human-machine-teaming/.

[60] See, for instance: Bureau of Oceans and International Environmental and Scientific Affairs, "Declaration of the United States of America and the United Kingdom of Great Britain and Northern Ireland on Cooperation in Artificial Intelligence Research and Development: A Shared Vision for Driving Technological Breakthroughs in Artificial Intelligence," U.S. Department of State, September 25, 2020, https://www.state.gov/declaration-of-the-united-states-of-america-and-the-united-kingdom-of-great-britain-and-northern-ireland-on-cooperation-in-artificial-intelligence-research-and-development-a-shared-vision-for-driving/.

[61] Corey Beaverson, *Allied Prototyping Initiative (API)* (Washington, D.C.: Office of the Under Secretary of Defense for Research and Engineering, June 16, 2020), 2–4, https://ac.cto.mil/wp-content/uploads/2020/08/api_overview_20200824.pdf.

[62] Office of the Under Secretary of Defense for Research and Engineering, "DOD Announces New Allied Prototyping Initiative Effort with Norway to Continue

Partnership in Advancing Solid Fuel Ramjet Technologies," U.S. Department of Defense, April 20, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2156251/DOD-announces-new-allied-prototyping-initiative-effort-with-norway-to-continue/; Office of the Under Secretary of Defense for Research and Engineering, "Department of Defense Announces New Allied Prototyping Initiative Effort With Australia to Continue Partnership in Developing Air Breathing Hypersonic Vehicles," U.S. Department of Defense, November 30, 2020, https://www.defense.gov/Newsroom/Releases/Release/Article/2429061/department-of-defense-announces-new-allied-prototyping-initiative-effort-with-a/.

[63] Other AI-adjacent technology priorities include space, cyber, quantum science, and biotechnology. Office of the Under Secretary of Defense for Research and Engineering, "Modernization Priorities," U.S. Department of Defense, accessed July 2, 2021, https://www.cto.mil/modernization-priorities/.

[64] Office of Naval Research, "International Cooperative Engagement Program for Polar Research (ICE-PPR)," U.S. Department of the Navy, accessed January 22, 2021, https://www.onr.navy.mil/Science-Technology/ONR-Global/ICE-PPR.

[65] Office of Naval Research, "International Cooperative Engagement Program for Polar Research."

[66] Gilli, "'NATO-Mation'," 47.

[67] Department of Defense Research & Engineering Enterprise, "Defense Laboratories and Centers," U.S. Department of Defense, June 7, 2019, https://rt.cto.mil/rtl-labs/.

[68] The U.S. Army Combat Capabilities Development Command has a larger global presence than the main hubs indicated in the map. See: Jennifer Becker, "Basic and Applied Research Collaboration Overview," U.S. Army CCDC Atlantic, February 27, 2019, 5, https://www.chimica.unito.it/att/CCDC_ATL_academic_March_2019_1.pdf; U.S. Army Combat Capabilities Development Command, "CCDC Map," November 2019, https://asc.army.mil/web/wp-content/uploads/2019/11/CCDC-Map-01.jpg.

[69] Department of Defense Research & Engineering Enterprise, "Defense Laboratories and Centers," U.S. Department of Defense, June 7, 2019, https://rt.cto.mil/rtl-labs/.

[70] James Borghardt, Patricia Gruber, and Matthew Farr, *2019 International Science Prospectus FY19* (Arlington, VA: Office of Naval Research, 2019), 10, http://mqt2019.org/wp-content/uploads/2019/12/FY-2019-International-Science-Prospectus-Final.pdf.

[71] To take the example of the Office of Naval Research Global headquarters and hubs research grants (previously known as Naval International Cooperative Opportunities Programs) in addition to several grantees in the U.K., Japan, and Australia, other AI-related research topics include: quantum science research with Argentina, Chile, Belgium and U.K.; swarms with Luxembourg, Belgium and the U.K.; basic and applied research on learning methods and representation with Vietnam, Malaysia, Japan, New Zealand; human-machine teaming with Chile; multi-agent settings with Serbia; and data mining and clustering with Mexico and Israel. See: Borghardt et al., *2019 International Science Prospectus FY19*, 19–32.

[72] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations Memo*, 66.

[73] See, for example: *Memorandum of Understanding between the Department of Defense of the United States of America and the Ministry of Defense of the Arab Republic of Egypt Concerning the Exchange of Scientists and Engineers*.

[74] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations Memo*, 66.

[75] U.S. Department of Defense, *Report to Congress Restructuring the Department of Defense Acquisition, Technology and Logistics Organization and Chief Management Officer Organization In Response to Section 901 of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114 - 328)* (Washington, D.C.: U.S. Department of Defense, August 2017), 8–9, https://DOD.defense.gov/Portals/1/Documents/pubs/Section-901-FY-2017-NDAA-Report.pdf.

[76] National Security Commission on Artificial Intelligence, *Final Report*, 2021, 318–319.

[77] Including international security partners in communities of practice may be more based on exchanges than on technology monitoring, but is currently under-exploited. For instance, the DOD Science, Technology, Engineering and Mathematics (STEM) Strategic Plan for Fiscal Years 2016–2020 does not mention international engagement. U.S. Department of Defense, *DOD STEM Strategic Plan FY2016-FY2020* (Washington, D.C.: U.S. Department of Defense, 2015), https://dodstem-assets.dodstem.us/files/DoD_STEM_Strategic_Plan_2015.pdf.

[78] Daniel Kliman and Brendan Thomas-Noone, "Now is the time to take DIUx global," *Defense News*, May 24, 2018, https://www.defensenews.com/opinion/commentary/2018/05/23/now-is-the-time-to-take-diux-global/; Joint Artificial Intelligence Center, "JAIC Welcomes First AI Foreign Exchange Officer," October 26, 2020, https://www.ai.mil/news_10_26_20-

jaic_welcomes_first_ai_foreign_exchange_officer.html; Lawrence and Cordey, "The Case for Increased Transatlantic Cooperation on Artificial Intelligence," 125; Stanley-Lockman, "Futureproofing transatlantic relations," 186.

[79] Kliman and Thomas-Noone, "Now is the time to take DIUx global."

[80] Peter Goldfein and André Adamson, "The Trilateral Strategic Initiative: A Primer for Developing Future Airpower Cooperation," *Air and Space Power Journal–Africa and Francophonie* 7, no. 1 (Winter 2016): 80, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-30_Issue-4/V-Goldfein.pdf.

[81] Goldfein and Adamson, "The Trilateral Strategic Initiative," 76.

[82] Once concluded, the MTEP could be useful to this end.

[83] This language is taken from a 1991 US-Egyptian agreement that governs engineer exchanges, itself based on the 1980 Scientist and Engineer Exchange Agreement and 1984 Exchange of Weapons Development Data agreements. See: *Memorandum of Understanding between the Department of Defense of the United States of America and the Ministry of Defense of the Arab Republic of Egypt Concerning the Exchange of Scientists and Engineers*, May 15, 1991, Article 1.1, https://www.acq.osd.mil/dpap/Docs/mou-egypt.pdf.

[84] For the Air Force, there are 16 countries with active agreements and exchange opportunities: Australia, Canada, Chile, Czech Republic, France, Germany, Israel, Italy, Japan, the Netherlands, Norway, Poland, South Korea, Spain, Singapore, and the U.K. In addition to India and Taiwan, ESEP MoUs are also in development with Finland, Sweden, and Switzerland. See: Deputy Under Secretary of the Air Force International Affairs Armaments Cooperation Division, "USAF Engineer and Scientist Exchange Program (ESEP)," U.S. Air Force, 2021, 5, https://www.safia.hq.af.mil/Portals/72/documents/ESEP/ESEP%20AY21%20-%20PROGRAM%20BROCHURE.pdf.

[85] Microsoft and Amazon are two of many examples. Other participating companies include software companies like Tesla and Apple, manufacturers SpaceX and Qualcomm, and the cloud-computing company VMWare. Google also previously participated in the U.S. Army Training with Industry program. See: Meghann Myers, "NCOs can apply for new slots in Army's Training with Industry program," *Army Times*, November 9, 2017, https://www.armytimes.com/news/your-army/2017/11/09/ncos-can-apply-for-new-slots-in-armys-training-with-industry-program/.

[86] Stanley-Lockman, "Futureproofing transatlantic relations," 186–187.

[87] In addition to the 30 Allies that make up NATO, the Alliance also works with a range of partner countries, listed at "Partners," North Atlantic Treaty Organization, https://www.nato.int/cps/en/natohq/51288.htm.

[88] For a recent overview of the role of the NATO bodies and agencies involved in defense innovation, see: Leona Alleslev, *Defence Innovation–Special Report*, (Brussels: NATO Parliamentary Assembly, November 20, 2020), 9–10, https://www.nato-pa.int/document/2020-revised-draft-report-defence-innovation-alleslev-041-stc-20-e-rev1.

[89] Denis Mercier, "SACT's opening remarks to the NAC/MC Away Day, NATO Supreme Allied Commander Transformation," North Atlantic Treaty Organization, March 22, 2018, https://www.act.nato.int/images/stories/media/speeches/180319_nac-mc-awayday.pdf.

[90] This includes the impact of EDTs on deterrence and defence, capability development, legal and ethical norms, and arms control aspects. See: "NATO: READY FOR THE FUTURE: Adapting The Alliance (2018–2019)" (Brussels: North Atlantic Treaty Organization), November 29, 2019, 17, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_191129-adaptation_2018_2019_en.pdf; and North Atlantic Treaty Organization, "Emerging and disruptive technologies," last updated June 18, 2021, https://www.nato.int/cps/en/natolive/topics_184303.htm?selectedLocale=en.

[91] "NATO Guide to Data Collection and Management for Analysis Support to Operations," NATO Science & Technology Organization, August 24, 2020, https://www.sto.nato.int/publications/STO%20Technical%20Reports/Forms/Technical%20Report%20Document%20Set/docsethomepage.aspx?ID=4441&FolderCTID=0x0120D5200078F9E87043356C409A0D30823AFA16F6010066D541ED10A62C40B2AB0FEBE9841A61&List=92d5819c-e6ec-4241-aa4e-57bf918681b1&RootFolder=/publications/STO%20Technical%20Reports/STO-TR-SAS-111; Edward Hunter Christie, "Artificial Intelligence at NATO: dynamic adoption, responsible use," *NATO Review*, November 24, 2020, https://www.nato.int/docu/review/articles/2020/11/24/artificial-intelligence-at-nato-dynamic-adoption-responsible-use/index.html; Edward Hunter Christie, "The NATO Alliance and the Challenges of Artificial Intelligence Adoption" in *NATO Decision-Making in the Age of Big Data and Artificial Intelligence* (NATO Allied Command Transformation, the University of Bologna and Istituto Affari Internazionali, March 2021), 89.

[92] Sonia Lucarelli, Alessandro Marrone, and Francesco N. Moro, "Technological Changes and a Transformed International Security Environment" in *NATO Decision-Making in the Age of Big Data and Artificial Intelligence*, 11; North Atlantic Treaty Organization, "Emerging and disruptive technologies at NATO," 2021.

[93] Lucarelli et al., "Technological Changes and a Transformed International Security Environment," 11.

[94] North Atlantic Treaty Organization, "Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021," June 14, 2021, https://www.nato.int/cps/en/natohq/news_185000.htm.

[95] Reding and Eaton, *Science and Technology Trends 2040*, 56–7; NATO Science & Technology Organization, *NATO Simulation Interoperability Test and Certification Service–Concept of Operations (CONOPS)* (Brussels: September 2019), https://apps.dtic.mil/sti/pdfs/AD1091464.pdf; Michael Street and Peter Lenk et al., "Lessons Learned from Initial Exploitation of Big Data and AI to Support NATO Decision Making" (Paris: NATO Science & Technology Organization, 2018); Vincent Lamigeon, "Thales va fournir le cloud sécurisé de l'OTAN," *Challenges*, January 25, 2021, https://www.challenges.fr/entreprise/defense/thales-va-fournir-le-cloud-securise-de-l-otan_747577.

[96] Ensuring EU-NATO complementarity and lack of duplication is relevant here. As a third state, potential U.S. participation in the European Defence Fund offers another way for the United States to align European capability development objectives with NATO priorities.

[97] Flournoy et al., "Building Trust through Testing," 25.

[98] Paul Beckley, "Revitalizing NATO's once robust standardization programme," NATO Defense College, August 1, 2020, https://www.ndc.nato.int/news/news.php?icode=1456.

[99] Such Standardization Agreements include: STANAG 4545 NATO Secondary Imagery Format; STANAG 4575 NATO Advanced Data Storage Interface, and STANAG 7085 NATO Interoperable Data Links for ISR Systems, among others.

[100] According to the NATO Terminology Database, an operational standard is defined as "a standard that specifies the conceptual, organizational or methodological requirements to enable materiel, installations, organizations or forces to fulfil their functions or missions." Available via the NATO Standardization Office website: https://nso.nato.int/nso/.

[101] Andrew Imbrie, Ryan Fedasiuk, Catherine Aiken, Tarun Chhabra, and Husanjot Chahal, "Agile Alliances: How the United States and its Allies can Deliver a Democratic Way of AI" (Center for Security and Emerging Technology, February 2020), 24, https://cset.georgetown.edu/wp-content/uploads/CSET-Agile-Alliances.pdf.

[102] Craig S. Smith, "Eric Horvitz on AI and Allies," *Eye on AI* (podcast), December 3, 2020, transcript available at https://www.eye-on.ai/podcast-archive.

[103] For example, the Royal Australian Air Force has tested its AI search-and-rescue system to identify an orange life raft on a river versus a sea with whitecaps to assess the transferability between contexts. See: Samara Kitchener, "Using Ai to search and save," Department of Defence of Australia, October 31, 2019, https://news.defence.gov.au/technology/using-ai-search-and-save; Holly Richardson, "Australian Air Force trialling AI search and rescue project off Stradbroke Island in Queensland," *ABC Australia*, May 10, 2020, https://www.abc.net.au/news/2020-05-11/air-force-artificial-intelligence-search-and-rescue-trial/12234000.

[104] More comprehensively, cooperation should focus on all aspects Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P). See: Reding and Eaton, *Science & Technology Trends 2020-2040*, 66.

[105] Margarita Konaev, Husanjot Chahal, Ryan Fedasiuk, Tina Huang, and Ilya Rahkovsky, "U.S. Military Investments in Autonomy and AI: A Strategic Assessment" (Center for Security and Emerging Technology, October 2020), 15, https://cset.georgetown.edu/research/u-s-military-investments-in-autonomy-and-ai-a-strategic-assessment/.

[106] Konaev, Huang, and Chahal, "Trusted Partners," 13.

[107] Michael D. Brasseur, Rob Murray, and Sean Trevethan, "NATO's 'startup' charts a bold future in maritime unmanned systems," *Defense News*, April 20, 2020, https://www.defensenews.com/opinion/commentary/2020/04/20/natos-start-up-charts-a-bold-future-in-maritime-unmanned-systems/.

[108] Martin Banks, "4 questions with NATO on its unmanned tech test," *Defense News*, October 28, 2019, https://www.defensenews.com/training-sim/2019/10/28/4-questions-with-nato-on-its-unmanned-tech-test/; North Atlantic Treaty Organization, "Portugal hosts maritime exercise in support of NATO's Maritime Unmanned Systems Initiative," September 25, 2019, https://www.nato.int/cps/en/natohq/news_168925.htm?selectedLocale=en.

[109] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations Memo*, 244.

[110] The Australian-led *Talisman Saber* 19 exercise is one example.

[111] See: NATO Science & Technology Organization, "NATO Modelling & Simulation Group: Research & Development of Standards, Guidance, Products and Services for M&S," accessed June 29, 2021, https://nmsg.sto.nato.int.

[112] For instance, the F-35 requires new virtual testing environments to simulate the performance of the system without the benefit of prior approximal testing data. The flagship testing infrastructure for the F-35, the Joint Simulation Environment (JSE) will have inherently multinational aspects–and include options for international testing, training, and experimentation. See: Timothy Menke, *Joint Simulation Environment for United States Air Force Test Support* (Paris: NATO Science & Technology Organization, October 18, 2019).

[113] NATO structures, as well as IT&E agreements, can help with the "development of testing methods, evaluation frameworks, and architectures, to include development of test beds, M&S capabilities, and test ranges to observe and analyze performance." See: Behler, *Director, Operational Test and Evaluation FY 2019 Annual Report*, 235.

[114] Defense Standardization Program, *International Standardization* (Washington, D.C.: U.S. Department of Defense, accessed December 10, 2020), https://www.dsp.dla.mil/Programs/International-Standardization/.

[115] Lin-Greenberg, "Allies and Artificial Intelligence," 72.

[116] Geoff Slocombe, "Autonomous Warrior 2018: Major air, land and sea exercise at Jervis Bay, NSW," *Asia-Pacific Defence Reporter*, September 26, 2018, https://asiapacificdefencereporter.com/autonomous-warrior-2018/; Mark Draper, Allen Rowe, and Jessica Bartik, "TTCP Autonomy Strategic Challenge," Air Force Research Laboratory Airman Systems Directorate, 2019, https://nari.arc.nasa.gov/sites/default/files/attachments/Day%201%20MarkDraper%20Slides.pdf.

[117] There were two exercises in November 2018 by the same name. The bilateral US-U.K. *Autonomous Warrior* Exercise in 2018 was a format for the two armies to test interoperability and stress-test spectrum requirements in the land domain for nearly 70 unmanned systems. While a relevant bilateral contribution, it is not discussed at length so as to maintain the focus on Five Eyes in this section. Grant Turnbull, "Why the British army tested robots in muddy fields," *C4ISRnet*, January 11, 2019, https://www.c4isrnet.com/unmanned/robotics/2019/01/11/why-the-british-army-tested-robots-in-muddy-fields/; UK Ministry of Defence, "Exercise Autonomous Warrior set to be a game-changer," *Medium*, December 14, 2018, https://defencehq.medium.com/exercise-autonomous-warrior-set-to-be-a-game-changer-47a70e43a816.

[118] Slocombe, "Autonomous Warrior 2018"; Draper et al., "TTCP Autonomy Strategic Challenge," 4; Glennn Moy, Slava Shekh, Martin Oxenham, and Simon Ellis-Steinborner, *Recent Advances in Artificial Intelligence and their Impact on Defence* (Canberra: Defence Science and Technology Group Joint and Operations Analysis Division, 2020), 17,

https://www.dst.defence.gov.au/sites/default/files/publications/documents/DST-Group-TR-3716_0.pdf.

[119] Draper et al., "TTCP Autonomy Strategic Challenge," 4–6, 14.

[120] Andrew Herring, "AUTONOMOUS WARRIOR 2018 a milestone in allied cooperation," *Navy Daily* (Australia), November 24, 2018, https://news.navy.gov.au/en/Nov2018/Fleet/4946/AUTONOMOUS-WARRIOR-2018-a-milestone-in-allied-cooperation.htm#.X-K_gS2cY6g.

[121] National Security Commission on Artificial Intelligence, *Interim Report* (Washington, D.C.: National Security Commission on Artificial Intelligence, November 2019), 91, https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Interim-Report-for-Congress_201911.pdf; Defence Science and Technology Group, "The Technical Cooperation Program," Australian Department of Defence, accessed January 7, 2021, https://www.dst.defence.gov.au/partnership/technical-cooperation-program.

[122] National Security Commission on Artificial Intelligence, *Interim Report and Third Quarter Recommendations*, 195; Arthur Holland Michel, *Eyes in the Sky* (Boston, MA: Houghton Mifflin Harcourt, 2019), 104.

[123] JAIC Public Affairs, "JAIC facilitates first-ever International AI Dialogue for Defense," Joint Artificial Intelligence Center, September 16, 2020, https://www.ai.mil/news_09_16_20-jaic_facilitates_first-ever_international_ai_dialogue_for_defense_.html; JAIC Public Affairs, "DOD Joint AI Center facilitates second International AI Dialogue for Defense," Joint Artificial Intelligence Center, January 27, 2021, https://www.ai.mil/news_01_27_21-DOD_joint_ai_center_facilitates_second_international_ai_dialogue_for_defense.html.

[124] JAIC Public Affairs, "DOD Joint AI Center Facilitates Third International AI Dialogue for Defense," Joint Artificial Intelligence Center, May 28, 2021, https://www.ai.mil/news_05_28_21-jaic_facilitates_third_international_ai_dialogue_for_defense.html.

[125] Lena Trabucco, "AI Partnership for Defense is a Step in the Right Direction – But Will Face Challenges," *OpinioJuris*, October 5, 2020, opiniojuris.org/2020/10/05/ai-partnership-for-defense-is-a-step-in-the-right-direction-but-will-face-challenges/.

[126] Zoe Stanley-Lockman, "Futureproofing transatlantic relations," 184–186.

[127] Behler, *Director, Operational Test and Evaluation FY 2019 Annual Report*, 49.

[128] U.S. Government Accounting Office, *NATO Allies' Implementation of Reciprocal Defense Agreements* (Washington, D.C., U.S. Government Accounting Office, March 1992), 2, https://www.gao.gov/assets/nsiad-92-126.pdf.

[129] *Memorandum of Understanding between the United States of America and Poland, DEFENSE: Government Quality Assurance*, May 31 and June 22, 2007, 2, https://www.state.gov/wp-content/uploads/2019/02/07-622.1-Poland-Defense.EnglishOCR.pdf.

[130] Office of the Under Secretary of Defense for Research and Engineering, "BARI: Bilateral Academic Research Initiative," U.S. Department of Defense, accessed June 29, 2021, https://basicresearch.defense.gov/Pilots/BARI-Bilateral-Academic-Research-Initiative/.

[131] Beaverson, *Allied Prototyping Initiative (API)*, 2–4, https://ac.cto.mil/wp-content/uploads/2020/08/api_overview_20200824.pdf.

[132] Office of Naval Research, "Foreign Comparative Testing Program," U.S. Navy, accessed July 6, 2021, https://www.onr.navy.mil/en/Science-Technology/ONR-Global/foreign-comparative-testing.

[133] Office of Naval Research, "International Cooperative Engagement Program for Polar Research (ICE-PPR)," U.S. Navy, accessed July 6, 2021, https://www.onr.navy.mil/en/Science-Technology/ONR-Global/ICE-PPR.

[134] Department of Defense Research & Engineering Enterprise, "Defense Laboratories and Centers," U.S. Department of Defense, June 7, 2019, https://rt.cto.mil/rtl-labs/; Becker, "Basic and Applied Research Collaboration Overview," 5.

[135] Air Force International Affairs, "Engineer and Scientist Exchange Program," U.S. Air Force, accessed July 6, 2021, https://www.safia.hq.af.mil/Force-Development/Engineer-and-Scientist-Exchange-Program/; Navy International Programs Office, "Personnel Exchanges," U.S. Navy, accessed July 6, 2021, https://www.secnav.navy.mil/nipo/Pages/About/Cooperative%20Programs/Personnel-Exchanges.aspx; Office of the Deputy Assistant Secretary of the Army for Defense Exports and Cooperation, "Engineer and Scientist Exchange Program," U.S. Army, accessed July 6, 2021, https://www.dasadec.army.mil/Portals/77/Documents/DASA%20DEC%20Public%20Website%20ESEP%20Page%204.10.20.pdf?ver=2020-04-13-140812-730.

[136] JAIC Public Affairs, "JAIC facilitates first-ever International AI Dialogue for Defense."