The Path of Least Resistance
Multinational Collaboration on AI for Military Logistics and Sustainment

CSET Issue Brief
Executive Summary

The United States’ global network of alliances and partnerships is a force multiplier in the strategic competition against China and Russia. With artificial intelligence as the focal point of this competition, fostering AI defense and security cooperation is becoming increasingly important. In fact, in its final report, the National Security Commission on Artificial Intelligence has recommended strengthening AI interoperability with U.S. allies and partners as a key element of building an AI-ready force by 2025.¹ The AI future of the United States is then inherently intertwined with that of our allies and partners.

Although there are powerful incentives for multinational collaboration on AI, there are also nonnegligible technical, bureaucratic, and political barriers that could prevent like-minded nations from realizing a shared vision for the responsible use of military AI. This issue brief summarizes these challenges and then makes the argument that multinational collaboration on AI applications for military logistics and sustainment offers the path of least resistance. Our key takeaways are:

- Multinational collaboration efforts on military applications of AI face an uphill battle. Public misgivings about the militarization of AI, tensions with Europe on questions of regulations and data privacy, lack of clarity regarding the best forum for collaboration, and technical challenges to ensuring that hardware and digital systems are interoperable and secure could impede efforts to work together.

- While no easy task, collaboration on AI-enabled technologies and applications related to military logistics and sustainment is technologically attainable, politically feasible, and strategically imperative.
• There are multiple pathways for collaboration on this set of technologies and applications, including joint standards for secure data sharing; collaborative research and development programs; multinational public-private partnerships; and joint military exercises that include AI-enabled logistics and sustainment technologies and capabilities.

As the Biden administration moves to implement its foreign policy agenda of rebuilding U.S. alliances and confronting China’s assertiveness, multinational collaboration on emerging technologies takes center stage. While not without challenges, joint projects centered on developing, maturing, and adapting AI applications for military logistics and sustainment offer both a viable and promising path forward.
Multinational Collaboration on Military AI: Imperatives and Challenges

There is a strong consensus among U.S. national security experts that collaboration with allies on artificial intelligence can promote common security interests and ensure that the future of emerging technologies reflects shared democratic values and ethical principles. The Department of Defense Artificial Intelligence Strategy, for example, calls for engaging with “international allies and partners” as a key step toward harnessing AI.\(^2\) Putting the strategy into practice, the Joint Artificial Intelligence Center (JAIC) has launched an AI Partnership for Defense, bringing together representatives of defense organizations from 13 nations to “create new frameworks and tools for data sharing, cooperative development, and strengthened interoperability.”\(^3\)

U.S. allies are generally supportive of collaboration, including around military applications of AI, and are particularly interested in ensuring common standards for interpretability, safety, and security of AI-enabled, safety-critical systems.\(^4\) As the NATO Deputy Secretary General Mircea Geoană has noted, “there are considerable benefits of setting up a transatlantic digital community cooperating on AI,” with NATO playing a key role “as a facilitator for innovation and exchange.”\(^5\) The congressionally mandated National Security Commission on Artificial Intelligence (NSCAI) has explicitly urged the Department of Defense and the State Department to support NATO’s AI initiatives as well as negotiate formal AI agreements with allies in the Indo-Pacific.\(^6\)

That the United States and its allies are voicing interest in collaboration on AI is a positive development considering that failing to work together could be costly. Because of the gap in technological and military capabilities between the United States and its allies, the development and integration of AI into military systems will not proceed at the same rate or scope. These disparities could create new problems and amplify existing challenges for coordination and interoperability in multinational coalitions, with potentially adverse implications for cohesion and military effectiveness.\(^7\) Indeed, as the NSCAI warns, U.S. allies are
already “concerned about being able to operate effectively together as the United States fields greater numbers of autonomous systems.”

The push toward closer collaboration, then, stems in part from the understanding that gaps in technological and military capabilities, amplified by uneven progress in AI, could harm the long-term health of U.S. alliances. Yet despite both this growing urgency and shared interest in multinational collaboration on AI, there are notable political, bureaucratic, and technological challenges that could impede progress.

While AI is a general purpose technology with a range of potential applications across industries and sectors, international collaboration on military applications of AI can become a politically thorny issue. The militarization of AI and especially increasing autonomy in weapons raise difficult ethical and legal questions on human control, accountability, and international regulation of these emerging technologies. Human rights groups and humanitarian organizations, chiefly under the umbrella of the Campaign to Stop Killer Robots, oppose the development and use of what is often referred to as lethal autonomous weapons systems (LAWS), even calling for a preemptive ban of fully autonomous weapons. Currently, there are about 30 countries that have expressed support for such a ban, including Austria and Brazil.

That said, there is no international consensus on how to regulate the process of integrating AI into military systems or the development and potential use of AI-enabled weapons. In international forums, the United States alongside allies like Australia, France, Israel, South Korea, and the United Kingdom, have opposed negotiating a new international treaty preemptively banning autonomous weapons. Yet France as well as Germany have also expressed interest in a nonbinding declaration on the regulation of LAWS, while others like Canada are open to transparency and confidence-building measures on the development and potential use of such weapons systems. In January 2021, the European Parliament released a report on military uses of AI that called for an European Union (EU)-wide strategy against LAWS, which the report defined as “weapons
systems without meaningful human control over the critical functions of targeting and attacking individual targets.”

As a whole, U.S. allies differ in their positions. Meanwhile, the main outlet for international deliberations on this issue—the Group of Governmental Experts on emerging technologies in the area of lethal autonomous weapons systems, established by the contracting parties to the Convention on Certain Conventional Weapons—has made little progress beyond agreeing on the principles to guide the discussions themselves.

Public opinion surrounding the militarization of AI is also relevant when considering potential obstacles to international collaboration. A 2020 public opinion survey found that about 61 percent of adults across 28 countries oppose the use of autonomous weapons. Meanwhile, a survey of U.S. public opinion showed that most respondents believed that autonomous weapons are ethically prohibited because they cannot be held accountable for wrongful actions and felt that the United States should work with other countries to ban them. Whereas military applications of AI include many other uses besides increased autonomy in weapon systems, public misgivings about LAWS could turn the tide against international collaboration on military AI writ large.

Relatedly, civilian AI researchers and engineers may take a stand against their companies working on defense technology, as was the case with Google employees protesting the Department of Defense contract implementing Project Maven. Defense AI research in allied countries could also attract negative international attention. In 2018, for instance, one of South Korea’s top universities, the Korea Advanced Institute of Science and Technology, became the target of a boycott by over 50 notable AI researchers for opening what they called “an AI weapons lab.” Such internal disagreements and international incidents could thwart multinational collaboration efforts on military AI.

Another potential barrier to collaboration, particularly with European allies, is the growing momentum around the idea of European digital sovereignty and increasing concerns about continued dependence on U.S. technology companies. Part of the
push for greater European technology independence stems from Europe being “caught in the crossfire” on a variety of technology issues, including 5G and internet regulation amid the intensifying strategic competition between the United States and China. European nations like France and Germany, among others, are becoming more assertive when it comes to control over their data. The experts behind France’s AI strategy, for instance, have advocated for a data policy that is “structured around the goals of sovereignty and strategic autonomy” as a prerequisite for the development of AI in France and in Europe, in an effort to “avoid becoming just ‘digital colonies’ of the Chinese and American giants.” Moreover, as Ulrike Franke explains, the EU has taken a stronger stance on protecting individuals’ digital rights through regulations such as the 2014 “right to be forgotten” and the 2018 General Data Protection Regulation. Differing views on China, a push toward additional regulations of U.S. technology companies, different approaches toward data privacy, and commercial competition can all hinder transatlantic cooperation on AI.

Alongside the diplomatic and political hurdles, there are also bureaucratic challenges. As the NSCAI observed, “the U.S. government lacks a coherent national security policy framework for security cooperation with our allies and partners in AI.” In other words, there is no clear point of contact to help allies navigate the vast Pentagon and intelligence community bureaucracies and facilitate government-wide AI collaboration.

Then, there is the question of the appropriate and most efficient forum for collaboration on military AI. JAIC’s AI Partnership for Defense is an important initiative, but as the NSCAI points out, JAIC alone cannot adequately address the broader challenges of allied AI interoperability. NATO remains “a natural platform for transatlantic cooperation on AI.” But the past four years have witnessed increasing tensions between NATO allies as well as between the United States and NATO. Moreover, the technology gap between NATO allies and the sensitive nature of national security data are significant barriers to technology sharing and transfer within the alliance. The Five Eyes intelligence alliance that includes Australia, Canada, New Zealand, the United Kingdom,
and the United States, on the other hand, could be a productive venue for collaboration due to existing protocols for sharing sensitive data. This forum, however, is perhaps best fitted for initiatives in the intelligence space, and will likely entail more narrowly scoped research and development (R&D) efforts because of the highly classified nature of its activities and relative distance from the commercial innovation ecosystem.25

Finally, on the technical front, there are numerous challenges to ensuring that hardware and digital systems are interoperable and secure. Creating and maintaining common or interoperable information systems and databases is a massive undertaking considering that in each country, the data resides in repositories lacking standardized formatting or maintained by contractors that keep such information proprietary, especially for data on sensors and weapon systems. Shared information systems and databases are also particularly vulnerable to disruption, manipulation, and data theft in part because of discrepancies in countries’ network security protocols and capabilities.26 These problems are hard to resolve in their own right. But the aforementioned political factors, especially the push toward greater data sovereignty by some of the European allies, only exacerbate these technical challenges for collaborations on AI.

The United States and its allies and partners clearly have powerful incentives to work together on AI, and in fact, failing to do so in the near future could come at a heavy cost. Despite this, there are significant political, bureaucratic, and technical challenges that could stall and even undermine multinational collaboration efforts. Nevertheless, as we discuss in the following section, AI applications for military logistics and sustainment offer an area for collaboration that is technologically attainable, politically feasible, and strategically imperative.
Focusing on AI-enabled Military Logistics and Sustainment

In military affairs, logistics is tasked with managing the global supply chain for the armed services, including “the transfer of personnel and materiel from one location to another, as well as the maintenance of that materiel.” Sustainment is a broader term, encompassing logistics as well as financial management, personnel services, and health services which together provide the support necessary to maintain operations until the mission is accomplished. The two functions are closely intertwined. NATO’s Allied Joint Doctrine for Logistics, for instance, offers a comprehensive definition of logistics that also entails elements of sustainment, encompassing the aspects of military operations that deal with “design and development, acquisition, storage, movement, distribution, maintenance, evacuation and disposition of materiel; transport of personnel; acquisition, construction, maintenance, operation and disposition of facilities; acquisition or furnishing of services; and medical and health service support.”

Logistics and sustainment are essential to military effectiveness, readiness, survivability, and endurance, and in many ways, constitute the lifeblood of military power. The Department of Defense, in turn, sees great promise in leveraging AI/machine learning (ML) technologies for military logistics and sustainment to better maintain equipment, reduce operational costs, and improve readiness. The Department of Defense’s AI strategy, for example, includes efforts related to AI-enabled logistics and sustainment, such as “implementing predictive maintenance and supply, and streamlining business processes,” as part of its strategic approach to “delivering AI-enabled capabilities that address key missions.” Joint Logistics, in turn, is one of the JAIC’s key mission initiatives, dedicated to “improving fleet readiness through AI-driven diagnostics, training, process improvements, demand forecasting, and supply chain optimization.”

The discussion below outlines the technological, political, and strategic imperatives and opportunities for multinational collaboration on AI-enabled military logistics and sustainment.
Naturally, the principal mission of militaries is national defense and the force (including logistics and sustainment functions) must be prepared for combat at any time. Modern militaries, however, are massive organizations that employ hundreds of thousands of people, if not more. The Department of Defense, for example, employs 2.91 million people, and less than half of them, or 1.3 million, are active duty personnel. And unlike military functions such as fires or movement and maneuver of forces and equipment, many of the tasks related to military logistics and other financial, personnel, and health services are administered in noncombat settings.

While we discuss how the United States and its allies can work together on AI for military logistics and sustainment in both combat and noncombat settings, there is no doubt that the environment in question matters a great deal. From data to computational power to available talent, as well as considerations like privacy, safety, and security, implementing AI for military logistics and sustainment functions performed in controlled environments similar to commercial settings is a different endeavor from deploying AI-enabled logistics and sustainment functions in contested and hostile environments. We take these differences into account where relevant, and acknowledge that even under the best of circumstances, there are still significant challenges for both the adoption of AI applications and multinational collaboration in this area.

**Technologically attainable**

*While not without its challenges, military logistics and sustainment tasks, especially those performed in noncombat settings, present a technologically attainable area for multinational collaboration in AI.*

Although much of the innovation in AI is occurring in the commercial sector, adopting and adapting commercial AI applications for military purposes is often impossible. Current AI technologies, and especially ML-based systems, tend to perform well in stable environments but struggle with uncertain and novel situations, and remain particularly vulnerable to adversarial attacks.
These vulnerabilities present an unacceptable level of risk in high-stakes military settings, where the environment is uncertain and adversarial by definition. The consequences of mistakes and even system failure, however, are less severe when it comes to some military logistics and sustainment tasks which are administered and managed in noncombat settings, and constitute what some have called enterprise AI applications.

Advances in AI for logistics in commercial aviation, maritime shipping, and transportation sectors are therefore more applicable to certain military logistics and sustainment tasks performed in noncombat settings than for specialized military equipment like autonomous ground combat vehicles or armed drones. In particular, there may be opportunities to adopt and adapt commercial applications for the intelligent automation of tasks such as scheduling equipment maintenance and repairs, updating and issuing licenses, supply tracking and forecasting, and other processes that control the flow of logistics throughout the military organization.\textsuperscript{34} To reiterate, these are much more than cost cutting and efficiency increasing measures; improvements in these areas enable military readiness and effectiveness in combat.\textsuperscript{35}

In addition to these opportunities to leverage AI-enabled technologies and tools available in the commercial sector in support of military logistics, there are also fewer barriers to in-house innovation within defense organizations. Many of the AI applications relevant to logistics and sustainment can be developed and used in relatively well-controlled and benign environments in settings akin to commercial civilian enterprises. Under such conditions, resources like data and infrastructure, including storage, ETL pipelines, communication bandwidth, and compute can be made available to train ML models for various AI applications.\textsuperscript{36} Notably, the 2016 Defense Science Board Summer Study on Autonomy raised a similar point regarding logistics planning and execution as “a particularly good candidate for testing and experimentation (T&E) ... because the behavior of logistic software can be evaluated against crisply known metrics.”\textsuperscript{37}

Considering both the potential for leveraging developments from the private sector and lower barriers to in-house innovation,
collaboration on AI for logistics and sustainment could also involve allies with more limited military-industrial capacities. Based on its fact-finding mission to Singapore, NATO’s Science and Technology Committee observed that “small and medium-sized Allies with smart scientists and engineers can play an outsized role in AI development and adoption.” This is a significant advantage, arguably unique to AI technologies, and especially timely considering that even the relatively wealthy U.S. allies are facing cuts to their defense budgets due to the economic fallout from the COVID-19 pandemic. Moreover, collaboration that includes input from small and medium-sized allies can strengthen interoperability, contribute to allied burden sharing, and buttress the long-term viability of U.S.-led defense partnerships.

This is not to say that adopting and developing, let alone collaborating on AI-enabled logistics will be an easy task for the U.S. military and allied defense organizations. The ML and deep learning algorithms behind commercial AI-enabled logistics are generally not optimized for military needs. And if the experience of the Department of Defense is any indication, there are multiple challenges with regards to the data needed to power AI applications—from lack of data to problems with traceability, access, and interoperability of data collected by different systems. Moreover, data security and privacy concerns as well as different legal frameworks for how personal data is collected, handled, processed, and stored remain a critical barrier to international collaboration. Lack of clarity surrounding how to implement the exemptions for research incorporated into the General Data Protection Regulation, for example, has stalled collaboration between the U.S. National Institutes of Health and some European counterparts.

These and other technical barriers and privacy-related concerns are indeed significant. But developments in privacy-preserving ML techniques, including homomorphic encryption, secure multi-party computation, and federated learning offer opportunities for allies to share and pool data without compromising the privacy of individual users and organizations whose data is being used. The United States can also work with allies to develop technical standards and
protocols for harmonizing data collection, formatting, storage, and archiving to ensure data security and integrity.\textsuperscript{43}

Overall, the U.S. military and allied defense organizations will face nonnegligible technical barriers whether adapting commercial AI technologies or building AI-enabled systems and tools in-house. From a comparative standpoint, however, military logistics and sustainment applications that fall under the broader category of enterprise AI applications present “low hanging fruit” for the U.S. military (and presumably for other technologically advanced militaries).\textsuperscript{44} Moreover, international collaboration on AI-enabled military logistics and sustainment is likely more within reach than collaboration on AI integrated into weapons systems or applications that feed on sensitive data collected by proprietary weapons and sensor systems.\textsuperscript{45}

\textbf{Politically feasible}

\textit{With key U.S. allies like the United Kingdom, Germany, France, South Korea and Japan already pursuing efforts to leverage AI for military logistics and sustainment, collaboration in this area seems politically feasible.}

The integration of AI into weapons systems has raised ethical concerns and opposition in some communities across the United States and in allied countries. Yet by focusing collaboration on AI applications for military logistics and sustainment functions, the United States and its allies could potentially sidestep the contentious “killer robots” debate. Collaborative efforts to develop and apply AI tools to areas such as defense supply chain management, personnel management, and equipment maintenance can improve existing processes and functions, save costs and increase efficiencies in defense organizations. Multinational collaboration around this set of goals and applications is less likely to galvanize widespread grassroots opposition than programs on AI-enabled drones or autonomous ground combat vehicles.

Moreover, some of the United States’ closest allies are already investing in AI and ML technologies for logistics and sustainment.
The United Kingdom’s Ministry of Defense’s (MOD) Autonomy Programme, for example, identifies defense resupply and logistics challenges through the Defense and Security Accelerator as one of its key activities. In 2019, MOD also allocated £66 million (about $83 million) to accelerate robotic projects for the British Army, including autonomous logistics vehicles supporting resupply missions in conflict zones. Notably, the UK’s Defense Science and Technology Laboratory and the U.S. Army Combat Capabilities Development Command’s Ground Vehicle Systems Center have been working together since 2016 on the Coalition Assured Autonomous Resupply project, prototyping semiautonomous logistics convoys, along with ground and aerial autonomous resupply systems, and demonstrating the interoperability of the two nations’ armies with autonomous driving technology.

France’s military AI strategy also views “logistics and operational readiness” as one of the priority areas for the defense ministry, including a focus on predictive maintenance. Notably, the strategy states that “mission performance and assisted maintenance applications, especially for cooperation with countries that have the same systems” as France pose no significant problems in terms of sharing classified data. And in addition to its key European partners, France is also open to collaboration with the United States given the similar approach to AI development.

Along similar lines, the German Army identifies AI for personnel and material management, including predictive maintenance, as one of the main areas for action on AI development.

Japan and South Korea are also increasingly investing in military applications of AI, including for logistics and sustainment. South Korea’s National Strategy for Artificial Intelligence lists national defense as a key area for AI applications, including using AI to “quickly analyze and process large-scale defense data and develop and support common services such as medical care, logistics, and administration.” Meanwhile, Japan’s Acquisition, Technology and Logistics Agency (ATLA) has identified “logistical support technologies” in its medium- to long-term defense technology outlook back in 2016. More recently, ATLA has been working with private sector partners on research and development projects.
applying AI for defense logistics and “streamlining system maintenance work.”

Efforts to advance collaboration on AI-enabled military logistics and sustainment will likely face some resistance. The aforementioned challenges related to data privacy are not merely technical in nature, but deeply political as well. Some European policymakers are pushing toward data sovereignty and less dependency on U.S. technology. Others are doubting whether the United States is willing to advance meaningful regulations over digital technologies and safeguards for data privacy. The question of a forum for collaboration remains a politically sensitive topic as well, even more so now in the aftermath of Brexit.

These challenges notwithstanding, the United States and its allies have shared interests and common policy objectives in ensuring the safe and responsible use of AI in alignment with democratic norms and principles. And with allies like the United Kingdom, France, Germany, South Korea, and Japan already promoting initiatives to leverage AI for military logistics and sustainment, this seems like a politically pragmatic area for collaboration.

**Strategically critical**

The strategic environment in Europe and the Asia-Pacific region heightens the importance of coordinating national and multinational logistics, while collaboration on AI-enabled logistics can provide an operational advantage in multinational operations.

The U.S. military is a global force that must remain ahead of competitors and adversaries and be prepared for a broad range of contingencies and missions. Yet in multinational operations, the gap in military and technological capabilities between the United States and its allies and partners, and more specifically, significant discrepancies in allies’ logistic capabilities, can negatively impact survivability, interoperability, cohesion, and ultimately, mission success. Thus, for the United States and its allies, collaboration on logistics and sustainment in general, and on AI-enabled logistics and sustainment in particular, is important for several operational and strategic reasons.
Operationally speaking, logistic support during multinational military operations differs from unilateral operations. Nations have different national and military objectives, cultures, capabilities, and approaches to logistic support and functions. These differences impact how the United States military organizes, prepares, and eventually executes logistic support during multinational operations. Moreover, in multinational operations, nations share a collective responsibility for logistics in support of the mission. Thus, the logistic capabilities of each allied nation affect not only their ability to support their own forces but the operational-level support capabilities of the coalition as a whole.

On a strategic level, the global threat landscape and U.S. security posture in Europe and the Asia-Pacific region elevate the significance of joint, streamlined logistics and comparable military endurance capabilities between the United States and its allies. In Europe, on NATO’s eastern flank, the Baltic states of Estonia and Latvia, (as well as potentially Lithuania) could be overrun by Russia’s superior military forces in a matter of days. Thus, in the event of a major conflict in the Baltic states, NATO would have to move thousands of troops and heavy military equipment from across Europe as well as from the United States very rapidly and efficiently to counter Russian aggression. Sound logistics—from the coordination and transfer of military cargo ships and private merchant vessels to the surge and movement of military equipment and supplies along Europe’s roads, rivers, and incompatible rail infrastructure—would prove essential to success.

Preventing China from becoming a regional hegemon in East Asia and strengthening the U.S.-led security architecture in the western Pacific is high on the list of U.S. strategic interests. Yet the U.S. military has no local shore bases from which to project power in the region, and its dependence on more distant bases in Guam, Japan, and South Korea, presents significant operational limitations. Moreover, U.S. air bases, aircraft carriers, surface vessels, ports, airfields, and logistics systems—those already in the region and those surge forces moving into the theater in the event of a crisis or a conflict—are currently vulnerable to Chinese air and missile attacks and cyberattacks.
U.S. national security experts are well aware of these challenges and recognize the need to work with allies to protect shared security interests in these strategically important regions. For instance, the NSCAI’s interim report recommends assisting NATO in its adoption of AI and negotiating formal AI cooperation agreements with allies and partners like Australia, India, Japan, New Zealand, South Korea, and Vietnam. Moreover, the report explicitly recommends that U.S. alliances, primarily NATO, “explore pilot projects in low-risk areas such as for enterprise AI applications (logistics and sustainment) to derive lessons that would support broader application of AI systems for alliance efforts.”

Along similar lines, in their assessment of U.S. competitiveness in the Indo-Pacific region, the Center for a New American Security recommends integrating logistics and sustainment considerations into the U.S. military strategy and operational concept development for China in order to ensure that the United States is able to project and sustain combat power in the Indo-Pacific region. These efforts, however, could be strengthened by paying closer attention to the role AI/ML technologies could have in enabling more responsive logistics systems as well as in building the capacity of key partners in the region.

Certainly, when it comes to international collaboration in general, or collaborative AI projects related to military logistics and sustainment more specifically, disagreements and complications are inevitable. The past four years have seen more friction between NATO member states as well as between the United States and NATO. Rebuilding U.S. alliances is high on the Biden administration’s agenda. But restoring trust and good collaborative relationships takes time, effort, and resources. Moreover, NATO member states have very different military and technological capabilities which makes it difficult to implement alliance-wide initiatives. And while confronting China’s assertiveness is a top priority for the United States, many of the United States’ European and Asia-Pacific allies have economic and technological relationships with China. Their objectives vis-à-vis China on
questions of geopolitics and technology are not necessarily aligned with those of the United States.

Nevertheless, the strategic and operational arguments in favor of working together on AI-enabled logistics and sustainment are quite powerful. Coordination on AI embedded in logistic systems can make for more efficient and streamlined movement of personnel and equipment, enable interoperability between systems and forces, and expedite the provision of medical services. Such improvements directly contribute to the readiness and endurance of allied military forces and their ability to deter and defeat adversaries if conflict erupts.

Pathways to Collaboration

The United States and its allies face powerful technical, political, and strategic reasons to pursue and deepen collaboration on AI
applications for logistics and sustainment. Whether working within existing frameworks or building new partnerships, there are multiple pathways for collaboration. The final NSCAI report, for example, offers a comprehensive list of ongoing multilateral efforts on AI and associated technologies as well as security alliances and partnerships, some of which could serve as a forum for allies to work together on AI-enabled logistics. Below, we recommend four options for allies to explore depending on their interests and capabilities.

1. The United States and its allies should establish joint standards and protocols for the safe and secure sharing, pooling, and storage of nonsensitive datasets relevant to AI applications for logistics and sustainment.

Data relevant to AI-enabled logistics and sustainment includes data on licensing, maintenance personnel, and repair schedules for predictive maintenance; video and navigation data from ground and aerial semiautonomous and autonomous resupply systems and convoys; data supporting maritime awareness and global shipping, and many other tasks and functions.

Considering that data is the foundation of AI/ML-based applications, the United States and its allies will have to agree on standards regulating data sharing, storage, and analysis to ensure privacy, fairness, security, and respect for civil liberties. Identifying the governmental body to lead standardization efforts is a key step. Within the Department of Defense, for example, the responsibility for “the use and implementation of standardization” rests with the Defense Standardization Program Office International Standardization Program. Another option is to build on the NSCAI recommendation that the U.S. National Institute of Standards and Technology lead efforts to “promote international standardization in areas that further U.S. and allies’ national security and defense interests in the appropriate and responsible use of AI.” Allies will also need to decide on the scope of such standardization efforts. One pathway for alliance-wide collaboration is through NATO standardization agreements that facilitate interoperability, in part by ensuring the commonality of doctrine, procedures or equipment used and compatibility between
allies’ products, processes, and services. That said, the lead body and institutional configuration for standardization efforts and data partnerships related to AI-enabled logistics and sustainment can and should vary depending on allies’ needs, interests, and capabilities.

2. The United States and its allies should collaborate on R&D initiatives related to AI for logistics and sustainment.

When taken together, the R&D spending of the United States and just six like-minded nations—France, Germany, India, Japan, South Korea, and the United Kingdom—account for more than 50 percent of global R&D investment. This is a massive capacity for innovation. And when coupled with the shared interest in AI solutions for logistics and sustainment, there are many opportunities for collaborative R&D projects related to these technologies.

One option is to add joint research and development initiatives related to AI for logistics and sustainment to the agenda of early-stage collaborative efforts like the JAIC’s AI Partnership for Defense. Future meetings coordinated by this partnership could serve as a launchpad for R&D projects that include any number of the interested member states. Another option is to expand existing bilateral and multilateral R&D collaborations to include projects related to AI applications for logistics and sustainment. The Technical Cooperation Program, for example, is a collaboration forum for defense research and development activities among Australia, Canada, New Zealand, the United Kingdom, and the United States.

3. The United States and its allies should promote multinational private-public partnerships to advance research, development, procurement and fielding of AI-enabled logistics and sustainment technologies.

The United States and its allies are home to many small, midsized, and large-scale private companies with international presence and expertise in AI solutions for financial and business processes, healthcare, autonomous vehicle technology, maintenance
management, and other areas relevant to logistics and sustainment. Private companies are at the forefront of innovation in AI, and there are great opportunities to leverage their expertise and commercial interests in defense to establish new and strengthen existing multinational private-public partnerships with a focus on AI applications for logistics and sustainment.

The United States could work with allies on a bilateral basis; for example, building on Germany or South Korea’s competitive edge in autonomous vehicles technology to explore opportunities for public-private partnership for innovation in autonomous resupply technologies. There is also the option of working with and through regional bodies like the EU to support existing initiatives and public-private partnerships located in allied countries.70 Another pathway suggested by experts at the Center for a New American Security in their report on building an alliance innovation base is to “launch a cross-national platform to build new companies” focused on national security technologies.71

4. The United States and its allies should include AI-enabled logistics and sustainment technologies and capabilities in joint military exercises.

As AI-enabled technologies become more commonplace, it is vital to include them in joint multinational military exercises.72 From simulations and computer assisted command post exercises to major field exercises that include combined arms live-fire maneuvers integrating air, naval, marine, land, and cyber forces as well as civilian elements, multinational military exercises help forge personal and professional partnerships between allies, ensure doctrinal and technical interoperability, and strengthen readiness.73 Multinational logistic support is different from unilateral logistic support. Thus, if allies expect to use AI-enabled logistic and sustainment technologies in multinational missions, they would benefit from experimenting and training to do so together.

Incorporating AI-enabled technologies into joint military exercises will allow allies to test and assess the technologies’ performance and viability in uncontrolled and dynamic environments—conditions in which AI systems are known to be brittle and
vulnerable to adversarial attacks. Utilizing AI-enabled logistical elements and functions in joint exercises can also help allied militaries collect feedback from users and assess compatibility between the new technologies and existing concepts of operations, tactics, techniques, and procedures. User feedback can serve to improve the technology, while lessons learned about the ways in which new technologies fit with operational doctrine can inform necessary adjustments, ultimately, strengthening interoperability and readiness.

Moreover, including AI-enabled logistics and sustainment technologies and capabilities in military exercises can help build trust between human operators and intelligent technologies. The issue of trust in human-machine teaming is particularly consequential in the context of multinational coalition because people from different countries can differ in their attitudes toward technology which in turn could affect interoperability, military effectiveness, and mission success as a whole.⁷⁴
Conclusion

The idea of an international technology alliance grounded in a shared set of democratic ideals and ethical standards for the development and use of emerging technologies is gaining ground in the United States and among its allies and partners. Yet as the strategic competition between the United States and China intensifies, the United States may charge ahead in integrating AI into its military systems while allies trail behind. The growing gap in military and technological capabilities, in turn, could undermine interoperability and threaten the long-term viability of multinational coalitions like NATO and other key U.S. alliances.

While there are notable technical, bureaucratic, and political barriers to multinational cooperation in AI, especially for military purposes, AI applications for logistics and sustainment represent both a promising and critical area for collaboration between the United States and its allies. There are many ways allies can work together in this space, including by developing joint standards for data sharing, investing in collaborative R&D programs, advancing multinational public-private partnerships, and integrating AI-enabled logistics and sustainment technologies into joint military exercises.

Depending on allies’ interests and capabilities, these efforts can take place within existing alliances, on a bilateral basis, or through a new and separate consortium dedicated specifically to cooperation on AI-enabled logistics and sustainment technologies. Working together with allies on this set of AI technologies will help advance shared security interests, promote interoperability, and ultimately, pave the path toward the ethical and responsible use of AI in military systems and missions.
Authors

Margarita Konaev is a research fellow with CSET, where Husanjot Chahal is a research analyst.

Acknowledgments

We are grateful for the feedback and insights of our CSET colleagues, Igor Mikolic-Torreira and Andrew Imbrie. Special thanks to Gregory C. Allen from the Joint Artificial Intelligence Center and Ulrike Esther Franke of the European Council on Foreign Relations for their thoughtful reviews of this report. We are also thankful to Matt Mahoney for fact-checking, and to Lynne Weil and the CSET external affairs team for editorial support.
Endnotes


“States Calling for a Treaty to Ban and Restrict Killer Robots.”


European Parliament, Artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (Brussels: European Union, January 2021), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html.

Of the 28 surveyed countries, the only one where the majority of respondents did not oppose the use of lethal autonomous weapons was India. “Global Survey Highlights Continued Opposition to Fully Autonomous Weapons,” Ipsos, February 2, 2021, https://www.ipsos.com/en-us/global-survey-highlights-continued-opposition-fully-autonomous-weapons.


boycott/researchers-to-boycott-south-korean-university-over-ai-weapons-work-idUSKCN1HB392.


18 Hobbs, “Europe’s digital sovereignty.”


20 While the GDPR came into force in 2018, it was the 2020 Court of Justice of the European Union decision in Schrems II rendering the EU-U.S. Privacy Shield invalid and closing off key mechanisms for transferring personal data from the EU to the U.S. that arguably has had the most consequential impact on trade and the development of emerging technologies. Joshua P. Meltzer, “The Court of Justice of the European Union in Schrems II: The impact of GDPR on data flows and national security” (Brookings Institution, August 5, 2020), https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.


22 National Security Commission on Artificial Intelligence, First Quarter Recommendations, 64-65.

23 North Atlantic Treaty Organization, “Cooperation on Artificial Intelligence will boost security and prosperity.”


38 Tonin, Artificial Intelligence.

39 We are grateful to Greg Allen for this observation as well as his input about the problems with military data.


42 We are grateful to Andrew Imbrie for this observation. For more on this topic, see Imbrie et al., “Agile Alliances,” 21–22.


55 Ulrike Franke, “Artificial divide: How Europe and America could clash over AI.”

57 NATO Standardization Office, NATO Standard: Allied Joint Doctrine for Logistics.


61 National Security Commission on Artificial Intelligence, Interim Report and Third Quarter Recommendations, 22.

62 National Security Commission on Artificial Intelligence, Interim Report and Third Quarter Recommendations, 226.

63 Ratner et al., “Rising to the China Challenge,” 17.


66 National Security Commission on Artificial Intelligence, Interim Report and Third Quarter Recommendations, 213.

67 United States Department of the Army, Army Regulation 34-1: Standardization: Interoperability (Washington, D.C., April 9, 2020), 29,

Kliman et al., “Forging an Alliance Innovation Base,” 11.


