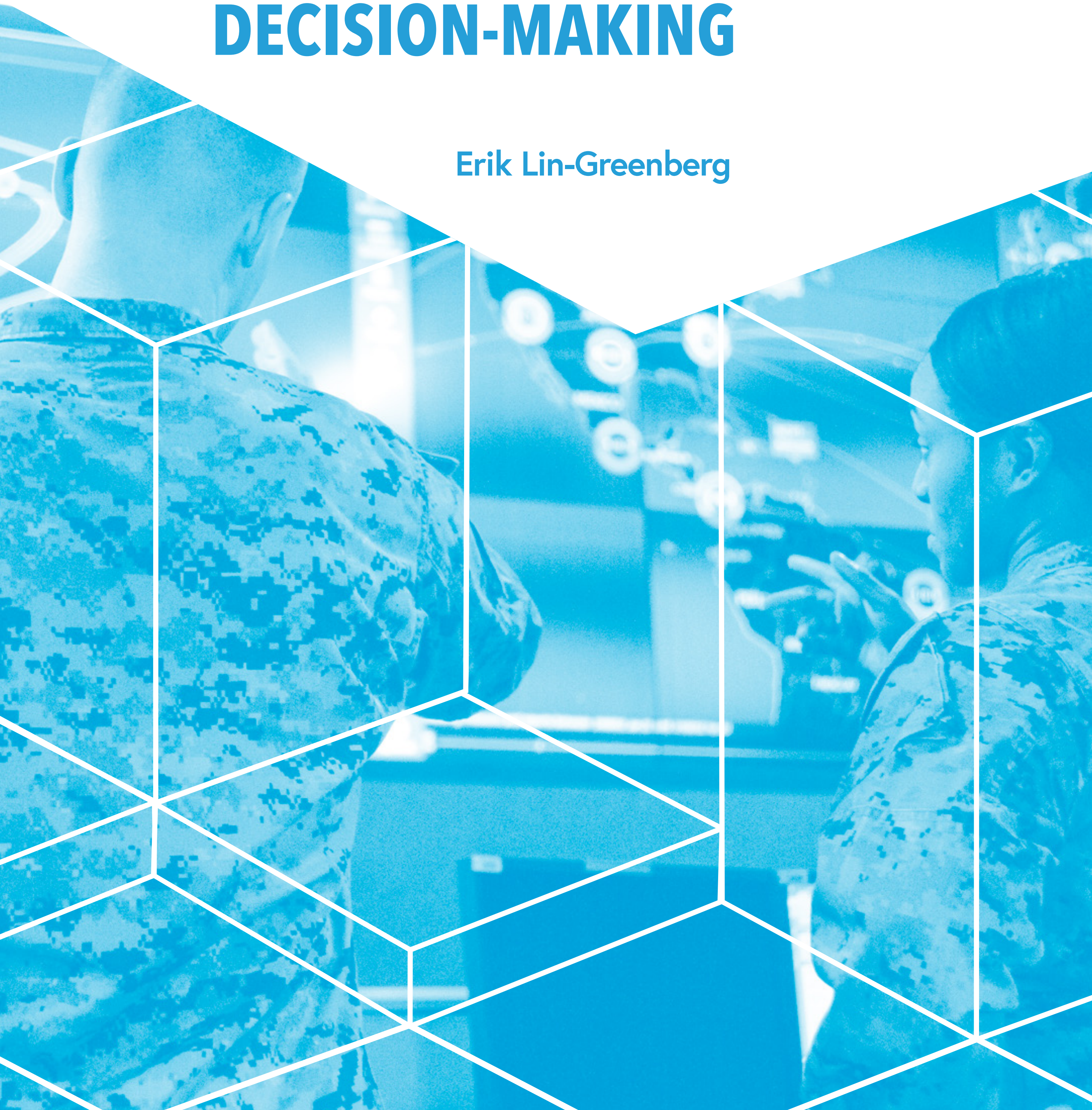
The Scholar

Texas National Security Review: Volume 3, Issue 2 (Spring 2020)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

ALLIES AND ARTIFICIAL INTELLIGENCE: OBSTACLES TO OPERATIONS AND DECISION-MAKING

Erik Lin-Greenberg



Artificial intelligence (AI) promises to increase military efficiency, but also poses unique challenges to multinational military operations and decision-making that scholars and policymakers have yet to explore. The data- and resource-intensive nature of AI development creates barriers to burden-sharing and interoperability that can hamper multinational operations. By accelerating the speed of combat and providing adversaries with a tool to heighten mistrust between allies, AI can also strain the complex processes that allies and security partners use to make decisions. To overcome these challenges and prepare for AI-enabled warfare, policymakers need to develop institutional, procedural, and technical solutions that streamline decision-making and enhance interoperability.

In June 2019, the United States announced a new artificial intelligence (AI) partnership with Singapore that calls for collaboration on the development and use of AI technologies in the national security domain.[1] Is this type of cooperation a harbinger of things to come? The burgeoning military use of AI — technology that carries out tasks that normally require human intelligence — has the potential to alter how states carry out military operations. AI-enabled technologies — like autonomous drone swarms and algorithms that quickly sift through massive amounts of information — can increase the speed and efficiency of warfare, but they may also exacerbate the coordination and decision-making challenges frequently associated with multinational military operations carried out by allies and security partners.

Policymakers and experts in the United States and other countries have urged international cooperation on the development and use of AI, but this guidance overlooks important questions about the challenges of AI collaboration in the security domain. President Donald Trump's executive order on AI directs "enhance[ed] international and industry collaboration with foreign partners and allies" to maintain "American leadership in AI."[2] Similarly, the congressionally chartered National Security Commission on Artificial Intelligence warns, "If the United States and its allies do not coordinate early and often on AI-enabled capabilities, the effectiveness of our military coalitions will suffer."[3] Several of Washington's allies have echoed these calls for collaboration. Germany's 2019 *National AI Strategy* advocates for "work[ing] with the nations leading in this field … to conduct joint bilateral and/or multilateral R&D activities on the development and use of AI."[4] While cooperation is important, what challenges might allies and partners encounter as they work together to develop and deploy AI in the military domain? And what steps might states take to overcome these obstacles?

States are racing to achieve superiority in the

[1] Prashanth Parameswaran, "What's in the New US-Singapore Artificial Intelligence Defense Partnership?" *The Diplomat*, July 1, 2019, https://thediplomat.com/2019/07/whats-in-the-new-us-singapore-artificial-intelligence-defense-partnership/.

[2] Donald J. Trump, "Executive Order on Maintaining American Leadership in Artificial Intelligence," The White House, Feb. 11, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/.

[3] "Interim Report," National Security Commission on Artificial Intelligence, November 2019, 45, https://drive.google.com/file/d/153OrxnuGE-jsUvlxWsFYauslwNeCEkvUb/view. The National Security Commission on Artificial Intelligence is an independent group of experts chartered by Congress to help shape U.S. AI development.

[4] *Nationale Strategie Für Künstliche Intelligenz [Artificial Intelligence Strategy]*, German Federal Government, November 2018, 41, http://www.ki-strategie-deutschland.de/.

AI domain, and AI research and development is flourishing: In early 2019, the U.S. Department of Defense unveiled its AI strategy.[5] Meanwhile, China has pledged to develop a $150 billion AI sector by 2030,[6] and Russian President Vladimir Putin famously asserted, "whoever becomes the leader in [AI] will become the ruler of the world."[7] AI development promises to bring enhanced accuracy and efficiency to complex and dangerous tasks, but policymakers and scholars have yet to fully explore how these benefits compare with potential risks — particularly in the context of multinational military operations.[8] To be sure, decision-makers have expressed concerns about the reliability of AI technologies and the ethical implications of delegating military operations to computers.[9] These AI-specific challenges, however, may magnify the coordination and commitment challenges that frequently plague military operations conducted by multinational alliances and coalitions.

Drawing from theories of alliance politics and analysis of emerging AI technologies, I map out two areas where AI could hamper multinational military operations. First, AI could pose challenges to operational coordination by complicating burden-sharing and the interoperability of multinational forces. Not all alliance or coalition members will possess AI capabilities, raising barriers to military cooperation as AI-enabled warfare becomes increasingly common. States with AI technologies will also need to overcome political barriers to sharing the sensitive data required to develop and operate AI-enabled systems. At the same time, rivals can stymie multinational coordination by using AI to launch deception campaigns aimed at interfering with an alliance's military command-and-control processes.

Second, AI could hamper alliance and coalition decision-making by straining the processes and relationships that undergird decisions on the use of force. By increasing the speed of warfare, AI could decrease the time leaders, from the tactical to strategic levels, have to debate policies and make decisions. These compressed timelines may not allow for the complex negotiations and compromises that are defining characteristics of alliance politics.[10] Decision-making may be further hampered if the "black box" and unexplainable nature of AI causes leaders to lack confidence in AI-enabled systems. And, just as adversaries could use AI to interfere with command and control, they could also use AI to launch misinformation campaigns that sow discord among allies and heighten fears that allies will renege on their commitments.

To be sure, barriers to multinational military cooperation are not new, but AI may intensify these difficulties.[11] To help overcome these obstacles to coordination and decision-making challenges, alliance and coalition leaders can draw lessons from past cases of successful cooperation and a growing corpus of national-level AI strategies to develop international agreements and standards that streamline the integration of AI into multinational operations.

This article makes three contributions to scholarly and policy debates in international relations. First, it investigates how technology shapes alliance relationships and multinational military operations. Most scholarly work on alliances and security partnerships has focused on the reasons behind their creation,[12] their institutional design

[5] *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, U.S. Department of Defense, 2019, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[6] Arthur Herman, "China's Brave New World Of AI," *Forbes*, Aug. 30, 2018, https://www.forbes.com/sites/arthurherman/2018/08/30/chinas-brave-new-world-of-ai/#3a7918bf28e9.

[7] Radina Gigova, "Who Putin Thinks Will Rule the World," *CNN*, Sept. 2, 2017, https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html.

[8] For one exception see, Martin Dufour, "Will Artificial Intelligence Challenge NATO Interoperability," NATO Defense College Policy Brief, Dec. 10, 2018, http://www.ndc.nato.int/news/news.php?icode=1239.

[9] Colin Clark, "Air Combat Commander Doesn't Trust Project Maven's Artificial Intelligence — Yet," *Breaking Defense*, Aug. 21, 2019, https://breakingdefense.com/2019/08/air-combat-commander-doesnt-trust-project-mavens-artificial-intelligence-yet/.

[10] Throughout the article, I use the term "alliance politics" to describe the political coordination among both formal treaty allies and less institutionalized security partners. Furthermore, for clarity, I use the term "allies" to encompass both formal allies and other security partners.

[11] Keith Hartley, "NATO, Standardisation and Nationalism: An Economist's View," *RUSI Journal* 123, no. 3 (1978): 57–60, https://doi.org/10.1080/03071847809422917; David S. Yost, "The NATO Capabilities Gap and the European Union," *Survival* 42, no. 4 (December 2000): 205.

[12] Stephen M. Walt, *The Origins of Alliance* (Ithaca, NY: Cornell University Press, 1990); Glenn H. Snyder, *Alliance Politics* (Ithaca, NY: Cornell University Press, 1997); Jesse C. Johnson, "External Threat and Alliance Formation," *International Studies Quarterly* 61, no. 3 (September 2017): 736–45, https://doi.org/10.1093/isq/sqw054; Matthew Digiuseppe and Paul Poast, "Arms Versus Democratic Allies," *British Journal of Political Science* 48, no. 4 (October 2018): 981–1003, https://doi.org/10.1017/S0007123416000247.

and processes,[13] their effectiveness at reassuring friends and deterring rivals,[14] and their survival amid changing political conditions.[15] Much of this work has overlooked the effects of specific technologies on alliance politics, with the exception of studies on nuclear weapons. Second, the article builds upon research examining the role of emerging technologies in international security, more broadly. Existing studies have explored how militaries adopt new technologies,[16] how those technologies affect conflict initiation and escalation,[17] and how they shape force structure and doctrine.[18] This article broadens this line of research by investigating how technology can both stymie and advance cooperation between states in the security domain. Third, the paper contributes to policy debates surrounding the increasing use of AI in military settings. Existing analyses have explored potential applications of AI,[19] its effects on the balance of power,[20] and the ethical and domestic political considerations associated with battlefield AI use.[21] A deeper understanding of how AI can influence security partnerships and alliances may help inform policymaking.

This paper proceeds in five parts. First, I briefly define artificial intelligence and describe its military applications. Second, I survey the scholarly literature on alliance politics and multinational operations, focusing on the challenges of planning and carrying out operations. Third, I identify how AI can magnify these challenges. Fourth, I investigate how these AI-associated challenges might be overcome. I conclude by outlining potential avenues for future research.

Artificial Intelligence and International Security Applications

Broadly defined, AI is the ability of computers and machines to perform tasks that traditionally require human intelligence.[22] AI has been applied to control self-driving cars and swarms of unmanned aircraft, to assist physicians in making medical diagnoses, and at the more quotidian level, to screen spam emails and act as virtual personal assis-

[13] James D. Morrow, "Alliances: Why Write Them Down?" *Annual Review of Political Science* 3, no. 1 (June 2000): 63–83, https://doi.org/10.1146/annurev.polisci.3.1.63; Daina Chiba, Jesse C. Johnson, and Brett Ashley Leeds, "Careful Commitments: Democratic States and Alliance Design," *Journal of Politics* 77, no. 4 (October 2015): 968–82, https://www.jstor.org/stable/10.1086/682074.

[14] Glenn H. Snyder, "The Security Dilemma in Alliance Politics," *World Politics* 36, no. 4 (July 1984): 461–95, https://www.jstor.org/stable/2010183; Thomas J. Christensen and Jack Snyder, "Chain Gangs and Passed Bucks: Predicting Alliance Patterns in Multipolarity," *International Organization* 44, no. 2 (Spring 1990): 137–68, https://www.jstor.org/stable/2706792; Michael Beckley, "The Myth of Entangling Alliances: Reassessing the Security Risks of U.S. Defense Pacts," *International Security* 39, no. 4 (Spring 2015): 7–48, https://doi.org/10.1162/ISEC_a_00197; Michael R. Kenwick, John A. Vasquez, and Matthew A. Powers, "Do Alliances *Really* Deter?" *Journal of Politics* 77, no. 4 (October 2015): 943–54, https://doi.org/10.1086/681958.

[15] Robert B. McCalla, "NATO's Persistence After the Cold War," *International Organization* 50, no. 3 (Summer 1996): 445–75, https://doi.org/10.1017/S0020818300033440; Celeste A. Wallander, "Institutional Assets and Adaptability: NATO after the Cold War," *International Organization* 54, no. 4 (Autumn 2000): 705–35, https://doi.org/10.1162/002081800551343; Brett Ashley Leeds, "Alliance Reliability in Times of War: Explaining State Decisions to Violate Treaties," *International Organization* 57, no. 4 (Fall 2003): 801–27, https://doi.org/10.1017/S0020818303574057; Brett Ashley Leeds and Burcu Savun, "Terminating Alliances: Why Do States Abrogate Agreements?" *Journal of Politics* 69, no. 4 (November 2007): 1118–32, https://doi.org/10.1111/j.1468-2508.2007.00612.x; Molly Berkemeier and Matthew Fuhrmann, "Reassessing the Fulfillment of Alliance Commitments in War," *Research & Politics* 5, no. 2 (April 2018), https://doi.org/10.1177%2F2053168018779697.

[16] Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1994); Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010).

[17] Michael C. Horowitz, Sarah E. Kreps, and Matthew Fuhrmann, "Separating Fact from Fiction in the Debate over Drone Proliferation," *International Security* 41, no. 2 (Fall 2016): 7–42, https://doi.org/10.1162/ISEC_a_00257; Sarah E. Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics," SSRN, Jan. 17, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3104014.

[18] Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, no. 2 (March/April 1996): 37–54, https://www.foreignaffairs.com/articles/united-states/1996-03-01/revolution-warfare; Melissa K. Griffith, "A Comprehensive Security Approach: Bolstering Finnish Cybersecurity Capacity," *Journal of Cyber Policy* 3, no. 3 (September 2018): 407–29, https://doi.org/10.1080/23738871.2018.1561919; Max Smeets, "Integrating Offensive Cyber Capabilities: Meaning, Dilemmas, and Assessment," *Defence Studies* 18, no. 4 (October 2018): 395–410, https://doi.org/10.1080/14702436.2018.1508349.

[19] Michael C. Horowitz, "The Promise and Peril of Military Applications of Artificial Intelligence," *Bulletin of the Atomic Scientists*, April 23, 2018, https://thebulletin.org/2018/04/the-promise-and-peril-of-military-applications-of-artificial-intelligence/; Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton & Company, 2019).

[20] Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018): 36–57, https://doi.org/10.15781/T2639KP49; Adrian Pecotic, "Whoever Predicts the Future Will Win the AI Arms Race," *Foreign Policy*, March 5, 2019, https://foreignpolicy.com/2019/03/05/whoever-predicts-the-future-correctly-will-win-the-ai-arms-race-russia-china-united-states-artificial-intelligence-defense/.

[21] Peter Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-Making," *International Review of the Red Cross* 94, no. 886 (Summer 2012), https://doi.org/10.1017/S1816383112000768; On the domestic politics of AI-enabled weapons use, see, Michael C Horowitz, "Public Opinion and the Politics of the Killer Robots Debate," *Research & Politics* 3, no. 1 (January 2016): 1–8, https://doi.org/10.1177%2F2053168015627183.

[22] *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, U.S. Department of Defense, February 2019, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

tants.[23] Underlying AI technologies are a variety of approaches including mathematical optimization, statistical methods, and artificial neural networks — computer systems that attempt to perform specific tasks in a similar way to the human brain.[24] Regardless of approach, AI typically uses large amounts of data to train and feed algorithms to accomplish tasks and processes that are normally associated with human cognition. Most current AI is considered to be "narrow," designed to achieve a specific task — like identifying objects in images. Researchers, however, are working to develop artificial general intelligence that can accomplish any task the human brain can.[25]

Narrow AI technology has increasingly been applied in the national security domain. Although much policy and scholarly writing focuses on lethal autonomous weapon systems — "killer robots" that can identify and engage targets without human intervention — AI is far more commonly employed in a range of more mundane military and national security tasks.[26] In some cases, AI is part of analytical processes, like the use of machine learning to classify targets in satellite imagery.[27] In other instances, it is part of the software used to operate physical systems, like autonomous planes or ships.[28] In both cases, AI is not a military capability in itself, but an enabler that can enhance the efficiency of military tasks and systems.[29]

Many regional and global military powers have already fielded AI-enabled military systems.[30] Israel and Russia, for instance, have reportedly tested self-driving tanks and armored vehicles capable of identifying targets without human direction.[31] The United States is making headway on Project Maven, the Defense Department's effort to use machine learning — an application of AI — to streamline the analysis of video gathered by drones.[32] Similarly, Japan's Self-Defense Force announced that it will equip its P-1 maritime patrol aircraft with AI technology that will more effectively identify vessels and other potential targets.[33] States have also begun incorporating AI into autonomous systems that can navigate without direction by human operators, often in swarms intended to overwhelm an enemy's defenses. In 2017, for instance, the U.S. Naval Postgraduate School and the Defense Advanced Research Projects Agency hosted a large-scale experiment where swarms of autonomous drones flew simulated combat missions against each other.[34]

The development of these systems should not come as a surprise. Military and political decision-makers seek to enhance the efficiency and accuracy of their state's military and to reduce risk and costs during operations. AI can help accomplish these objectives. In many contexts, AI can make assessments and judgements with greater speed and accuracy than humans, and with less manpower. For example, AI can help quickly dig through vast quantities of imagery and video data to pinpoint objects of interest, like military vehi-

[23] Javier Chagoya, "NPS, Academic Partners Take to the Skies in First-Ever UAV Swarm Dogfight," Naval Postgraduate School, Feb. 22, 2017, https://web.nps.edu/About/News/NPS-Academic-Partners-Take-to-the-Skies-in-First-Ever-UAV-Swarm-Dogfight.html; Riccardo Miotto et al., "Deep Patient: An Unsupervised Representation to Predict the Future of Patients from the Electronic Health Records," *Scientific Reports*, no. 6 (2016), https://doi.org/10.1038/srep26094.

[24] For a primer on these concepts, see, Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford: Oxford University Press, 2016).

[25] For some of the latest research on artificial general intelligence, see, Patrick Hammer et al., eds., *Proceedings of the 12th International Conference on Artificial General Intelligence (Shenzhen, China)* (New York: Springer, 2019).

[26] M.L. Cummings, *Artificial Intelligence and the Future of Warfare*, Chatham House, January 2017, https://www.chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf.

[27] "Deep Learning Model Speeds Up, Automates Satellite Image Analysis," Lockheed Martin, June 5, 2019, https://news.lockheedmartin.com/news-releases?item=128745.

[28] Megan Eckstein, "Sea Hunter Unmanned Ship Continues Autonomy Testing as NAVSEA Moves Forward with Draft RFP," *USNI News*, April 29, 2019, https://news.usni.org/2019/04/29/sea-hunter-unmanned-ship-continues-autonomy-testing-as-navsea-moves-forward-with-draft-rfp.

[29] Horowitz, "The Promise and Peril of Military Applications of Artificial Intelligence."

[30] This paragraph focuses on the use of AI for conventional interstate military operations, but states are also using AI to bolster their internal security. Autocratic states have leveraged AI to monitor domestic populations and root out dissent. China, for example, is building a web of surveillance systems that employ automated facial recognition and other AI technology to track members of the public. See, Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

[31] Sebastien Roblin, "Russia's Uran-9 Robot Tank Went to War in Syria (It Didn't Go Very Well)," *National Interest*, Jan. 6, 2019, https://nationalinterest.org/blog/buzz/russias-uran-9-robot-tank-went-war-syria-it-didnt-go-very-well-40677; Judah Ari Gross, "Defense Ministry Unveils 3 Prototypes for Israel's Tanks of the Future," *Times of Israel*, Aug. 4, 2019, https://www.timesofisrael.com/defense-ministry-unveils-3-prototypes-for-israels-tanks-of-the-future/.

[32] Colin Clark, "In 1st Interview, PDUSDI Bingen Talks Artificial Intelligence, Project Maven, Ethics," *Breaking Defense*, Aug. 26, 2019, https://breakingdefense.com/2019/08/in-1st-interview-pdusdi-bingen-talks-artificial-intelligence-project-maven-ethics/.

[33] Kosuke Takahashi, "Japan to Outfit Kawasaki P-1 MPAs with AI Technology," *Jane's 360*, Nov. 13, 2019, https://www.janes.com/article/92545/japan-to-outfit-kawasaki-p-1-mpas-with-ai-technology.

[34] Chagoya, "NPS, Academic Partners Take to the Skies in First-Ever UAV Swarm Dogfight."

cles, with little human involvement.[35] In contrast, geospatial intelligence exploitation that is not assisted by AI is a time-intensive and manpower-intensive process.[36] AI can also be used to operate autonomous weapon systems that allow states to launch military operations without putting friendly personnel in harm's way. These systems can decrease the risk of friendly casualties and reduce the political barriers to launching military operations.[37] The efficiency-enhancing and risk-reducing characteristics of AI-enabled systems will likely appeal to casualty-averse and cost-conscious leaders. Indeed, AI technologies might allow these leaders to launch operations not previously possible because of efficiency concerns or high degrees of risk to friendly forces.

Allies, Partners, and the Challenges of Artificial Intelligence

Military operations today are commonly carried out by alliances or other multilateral coalitions — formal or informal arrangements between states.[38] Allies cooperate militarily and diplomatically to respond to mutual threats and achieve common objectives, yielding both political and military benefits.[39] Politically, multinational operations can impart legitimacy to military operations in the eyes of both domestic and international audiences. Support for military action from a broad coalition of allies and partners can serve as a cue to the public that the action is justified, and help counter narratives that a state's military operations are improper or seek to upset the status quo.[40] From a military perspective, alliances and coalitions allow states to share the burden of operations.[41] Unlike unilateral operations, where a single state provides all personnel and equipment, alliances allow for the division of labor across all member states. To facilitate cooperation, allies often engage in consultative decision-making, develop shared operating procedures, build integrated command-and-control networks, acquire interoperable weapon systems that can integrate on the battlefield, and participate in joint military exercises.

Although alliances and multilateral coalitions can bolster the security of member states and the efficiency of their military operations, membership can create complications for decision-making and the coordination of military operations. First, alliances and coalitions must overcome operational challenges surrounding the integration and coordination of military forces. Modern military operations require the close coordination of participating forces, shared intelligence to guide planning and mission execution, and weapon systems capable of communicating with and operating alongside each other. The military of each alliance or coalition member state brings with it different equipment, policies, and tactics, meaning that a state's forces may not fully integrate with the forces of its allies.[42] Moreover, partners are often reluctant to share sensitive operational and intelligence information.[43] Beyond these institutional issues, more commonplace matters — such as the different languages and military cultures of each member state — can hinder interoperability during contingency operations.[44]

Second, alliance and coalition leaders may have trouble deciding what policies their coalition should pursue. Although allies typically face a common threat and share many policy objectives, each state still maintains its own priorities and goals. State leaders therefore respond to domestic constituencies and pursue their own national

[35] Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," U.S. Department of Defense, July 21, 2017, https://www.defense.gov/Explore/News/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

[36] For studies that assess the time intensive nature of intelligence analysis, see, Dino A. Brugioni, *Eyes in the Sky: Eisenhower, the CIA and Cold War Aerial Espionage* (Annapolis, MD: Naval Institute Press, 2010); Hugh Gusterson, *Drone: Remote Control Warfare* (Cambridge, Massachusetts: The MIT Press, 2016), 59–82; Chris Woods, *Sudden Justice: America's Secret Drone Wars* (Oxford: Oxford University Press, 2015).

[37] John Kaag and Sarah Kreps, *Drone Warfare* (Cambridge, UK: Polity, 2014).

[38] Walt, *The Origins of Alliance*, 12.

[39] Snyder, *Alliance Politics*, 7.

[40] Jonathan A. Chu, "Essays on Liberal Norms, Public Opinion, and the Law of War," PhD Dissertation, Stanford University, 2018. Support from international organizations other than alliances can also serve as a cue. See, Erik Voeten, "The Political Origins of the UN Security Council's Ability to Legitimize the Use of Force," *International Organization* 59, no. 3 (July 2005): 527–57, https://doi.org/10.1017/S0020818305050198.

[41] Mancur Olson, Jr. and Richard Zeckhauser, "An Economic Theory of Alliances," *Review of Economics and Statistics* 48, no. 3 (August 1966): 266–79, https://www.jstor.org/stable/1927082; Andres J. Gannon, "How States Fight: Measuring Heterogeneity in the Distribution of State Military Capabilities" (Working Paper, 2019).

[42] *Joint Publication 3-16: Multinational Operations*, Joint Chiefs of Staff, March 1, 2019, I-3, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_16.pdf; Eric Larson et al., *Interoperability: A Continuing Challenge in Coalition Air Operations* (Santa Monica, CA: Rand, 2000).

[43] James Igoe Walsh, *The International Politics of Intelligence Sharing* (New York: Columbia University Press, 2009), chap. 1.

[44] Roger H. Palin, *Multinational Military Forces: Problems and Prospects* (Oxford: Oxford University Press, 1995).

interests, which, at times, may be at odds with alliance goals.[45] At best, these divergent interests result in coordination problems that draw out decision-making timelines.[46] At worst, they generate mistrust between partners and raise concerns of being abandoned during a crisis or "chain-ganged" into unwanted wars.[47]

Politically, "AI haves" may complain that "AI have-nots" are not adequately contributing to a mission, straining relations between allies. Operationally, capability gaps can hamper an alliance's ability to deploy forces or achieve military objectives.

While alliances and coalitions are comprised of member states with shared interests, there is significant variation in the degree of formalization of security partnerships that can affect how they plan and execute military operations. On the formal end of the continuum are alliances like NATO that are governed by treaties. These formal treaties invoke obligations and a sense of trust not typically found in less formalized, tacit arrangements.[48] On the less formal end of the spectrum are coalitions, security arrangements that are generally more ad hoc and focused on achieving a specific and narrow goal.[49] For example, George W. Bush's "coalition of the willing" brought together more than three dozen countries during the 2003 Iraq War.[50] Because of their more limited goals, coalitions are often temporary entities that exist only until their mission is accomplished, and frequently lack the institutional arrangements that help strengthen ties and coordination between allies. The analysis in this article applies across the continuum of formalization, but the challenges that AI poses to alliance operations and decision-making should be more vexing for coalitions that lack formalization. For clarity throughout the remainder of the article, I use the term alliances to describe security partnerships across the spectrum of formalization.

AI Obstacles to Alliance Operations

At the operational level, AI can complicate burden-sharing and the interoperability of alliance military forces. The development and integration of AI technology in the security domain poses three challenges to coordination during alliance military operations. First, not all states will develop military applications of AI at the same rate. Within an alliance, some states will possess and effectively operate AI-enabled capabilities, while others will not. This unequal distribution of technology can hinder burden-sharing and interoperability. Second, allies will need to resolve the political and technical challenges associated with developing interoperable AI-enabled systems and sharing the data that underpins AI technology. Data are often difficult to share and states are often loath to share sensitive information. Third, adversaries are likely to use AI to disrupt allied military operations.

Complicating Burden-Sharing: Artificial Intelligence Haves and Have-Nots

Despite the surge in international attention on AI, not all states have developed robust AI capabilities, particularly for military applications. One recent study finds significant variation in the capacity of states to "exploit the innovative potential of AI" for government purposes.[51] States like the

[45] Kenneth N. Waltz, *Theory of International Politics* (Boston, MA: McGraw Hill, 1979), 163-170; Snyder, "The Security Dilemma in Alliance Politics"; John J. Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (Winter 1994/1995): 11, https://www.jstor.org/stable/2539078.

[46] Mearsheimer, "The False Promise of International Institutions," 32; For an assessment of the various factors that can shape decision-making timelines in international organizations, see, Heidi Hardt, *Time to React: The Efficiency of International Organizations in Crisis Response* (Oxford: Oxford University Press, 2017).

[47] Christensen and Snyder, "Chain Gangs and Passed Bucks"; Snyder, "The Security Dilemma in Alliance Politics"; Leeds, "Alliance Reliability in Times of War." Some scholars argue that the risks of entangling alliances are overstated: Beckley, "The Myth of Entangling Alliances."

[48] Morrow, "Alliances: Why Write Them Down?

[49] *Joint Publication 3-16: Multinational Operations*, I-3. This type of relationship is sometimes referred to as an "alignment." Roger Dingman, "Theories of, and Approaches to, Alliance Politics," in *Diplomacy: New Approaches in History, Theory, and Policy*, ed. Paul Gordon Lauren (New York: Free Press, 1979), 245–66.

[50] Ewen MacAskill, "US Claims 45 Nations in 'Coalition of Willing,'" *The Guardian*, March 18, 2003, https://www.theguardian.com/world/2003/mar/19/iraq.usa.

[51] *Government Artificial Intelligence Readiness Index 2019*, Government of Canada and Oxford Insights, 2019, 5, https://ai4d.ai/wp-content/uploads/2019/05/ai-gov-readiness-report_v08.pdf.

United Kingdom, Germany, and the United States receive high marks for AI readiness, while other allies like Spain, Turkey, and Montenegro fall lower on the readiness scale.[52] This unequal distribution of AI technology can result from differences in the organizational, financial, and human capital available to develop and deploy new technologies and differences in political support for the use of AI.[53] Uneven distribution of AI technologies has important implications for the ability of allies and partners to divide military tasks during crises.

Variation in the capacity to adopt and integrate AI technology into state militaries can create AI "haves" and "have-nots." Some states — like Germany — possess a robust technology sector, have the financial resources to fund research and acquisitions, and maintain defense bureaucracies that are sufficiently skilled and flexible to integrate new AI technologies.[54] Indeed, many of these states have created government institutions to manage military AI development. The United States, for example, established the Joint Artificial Intelligence Center in 2018 to coordinate the Defense Department's AI programs.[55] Other states lack these resources and are unable to rigorously pursue new AI capabilities. For instance, many of NATO's economically weaker members have focused their defense spending on modernizing conventional forces and updating Cold War-era hardware, and not on AI development.[56]

Even if a state has the resources to develop AI capabilities, limited public support for AI-enabled military systems can hamper such efforts. Opposition can stem from the uncertainty surrounding AI's functionality, or from moral and ethical objections to delegating decisions on the use of force to computers. One recent cross-national survey, for instance, finds significant public disapproval of the use of lethal autonomous weapons among key U.S. allies. To be sure, autonomous weapons and AI are distinct, but AI is incorporated into the software architecture of most autonomous systems, and pundits and the public often conflate the two.[57] In South Korea and Germany, 74 and 72 percent of the local populations, respectively, oppose their use (compared to 52 percent opposition among the U.S. public).[58] These two countries are close U.S. allies that host dozens of U.S. military installations and over 60,000 American troops.[59]

Tepid public support at home and abroad can stymie alliance military operations in two ways. First, public opposition to the use of AI among allied populations may lead policymakers to restrict the use of AI-enabled technologies for military operations. In the event of future hostilities, for example, the South Korean or German governments might oppose an ally's use of AI-enabled lethal weapon systems on their territory.[60] Indeed, advocacy from the public and activist groups has led a growing number of states — including U.S. allies like Pakistan and Jordan — to call for bans on the use of lethal autonomous weapon systems.[61]

Second, civilian engineers and researchers that develop AI technology may refuse to work on military AI contracts. Disruptions to AI development can hinder the fielding of new capabilities and generate mistrust between the government and civilian firms. Google employees, for instance, protested their involvement in Project Maven, a Defense Department program that uses AI to analyze video collected by military drones.[62] In a letter to their CEO, the employees argued that "Google should

[52] *Government Artificial Intelligence Readiness Index 2019*, 32–37.

[53] Horowitz, *The Diffusion of Military Power*, chap. 2.

[54] For research on the factors that can lead to variation in military innovation and technological adoption, see, Rosen, *Winning the Next War*, Dima Adamsky, *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel* (Stanford, CA: Stanford University Press, 2010); and Horowitz, *The Diffusion of Military Power*.

[55] Terri Moon Cronk, "DOD Unveils Its Artificial Intelligence Strategy," U.S. Department of Defense, Feb. 12, 2019, https://www.defense.gov/Explore/News/Article/Article/1755942/dod-unveils-its-artificial-intelligence-strategy/.

[56] Albania, for instance, has focused on replacing Cold War-era equipment. "Modernization of the Armed Forces," Republic of Albania Ministry of Defense, Oct. 12, 2019, http://www.mod.gov.al/eng/index.php/security-policies/others-from-mod/modernization/68-modernization-of-the-armed-forces.

[57] "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense," Defense Innovation Board, Oct. 31, 2019, 5, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

[58] "Six in Ten (61%) Respondents Across 26 Countries Oppose the Use of Lethal Autonomous Weapons Systems," *Ipsos*, Jan. 21, 2019, https://www.ipsos.com/en-us/news-polls/human-rights-watch-six-in-ten-oppose-autonomous-weapons.

[59] "Number of Military and DoD Appropriated Fund Civilian Personnel Permanently Assigned by Duty Location and Service/Component (as of Sept. 30, 2019)," Defense Manpower Data Center, Nov. 8, 2019, https://www.dmdc.osd.mil/appj/dwp/dwp_reports.jsp.

[60] Recent research suggests public opposition to the use of lethal autonomous weapon systems decreases when rivals acquire similar systems. See, Horowitz, "Public Opinion and the Politics of the Killer Robots Debate."

[61] "Country Views on Killer Robots," Campaign to Stop Killer Robots, Aug. 21, 2019, https://www.stopkillerrobots.org/wp-content/uploads/2019/08/KRC_CountryViews21Aug2019.pdf.

[62] Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End."

not be in the business of war," explaining that the company should not "outsource the moral responsibility of [its] technologies to third parties," and that work on Defense Department-backed AI would "irreparably damage Google's brand."[63] The resistance ultimately led Google to terminate its involvement in the contract and generated public criticism of the Defense Department's AI efforts.[64]

The existence of "AI haves" and "AI have-nots" within an alliance can complicate burden-sharing — a central tenet of military alliances. On one hand, states with robust AI capabilities can specialize their contributions to alliance operations and focus on providing AI-related capabilities. If, however, AI applications become a necessity for warfighting in the future, states that lack AI capabilities may be less able to contribute to alliance operations. States better equipped with AI capabilities may subsequently be forced to take on a greater share of work, generating both political and operational challenges. Politically, "AI haves" may complain that "AI have-nots" are not adequately contributing to a mission, straining relations between allies. Operationally, capability gaps can hamper an alliance's ability to deploy forces or achieve military objectives. During the NATO-led air war over Kosovo in 1999, for instance, many NATO members possessed limited numbers of precision-guided munitions in their arsenals and often lacked the training to employ them, curtailing their ability to contribute to operations.[65] As a result, responsibility for carrying out the air campaign fell to a small number of allies. In a larger conflict, burden-sharing might be critical to sustaining operations or securing battlefield victories.

Data Sharing and Standardization

As the number of states that employ military AI applications grows, the ability of allies to operate collectively will depend, in part, on the sharing of data that fuels AI systems. AI requires massive amounts of data to train and feed algorithms and models. To identify a surface-to-air missile site, for instance, an AI image classifier must learn to differentiate missile sites from other facilities by studying images of known missile sites. The more data used to train these systems, the more accurate the system will be.[66] Once fielded, AI-enabled systems like the image classifier must continue to be fed imagery from reconnaissance aircraft, satellites, or other assets in a format that allows for target identification. Shared data might be needed to enhance the accuracy of AI-enabled systems or to increase the effectiveness of multinational operations. For example, some member states may be better positioned than others to gather data on a shared rival, increasing the amount of data available to AI systems.[67]

Because of its central role in AI development and operations, the U.S. military has described data as a "strategic asset," yet sharing data — even within the U.S. military — has posed a significant challenge.[68] Lt. Gen. Jack Shanahan, founding director of the Department of Defense's Joint Artificial Intelligence Center, lamented that data "has stymied most of the [military] services when they dive into AI." Specifically, "they realize how hard it is to get the right data to the right place, get it cleaned up, and train algorithms on it."[69] There are two primary factors that underlie these challenges. First, data resides in thousands of different repositories and often lacks standardized formatting. Video from the U.S. military's fleet of reconnaissance aircraft, for instance, is stored on multiple separate networks and in different data formats. Second, significant amounts of data collected by weapons and sensor systems are considered proprietary by the contractors that design and maintain the equipment. Firms must first release or "unlock" this data before it can be analyzed or fed into other systems.[70]

Although shared data is needed to develop AI technologies that can integrate with allied equipment, states face both political and technical barriers to sharing security sector information. From a political standpoint, even the closest allies may be hesitant to share the sensitive data that undergirds military AI systems. States fear that sharing sensitive data might reveal intelligence sources and methods, the revelation of which could com-

[63] "Letter from Google Employees to Alphabet CEO Regarding Project Maven," April 2018, https://static01.nyt.com/files/2018/technology/googleletter.pdf.

[64] Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," *New York Times*, June 1, 2018, https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

[65] Larson et al., *Interoperability*, 18.

[66] This assumes that training data is accurate.

[67] Walsh, *The International Politics of Intelligence Sharing*, 7–8.

[68] *The United States Air Force Artificial Intelligence Annex to the Department of Defense Artificial Intelligence Strategy*, United States Air Force, 2019, https://www.af.mil/Portals/1/documents/5/USAF-AI-Annex-to-DoD-AI-Strategy.pdf.

[69] Sydney J. Freedberg, Jr., "Pentagon's AI Problem Is 'Dirty' Data: Lt. Gen. Shanahan," *Breaking Defense*, Nov. 13, 2019, https://breakingdefense.com/2019/11/exclusive-pentagons-ai-problem-is-dirty-data-lt-gen-shanahan/.

[70] Freedberg, "Pentagon's AI Problem Is 'Dirty' Data."

promise ongoing operations or strain political relationships. During the Vietnam War, for example, the United States was hesitant to share intelligence with its ally South Vietnam. Officials feared that communist sympathizers in the ranks of South Vietnam's military and intelligence services would pass information to North Vietnam and the Vietcong. They were also concerned that intelligence might highlight that the United States was planning operations that did not align with South Vietnam's government priorities.[71] States also worry that shared information could be used for purposes other than initially intended or in ways that are at odds with the sharing state's interests. Turkey, for instance, may have used intelligence shared as part of counter-Islamic State operations to instead target Kurdish forces in northern Syria.[72]

To minimize these perceived risks, states often impose restrictions on information sharing. One of the most common control measures is sharing only finished intelligence — products such as briefings or reports derived from a variety of different intelligence sources.[73] These products provide assessments, but generally omit technical data — like details about the information source — that could reveal intelligence-gathering procedures and methods. Although data sharing is a type of intelligence sharing, developing and operating AI-enabled systems may require the exchange of more complete raw data in far larger quantities than traditional intelligence sharing. Raw data, which includes imagery files and signals intercepts, can include metadata such as spectral signatures of imagery or characteristics of electronic emissions that can be used to feed AI systems.[74] Since this information can expose precise capabilities and shortcomings of a state's intelligence systems, decision-makers may be hesitant to share it — especially in the large quantities needed to develop and run many AI-enabled systems.

There are also technical obstacles to data sharing. Just as the U.S. intelligence community and military stores information in nonstandardized formats on multiple systems, so too do national security institutions in other allied states. Across an alliance, the same type of data might reside on hundreds of different networks and in different formats, making it difficult to share data or to develop interoperable systems. To use data from other alliance partners, data must first be located, transferred out of a state's classified computer network, and reformatted into a standardized, usable form. Given that the U.S. military has faced significant data management challenges in its own AI development, we should expect alliances — with their greater number of institutional actors and data sources — to encounter even greater obstacles to data sharing.

Vulnerabilities: AI and Data

In addition to barriers to sharing, allies face the possibility that the data that they do share may be especially vulnerable to adversary manipulation. Engineers and military leaders worry that rivals could hack into data repositories and "poison" data — inserting fake data or making existing data deliberately flawed.[75] In one recent academic study, researchers used data poisoning to cause an algorithm designed to identify street signs to misclassify stop signs as speed limit signs.[76] In the military domain, a rival could poison imagery data in order to throw off AI target recognition systems, leading the system to miss military targets, classify them as nonmilitary ones, or identify civilian infrastructure as military facilities. At best, this could require manpower-intensive efforts to secure and sanitize data or lead states to turn back to manual analysis of targets. At worst, this could lead to the inadvertent targeting of noncombatants.

While the risk of data poisoning plagues all AI users, alliance military operations may be particularly susceptible because data inputs from multiple states are used to train and operate AI-enabled systems across the alliance. Flawed data inputs from one state can therefore have cascading effects across an alliance's operations. Rivals will recognize that different members of an alliance defend their networks and data with different levels

[71] Walsh, *The International Politics of Intelligence Sharing*, 59–78.

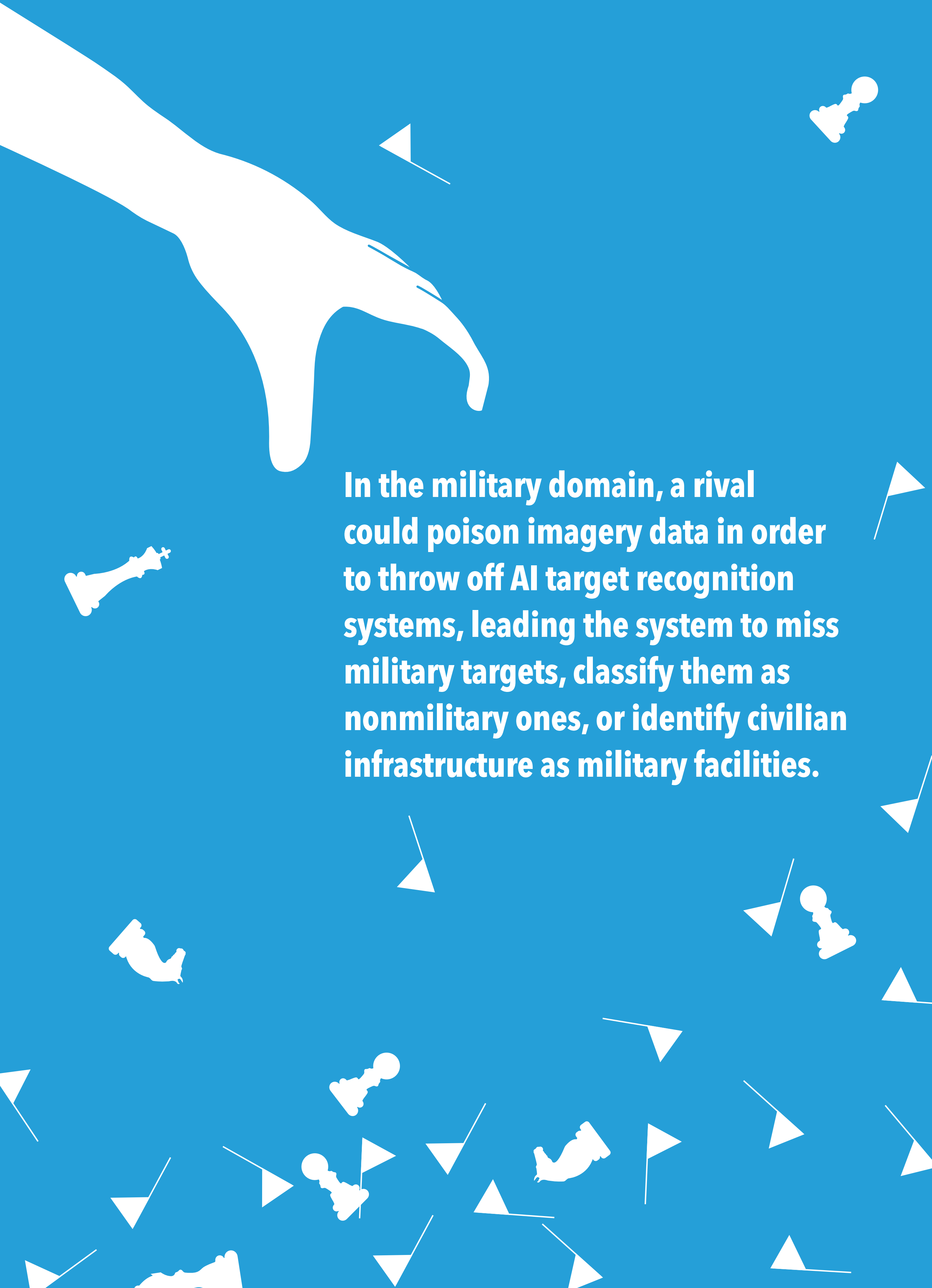
[72] Ben Hubbard and Carlotta Gall, "Turkey Launches Offensive Against U.S.-Backed Syrian Militia," *New York Times*, Oct. 9, 2019, https://www.nytimes.com/2019/10/09/world/middleeast/turkey-attacks-syria.html.

[73] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Thousand Oaks, CA: CQ Press, 2012), 74–75.

[74] D. L. Young, "Motion Imagery Metadata Standards Assist in Object and Activity Classification," in *2010 IEEE 39th Applied Imagery Pattern Recognition Workshop (AIPR)*, 2010, 1–4.

[75] David J. Miller, Zhen Xiang, and George Kesidis, "Adversarial Learning in Statistical Classification: A Comprehensive Review of Defenses Against Attacks," ArVix, Dec. 2, 2019, 3–4, https://arxiv.org/abs/1904.06292.

[76] Tianyu Gu et al., "BadNets: Evaluating Backdooring Attacks on Deep Neural Networks," *IEEE Access*, no. 7 (2019): 47230–44.



In the military domain, a rival could poison imagery data in order to throw off AI target recognition systems, leading the system to miss military targets, classify them as nonmilitary ones, or identify civilian infrastructure as military facilities.

of safeguards. As a result, rivals may target data stored by states where they have easier access.[77]

Adversaries can also use AI to launch deception campaigns designed to interfere with alliance military command and control. Militaries have long tried to deceive their adversaries during wartime and crises. During World War II, for instance, allied forces used a complex ruse involving imaginary armies equipped with inflatable tank and plane decoys to deceive Nazi planners about the location of the D-Day landings.[78] While states and other actors have a range of tools with which to carry out deception operations, AI allows them to launch deception campaigns using digital decoys and misinformation rather than physical ones.

One AI tool actors can use to complicate alliance operations are deepfakes, manipulated videos and audio that realistically mimic the behaviors or speech of an actual person. In 2018, for instance, the digital media outlet *Buzzfeed* produced a film in which a deepfake of former President Barack Obama appeared to utter obscenities and criticize Trump.[79] Deepfake creation relies on deep-learning algorithms that learn by observing photos, audio, and video of an individual to produce lifelike representations that can be programmed to say or do things that the actual person never did. Although early deepfakes were easily detectable to the naked eye, techniques such as generative adversarial networks have enhanced the quality and believability of deepfakes. This technique features two competing neural networks: a generator and a discriminator. The generator produces an initial deepfake, while the discriminator compares the AI-generated "fake" with genuine images from a training data set. The generator then updates the fakes until the discriminator can no longer distinguish the AI-generated image from the actual images.[80] As AI technology advances, rivals may be better able to use AI to carry out deception campaigns.

Deepfakes could be used in a variety of ways. An adversary might create deepfakes of senior alliance commanders to issue incorrect or contradictory orders to troops in the field, or use AI to produce fake intelligence reports.[81] A rival might use video or audio recordings of an actual commander obtained from public media reports or intercepted communications to generate deepfake commands. Or, they could use generative adversarial networks to create fake satellite intelligence imagery that misrepresents the ground truth.[82] Once transmitted via video teleconference, phone, email, or radio, these false commands and intelligence reports could cause troops to redeploy in a way that aids the rival or simply generates confusion. Nefarious actors have already successfully employed these types of ruses. In 2019, for example, criminals used AI to clone the voice of a British energy firm executive and directed a company employee to transfer hundreds of thousands of dollars into a bank account controlled by the criminals.[83] The software needed to carry out these efforts is easily available, demands little data for training, and increasingly requires minimal computer programming knowledge. Indeed, some voice cloning programs are available for free or at a low cost on the internet.[84]

Alliance military forces may be particularly vulnerable to AI-enabled misinformation and deception because multinational command-and-control processes involve coordination across multiple states.[85] Personnel may have limited previous experience working with international partners, and as a result, be unfamiliar with their ally's operating protocols and less adept at working within a multinational chain of command. Adversaries can exploit this unfamiliarity with coalition operations to inject

[77] Rivals often seek less secured sources of classified data. For instance, Chinese hackers routinely targeted U.S. defense contractors, which were perceived as less secure, in addition to military networks. See, Gordon Lubold and Dustin Volz, "Chinese Hackers Breach U.S. Navy Contractors," *Wall Street Journal*, December 14, 2018, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401.

[78] Joshua Levine, *Operation Fortitude: The Story of the Spies and the Spy Operation That Saved D-Day* (Guilford, CT: Lyons Press, 2011).

[79] David Mack, "This PSA About Fake News from Barack Obama Is Not What It Appears," *BuzzFeed News*, April 17, 2018, https://www.buzzfeednews.com/article/davidmack/obama-fake-news-jordan-peele-psa-video-buzzfeed.

[80] Martin Giles, "The GANfather: The Man Who's Given Machines the Gift of Imagination," *MIT Technology Review*, Feb. 21, 2018, https://www.technologyreview.com/s/610253/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/.

[81] The U.S. government considers "The transmission of false or misleading radio or telephone message [of] false orders purporting to have been issued by the enemy command" to be a legitimate ruse to degrade adversary operations. See, *Field Manual 3-13.4: Army Support to Military Deception*, U.S. Army, 2019, https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1006341, 2-18.

[82] In recent years, China has made significant advances in this type of AI application. See, Patrick Tucker, "The Newest AI-Enabled Weapon: 'Deep-Faking' Photos of the Earth," *Defense One*, March 31, 2019, https://www.defenseone.com/technology/2019/03/next-phase-ai-deep-faking-whole-world-and-china-ahead/155944/.

[83] Drew Harwell, "An Artificial-Intelligence First: Voice-Mimicking Software Reportedly Used in a Major Theft," *Washington Post*, Sept. 4, 2019, https://www.washingtonpost.com/technology/2019/09/04/an-artificial-intelligence-first-voice-mimicking-software-reportedly-used-major-theft/.

[84] Software like Lyrebird AI can create a digital voice using just a small audio sample.

[85] *Joint Publication 3-16: Multinational Operations*, chap. II.

AI-generated false commands. The time pressure, stressors, and complexity of military operations increase the likelihood that lower-level commanders will carry out these deepfake commands. These challenges will become more vexing as the quality of deepfakes increases and deciphering real from tampered content becomes more difficult.

Obstacles to Alliance Decision-Making

In addition to creating obstacles to the conduct of multinational military operations, AI can also strain the ability of alliance leaders to make decisions during a crisis. Alliance decision-making is often characterized as a contentious process in which policymakers from states with different national interests, military capabilities, and risk tolerances coordinate their preferences.[86] Policymakers seek to advance their state's own interests during deliberations, frequently leading to negotiated policy compromises. NATO allies, for instance, routinely have policy disagreements — take, for instance, clashes over the response to Egypt's nationalization of the Suez Canal in 1956 and over the 2003 U.S. invasion of Iraq.[87] Alliances and coalitions are also fraught with commitment problems, where states fear that allies will back out of agreements or drag them into unwanted conflicts.[88] Divergent national positions and fears of abandonment can lead decision-making consultations between states to be drawn out, and, if conducted in the midst of a crisis, leave alliances unable to respond decisively to threats.[89]

AI can complicate the coordination required for alliance decision-making and the subsequent ability to command and control multinational forces in three key ways. First, AI technologies promise to accelerate the speed of military operations, reducing the amount of time available for deliberations between states. Second, there are varying levels of uncertainty surrounding the reliability and effectiveness of AI technologies. If decision-makers from different states hold different degrees of trust in the ability of AI systems to provide accurate information or take appropriate actions, they may be hesitant to use these systems when making decisions on the use of force. Third, adversaries may use AI-enabled disinformation campaigns to degrade trust between allies and heighten fears that member states will renege on their alliance commitments.

Compressed Decision-Making Timelines

The proliferation of AI-enabled technologies among both friends and rivals will compress the time policymakers and military commanders have to deliberate over political and military decisions. In the hands of allies, AI-assisted intelligence, surveillance, and reconnaissance or command-and-control systems may identify adversary military maneuvers faster than non-AI systems. Once presented with this information, alliance decision-makers may need to quickly decide how to respond — particularly if adversary forces pose an immediate threat or must be targeted within a narrow window of opportunity.

The U.S. military has already started to develop this type of capability. As part of a series of exercises, the Defense Department demonstrated a command-and-control network that uses AI to automatically detect enemy activity and pass targeting information between multiple intelligence and military assets. During one of these exercises, a space asset detected a simulated enemy ship, but was unable to identify it. The network automatically cued an intelligence, surveillance, and reconnaissance platform to collect additional information on the adversary vessel, which it then sent to a command-and-control asset. The command-and-control platform used AI to select the best platform available to strike the enemy ship and passed targeting data to the nearby U.S. naval destroyer that would engage the adversary vessel. AI significantly shortened the targeting process relative to efforts without AI technology. When describing the AI-enabled network in November 2019, U.S. Air Force Chief of Staff Gen. David Goldfein announced, "This is no longer PowerPoint. It's real."[90]

At the strategic level, this type of AI-enabled command-and-control system could present decision-makers with intelligence that a rival is pre-

[86] Michelle L. Pryor et al., "The Multinational Interoperability Council: Enhancing Coalition Operations," *Joint Forces Quarterly*, no. 82 (July 2016), http://ndupress.ndu.edu/Media/News/News-Article-View/Article/793350/the-multinational-interoperability-council-enhancing-coalition-operations/.

[87] Philip Zelikow and Ernest R. May, *Suez Deconstructed: An Interactive Study in Crisis, War, and Peacemaking* (Washington, D.C.: Brookings Institution Press, 2018); Steven R. Weisman, "Threats and Responses: The Alliance; Fallout from Iraq Rift: NATO May Feel a Strain," *New York Times*, Feb. 11, 2003, https://www.nytimes.com/2003/02/11/world/threats-and-responses-the-alliance-fallout-from-iraq-rift-nato-may-feel-a-strain.html.

[88] Christensen and Snyder, "Chain Gangs and Passed Bucks."

[89] Paul B. Stares, *Command Performance: The Neglected Dimension of European Security* (Washington, D.C: Brookings Institution Press, 1991), 8–9.

[90] Valerie Insinna, "US Air Force Chief Calls on Gulf Nations to Resolve Political Tensions, Focus on Iran Threat," *Defense News*, Nov. 16, 2019, https://www.defensenews.com/digital-show-dailies/dubai-air-show/2019/11/16/us-air-force-chief-calls-on-gulf-nations-to-resolve-political-tensions-focus-on-iran-threat/.

paring to deploy strategic forces — like ballistic missile submarines or mobile missile launchers — from its garrisons during a crisis. In such a case, senior policymakers from various alliance member states might hold differing opinions on how best to respond, but would have little time to debate their options before the adversary's forces are dispersed and more difficult to locate.[91] Commanders at the operational and tactical levels of alliance operations will face similar challenges as AI-enabled systems more rapidly provide battlefield intelligence about rival forces. As a result, commanders may be forced to quickly decide whether to strike a fleeting target detected by an AI-enabled system. To be sure, decision-makers in unilateral operations will confront these same issues, but settling on the best course of action is more complex in settings where multiple actors have a say in the decision-making process.[92]

An adversary's use of AI-enabled systems can also compress timelines and complicate alliance decision-making. Just as AI can boost the tempo of allied operations, it can increase the frequency and speed of a rival's military actions. AI-enabled autonomous weapon systems that allow states to launch military operations without putting personnel in harm's way may lead rival leaders to launch operations that they might not otherwise carry out.[93] China, for instance, has developed and exported autonomous drones capable of identifying targets and carrying out lethal strikes with little or no human oversight.[94] Further, a rival's integration of AI into its command-and-control networks may speed its decision-making process. Indeed, China's military has expressed an interest in leveraging AI for military decision-making.[95] A publication from the Central Military Commission Joint Operations Command Center, for example, described how the use of AI to play the complex board game Go "demonstrated the enormous potential of artificial intelligence in combat command, program deduction, and decisionmaking."[96] These systems could be employed against the United States and its allies in the Indo-Pacific region, forcing allied commanders to respond more quickly to these threats.

Uncertainty Surrounding AI Technology

AI can also strain alliance decision-making by fueling uncertainty about information and military actions. Unlike human analysts or military personnel who can be asked to explain and justify their findings or decisions, AI generally operates in a "black box."[97] The neural networks that underpin many cutting-edge AI systems are opaque and offer little insight into how they arrive at their conclusions.[98] These networks rely on deep learning, a process that passes information from large data sets through a hierarchy of digital nodes that analyze data inputs and make predictions using mathematical rules. As data flows through the neural network, the net makes internal adjustments to refine the quality of outputs. Researchers are often unable to explain how neural nets make these internal adjustments. Because of this lack of "explainability," users of AI systems may have difficulty understanding failures and correcting errors.[99]

Policymakers have called for the development of more transparent AI systems, and researchers

[91] For divergent viewpoints on the challenge of finding mobile targets see, Michael S. Gerson, "No First Use: The Next Step for U.S. Nuclear Policy," *International Security* 35, no. 2 (Fall 2010): 26–27, https://doi.org/10.1162/ISEC_a_00018; Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, no. 1–2 (2015): 38–73, https://doi.org/10.1080/01402390.2014.958150.

[92] Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge, MA: Harvard University Press, 1971), 53–65.

[93] Scholars have argued that technologies that reduce risk to friendly forces create a moral hazard where leaders deploy military forces on missions where they would otherwise not use force. See, Kaag and Kreps, *Drone Warfare*.

[94] Patrick Tucker, "SecDef: China Is Exporting Killer Robots to the Mideast," *Defense One*, Nov. 5, 2019, https://www.defenseone.com/technology/2019/11/secdef-china-exporting-killer-robots-mideast/161100/.

[95] Elsa B. Kania, "Chinese Military Innovation in the AI Revolution," *The RUSI Journal* 164, no. 5–6 (2019): 26–34, https://doi.org/10.1080/03071847.2019.1693803.

[96] Gregory C. Allen, "Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security," Center for a New American Security, Feb. 2019, 6.

[97] Ariel Bleicher, "Demystifying the Black Box that Is AI," *Scientific American*, Aug. 9, 2017, https://www.scientificamerican.com/article/demystifying-the-black-box-that-is-ai/.

[98] Paul Scharre, *Autonomous Weapons and Operational Risk*, Center for New American Security, February 2016, 14–17, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf?mtime=20160906080515; Paul Scharre, *Artificial Intelligence and National Security* (Washington, D.C.: Congressional Research Service, 2019), 29–32.

[99] David Gunning, "Explainable Artificial Intelligence (XAI)," Presentation at Proposers Day, DARPA, Aug. 11, 2016, https://www.darpa.mil/attachments/XAIIndustryDay_Final.pptx.

are working to develop explainable AI tools that peer inside the AI black box.[100] Yet, many decision-makers remain uncomfortable with the uncertainty surrounding AI-enabled systems. The commander of the U.S. Air Force's Air Combat Command, for instance, publicly explained that he was not yet willing to rely on AI programs to analyze the full-motion video collected by reconnaissance drones. He argued that although systems are improving, they are still unable to consistently provide accurate analysis.[101] So long as the decisions and analysis of AI systems remain opaque, military commanders may be reluctant to trust AI-enabled systems. And if used, AI may contribute to the fog of war, rather than reduce it, making it difficult to make decisions using information delivered by AI technologies.

The operational implications associated with uncertainty and lack of trust in AI would likely be exacerbated in multinational alliance contexts. There is significant cross-national variation in trust in AI technologies, even among close allies. One 2018 survey, for instance, found that just 13 percent of respondents in Japan and 17 percent of respondents in South Korea trust artificial intelligence, compared to 25 percent of respondents in the United States. Similar disparities exist between the United States and many of its NATO allies. In Spain, 34 percent of respondents trust artificial intelligence, compared to 21 percent in Canada, 40 percent in Poland, and 43 percent in Turkey.[102] Given this variation, policymakers and commanders from some states may be more reluctant to use AI-enabled systems or trust the information they deliver than leaders from other states during multinational operations.

Allied decision-makers will also face uncertainty when confronting a rival's use of AI-enabled technologies. Leaders will be forced to wrestle with whether to respond to actions carried out by AI-enabled systems — like autonomous aircraft or ships — in the same way as actions carried out by traditionally manned assets. Existing doctrine and law are generally silent on these issues, providing no guidance on the appropriate response. States have drafted domestic policies to govern their own use of autonomous weapon systems, but these regulations and international law make no distinction between how states should react to a rival's AI-enabled military actions versus "traditional" military actions.[103] Yet, decision-makers may believe that a rival's use of AI technologies demands different responses than those involving manned platforms.[104] What happens if a rival claims that an attack carried out by an AI-enabled system was the result of a flawed algorithm? Should air defense forces respond differently to an adversary's autonomous drones that penetrate friendly airspace than to a manned aircraft that does the same? Decision-makers may find themselves with little time to consider these complicated issues, particularly as AI technology accelerates the speed of a rival's military operations.

Adversary Manipulation and Interference

Even if states were to trust their own AI technologies, rivals and malicious actors can use AI to sow discord that can hamper decision-making. Trust and close relationships are crucial when multiple states coordinate security-related decisions since policymakers must be confident that allies will not renege on commitments. Leaders have long held fears of being abandoned by allies or of being drawn into unwanted conflicts.[105] These fears are magnified when leaders suggest they might not follow through with their alliance commitments or engage in provocative actions.[106] Trump, for instance, raised questions about Washington's commitment to its allies when he

[100] DARPA, for instance, has launched a program to develop AI that allows for greater transparency and interpretability. Gunning, "Explainable Artificial Intelligence (XAI)"; "AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense (Washington, D.C.: Defense Innovation Board, 2019)," 9, https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

[101] Clark, "Air Combat Commander Doesn't Trust Project Maven's Artificial Intelligence — Yet."

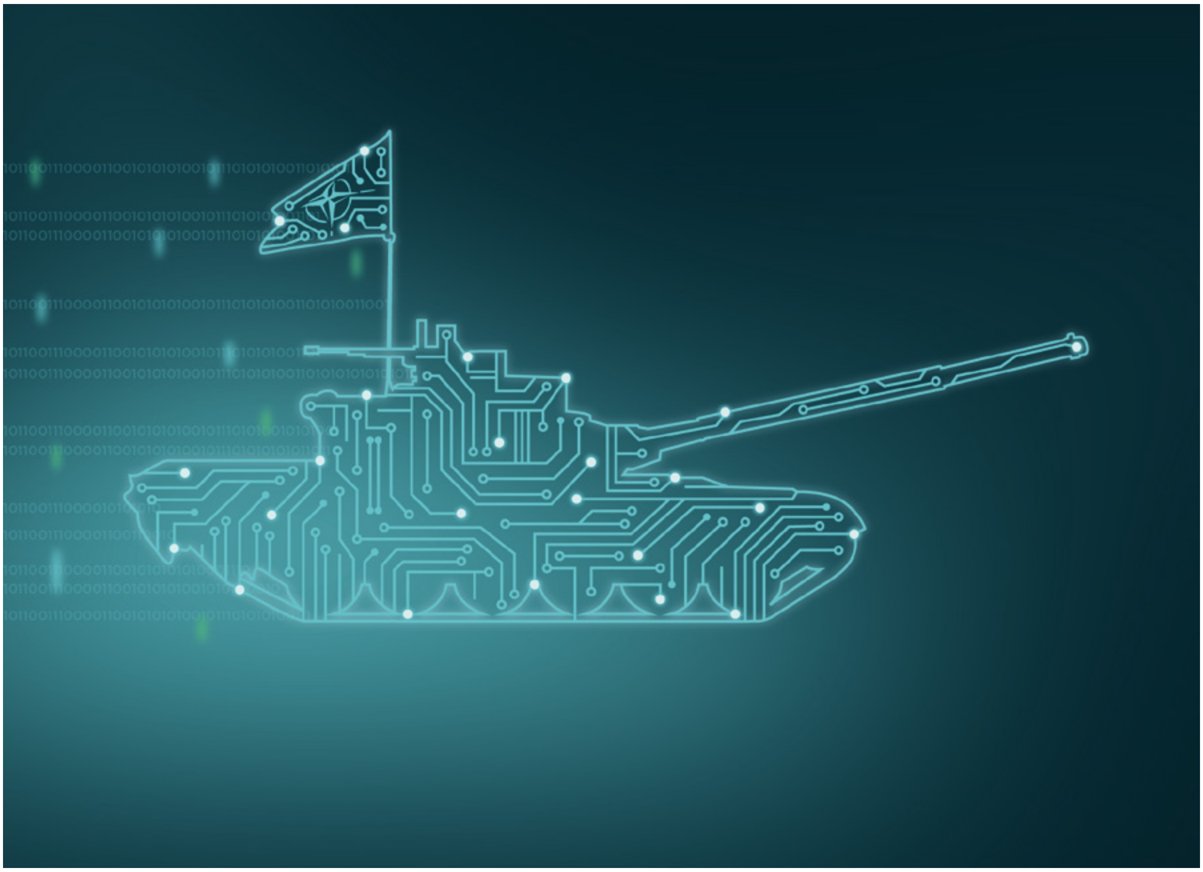
[102] "Entrepreneurialism: The Emergence of Social Entrepreneurialism to Compete with Business Entrepreneurialism," Ipsos Global Affairs, November 2018, 40, https://www.ipsos.com/sites/default/files/ct/news/documents/2018-10/entrepreneurialism-2018-global-report.pdf. Respondents were asked whether they "agree," are "neutral", or "disagree" with the statement, "I trust artificial intelligence."

[103] "Department of Defense Directive 3000.09: Autonomy in Weapon Systems," Department of Defense, Nov. 21, 2012, https://www.hsdl.org/?view&did=726163.

[104] Trump, for instance, argued that the downing of an unmanned drone demanded a different response than the downing of a manned aircraft. See, Michael D. Shear et al., "Strikes on Iran Approved by Trump, then Abruptly Pulled Back," *New York Times*, June 20, 2019, https://www.nytimes.com/2019/06/20/world/middleeast/iran-us-drone.html; For a more generalized study on escalation in response to activity by and involving unmanned platforms, see, Erik Lin-Greenberg, "(War)Game of Drones: Remote Warfighting Technology and Escalation Control (Evidence from Wargames)," SSRN Scholarly Paper, June 25, 2019, https://dx.doi.org/10.2139/ssrn.3288988.

[105] Christensen and Snyder, "Chain Gangs and Passed Bucks." One study shows that states fail to fulfill alliance commitments, on average, 50 percent of the time; Berkemeier and Fuhrmann, "Reassessing the Fulfillment of Alliance Commitments in War."

[106] Julian E. Barnes and Helene Cooper, "Trump Discussed Pulling U.S. from NATO, Aides Say Amid New Concerns Over Russia," *New York Times*, Jan. 14, 2019, https://www.nytimes.com/2019/01/14/us/politics/nato-president-trump.html.



publicly questioned the value of defending certain NATO member states.[107] An adversary could use AI to drive misinformation campaigns that latch onto these concerns in an effort to strain ties or deepen cleavages between allies.

Just as adversaries can use deepfakes to interfere with operational-level coordination, they can also use AI technologies to breed confusion and mistrust that hamper strategic decision-making. Actors seeking to disrupt alliance cohesion might create deepfakes depicting leaders of alliance member states questioning the value of an alliance, criticizing other leaders, or threatening to take actions that could draw an alliance into an unwanted conflict. These falsified videos or recordings could boost uncertainty of an ally's commitments or induce panic over fears of abandonment during a crisis. The decision-making process may be slowed as policymakers try to understand their allies' true intentions and preferences, or convince domestic publics that an ally's "statements" are in fact AI-produced misinformation.

The Way Forward

Although the proliferation of military AI technology has the potential to frustrate alliance military operations and decision-making, these obstacles are not insurmountable. Allies have previously worked together on missions that involved new technology, shared highly sensitive information, and learned to cope with compressed decision-making timelines. Drawing lessons from historical exemplar cases where allies have wrestled with new technology, coupled with guidance from emerging national AI policies and analysis of new technologies, I identify ways that alliances can overcome the pitfalls of AI integration in an environment in which AI is increasingly common.

Increasing AI Interoperability and Data Sharing

To ensure alliances and coalitions are able to leverage AI technologies during their operations, states will need to remove barriers to data sharing and access. One initial step to enabling this type of interoperability is to establish formal

[107] Eileen Sullivan, "Trump Questions the Core of NATO: Mutual Defense, Including Montenegro," *New York Times*, July 18, 2018, https://www.nytimes.com/2018/07/18/world/europe/trump-nato-self-defense-montenegro.html.

agreements that govern the development and use of AI-enabled technologies and associated data. These formal agreements will not only prescribe procedures for collaboration, but help assuage fears that allies will renege on commitments.[108] Agreements that explicitly define the responsibilities and expectations of member states help eliminate vagaries that otherwise allow a state to back out of commitments with partners.[109]

To integrate AI into alliance operations, policymakers will need to first establish how they will jointly develop and employ AI capabilities. This entails identifying the types of operations in which allies are willing to use AI-enabled technologies. Some states may only be willing to employ AI military systems in limited areas and eschew using AI for certain tasks. The U.S.-Singapore agreement, for example, stipulates that the two states will focus their AI efforts on humanitarian assistance and disaster relief operations.[110] More narrowly scoped agreements that focus on noncombat operations may prove more palatable to policymakers and their domestic publics. These narrow agreements could serve as useful first steps to collaboration, but still yield lessons and best practices applicable across the full range of military operations.

Developing data-sharing policies and technical standards may be difficult given the sensitive nature of national security information and the variation in technical standards across alliance member states. Allies, however, have found ways to coordinate cooperation, even in sensitive areas. The United States and its Five Eyes partners — the United Kingdom, Canada, Australia, and New Zealand — have long maintained agreements that govern intelligence collaboration. The 1946 United Kingdom-United States Agreement, for example, established formal rules for sharing signals intelligence — intercepted electronic emissions and communications.[111] The agreement spelled out how the states would cooperate on the collection, analysis, and dissemination of signals intelligence, while a technical appendix provided detailed technical and procedural guidance on communications intercept equipment and decryption and translation processes.[112] Specifically, the agreement called on states to "make available to the other [states] continuously, currently, and without request, all raw traffic, [communications intelligence] end-product and technical material acquired or produced."[113] Some existing intelligence sharing agreements might allow for the exchange of the sensitive data needed to train and operate AI systems. When existing agreements are not in place or do not cover the types of data required for AI-enabled warfare, policymakers will need to develop new bilateral or multilateral agreements that enable interoperability and data sharing. These agreements and the procedures used to implement them will likely vary depending on the states involved and the degree and purpose of cooperation. In some cases, cooperation may be narrowly scoped to limited data sharing in support of a specific operation. In other cases, agreements may be far broader and cover issues related to research and development, interoperability, and extensive data sharing.

Even when formalized agreements establish the processes and institutions that enable AI cooperation between states, many leaders may remain hesitant to share the sensitive data that underpins AI development and operations. Information-sharing arrangements are plagued by commitment problems as states can back out of their agreements to exchange data if they fear that data will be leaked or their capabilities and shortcomings will be revealed.[114] This might be particularly true in ad hoc coalitions or larger alliances, where relationships between member states may be weaker. Recent technological advances, however, may help overcome these commitment problems by convincing member states that their data will remain secure even when shared.

In particular, developments in the field of cryptology allow states to share data with partners for use in AI systems, while hiding the exact content of input data. Secure multiparty computation, for example, is a privacy-preserving technique in which AI algorithms perform their computations using an

[108] Morrow, "Alliances: Why Write Them Down?"

[109] On the importance of explicit commitments, see, Snyder, *Alliance Politics*.

[110] Parameswaran, "What's in the New US-Singapore Artificial Intelligence Defense Partnership?"

[111] For a description of the agreement and a collection of declassified documents about the agreement, see, "Declassified Documents: UKUSA Agreement Release 1940-1956," National Security Agency, accessed Dec. 8, 2019, https://www.nsa.gov/news-features/declassified-documents/ukusa/.

[112] "British-U.S. Communication Intelligence Agreement (Previously Classified Top Secret)," March 5, 1946, retrieved from the U.S. National Security Administration, https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/ukusa/agreement_outline_5mar46.pdf.

[113] "British-U.S. Communication Intelligence Agreement (Previously Classified Top Secret)," appendix C.

[114] Walsh, *The International Politics of Intelligence Sharing*, 9–11.

input that remains secret, but provide an output that is public to all authorized users.[115] Secure multiparty computation has been increasingly used in the medical and financial sectors where analysts seek to assess trends but need to protect individual-level health and fiscal data to avoid violating privacy regulations.[116] This and other privacy preserving approaches could be applied to a range of AI-enabled alliance military tasks, such as the classification of objects in satellite and reconnaissance imagery. Member states might feed sensitive intelligence data into a secure multiparty computation-based system managed by an alliance's intelligence fusion center, which would then return information about potential targets, without revealing attributes about each state's intelligence inputs.

To successfully integrate AI and share data, however, partners will also need to establish technical standards to ensure data is stored and formatted in ways that make it easily accessible to and usable by various alliance members. In designing these agreements, alliance policymakers might draw insights from existing state-level AI guidelines and alliance standardization protocols. The U.S. National Institute for Standards and Technology, for example, released its AI standards in February 2019. The guidance calls for defining data specifications that ensure AI technologies meet "critical objectives for functionality, interoperability, and trustworthiness."[117] In the alliance military context, this might mean ensuring that data associated with geospatial or signals intelligence are formatted and labeled in a common manner and stored on shared alliance networks. Or, it could mean establishing alliance-wide protocols for data security and integrity to minimize the risks of data poisoning. These specifications could be codified in formal arrangements like NATO's standardization agreements, which provide standards for thousands of systems and processes ranging from aerial refueling equipment to satellite imagery products.[118] These standards ensure "doctrine, tactics, and techniques are developed in harmony" to help allies "operate effectively together while optimizing the use of resources."[119]

Even when formalized agreements establish the processes and institutions that enable AI cooperation between states, many leaders may remain hesitant to share the sensitive data that underpins AI development and operations.

Streamlining Decision-Making and Command and Control

AI is not the first military development to reduce the amount of time alliance leaders have for crisis decision-making. Warsaw Pact military modernization in the 1970s, for instance, led NATO to reevaluate the amount of warning it would have in advance of an invasion of Western Europe. Prior to 1978, analysts estimated that the Soviets and their allies needed 30 days to prepare for an attack, giving alliance leaders a week to decide on response options. The expansion of Warsaw Pact offensive military capabilities reduced the preparation timeline to 14 days, slashing the window for NATO deliberation to just four days.[120] To mitigate the risks of protracted decision-making timelines, NATO took several steps to improve its ability to rapidly react. Specifically, senior NATO military commanders were given greater authority to order defensive measures in time-sensitive circumstances that precluded political authorization. The alliance also revamped and streamlined communications systems and procedures that facilitated alliance consulta-

[115] Andrew C. Yao, "Protocols for Secure Computations," in *SFCS: '82: Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, November 1982, 160–64.

[116] Dan Bogdanov, Riivo Talviste, and Jan Willemson, "Deploying Secure Multi-Party Computation for Financial Data Analysis," Working Paper, 2011, http://eprint.iacr.org/2011/662; Mbarek Marwan, Ali Kartit, and Hassan Ouahmane, "Applying Secure Multi-Party Computation to Improve Collaboration in Healthcare Cloud," *2016 Third International Conference on Systems of Collaboration (SysCo)*, 2016, 1–6.

[117] *U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*, National Institute of Standards and Technology, Aug. 9, 2019, 8, https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

[118] "Standardization Agreement 3971: Air-to-Air Refuelling," NATO Standardization Office, April 26, 2019; "Standardization Agreement 2586: NATO Geospatial Metadata Profile" NATO Standardization Office, Feb. 25, 2019). A complete list of standardization agreements is available at: https://nso.nato.int/nso/nsdd/listpromulg.html.

[119] Cihangir Aksit, "Smart Standarization: A Historical and Contemporary Success at NATO," NATO Standardization Agency, May 2014, 1, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_05/20140528_140528-smart-standardization.pdf.

[120] Stares, *Command Performance*, 9–10.

tions and engaged in additional exercises focused on military alerts and mobilizations.[121]

More recently, NATO's development of an alliance ballistic missile defense capability again raised the prospect that military commanders might be forced to make decisions on the use of force — albeit in a defensive manner — without time for political deliberations. In the event a rival were to fire missiles at Europe, intercept timelines would not allow for political consultation.[122] To prepare for the potentiality of defending Europe from missile attack, NATO considered pre-delegating launch authority to lower-level commanders.[123] Under specific rules of engagement, NATO commanders would be authorized to make decisions on the targeting of inbound missiles without waiting for approval from higher headquarters. These guidelines would ensure the alliance would be able to defend itself even if there was insufficient time for more senior commanders and policymakers to debate policy choices.

Just as pre-delegation of authorities to lower-level commanders helped NATO streamline crisis decision-making in the past, it may also help alliance decision-makers respond to "machine speed" operations that leave insufficient time for deliberation.[124] Military commanders need guidelines for how to respond to an adversary's AI-enabled actions and for how to employ information provided by friendly AI systems. As states increasingly deploy autonomous weapon systems that incorporate AI technologies, military commanders also need to know whether to react differently to a rival's operations that are carried out using traditional platforms than to those conducted using AI-enabled systems. More importantly, they need the authority to make these decisions without real-time direction from superiors. While pre-delegation may increase the ability of decision-makers to respond quickly, it has its downsides. Junior commanders may inadvertently use force in ways not desired by alliance policymakers, or increase the opportunities for rivals to launch AI-enabled deception campaigns.

In addition to streamlining decision-making processes, it is crucial that alliance leaders find ways to mitigate the risks that AI-enabled misinformation or deception campaigns pose to alliance solidarity and military command and control. The development of strategic communication strategies helps counter misinformation, and technical and procedural updates can harden command-and-control processes against AI-enabled interference. NATO has already taken steps in this direction, establishing a Strategic Communications Center of Excellence that supports the development of best practices to minimize the effects of disinformation.[125] Among the center's priorities is boosting resilience to misinformation campaigns by raising awareness about the ways that rivals might disseminate fake information.[126] These efforts can be bolstered by leveraging technological advances like deepfake detection software that quickly identifies falsified information.[127] Alliances and coalitions could also create agencies charged with detecting deepfakes that threaten alliance cohesion or military operations and then informing the public or military units about these falsified videos, recordings, and images. Creating these organizations, however, requires manpower and funding that allies may be unwilling to contribute.

A Path Forward for Alliance AI Integration

In recent years, alliances have successfully relied on a mix of formal agreements and technical measures — like those described above — to streamline interoperability and decision-making. For example, NATO established the Afghan Mission Network, a computer system that enabled participants in the NATO-led International Stabilization and Assistance Force to communicate and exchange battlefield information. At its height, this force included personnel from more than three dozen states working to train Afghan security forces, rebuild Afghan

[121] Stares, *Command Performance*, 10; Richard K. Betts, *Surprise Attack: Lessons for Defense Planning* (Washington, D.C.: Brookings Institution Press, 1982), 222–23.

[122] Stephan Frühling and Svenja Sinjen, "Missile Defense: Challenges and Opportunities for NATO," *NATO Defense College Research Paper*, no. 60 (June 2010), https://www.files.ethz.ch/isn/120605/rp_60.pdf.

[123] In 2010, the Group of Experts on a New Strategic Concept for NATO recommended this type of delegation in the event of a missile or cyber attack. See, "NATO 2020: Assured Security; Dynamic Engagement," NATO, May 17, 2010, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf.

[124] Former U.S. Deputy Secretary of Defense Bob Work used the term "machine speed" to describe the acceleration of operations carried out by AI systems. See, Bob Work, "Remarks to the Association of the U.S. Army Annual Convention," U.S. Department of Defense, Oct. 4, 2016, https://www.defense.gov/Newsroom/Speeches/Speech/Article/974075/remarks-to-the-association-of-the-us-army-annual-convention/.

[125] "About Us," NATO Strategic Communications Centre of Excellence, accessed Feb. 20, 2020, https://www.stratcomcoe.org/about-us.

[126] "NATO Takes Aim At Disinformation Campaigns," *NPR Morning Edition*, May 10, 2017, https://www.npr.org/2017/05/10/527720078/na-to-takes-aim-at-disinformation-campaigns.

[127] "Semantic Forensics (SemaFor) Proposers Day," Defense Advanced Research Projects Agency, accessed Aug. 28, 2019, https://www.darpa.mil/news-events/semantic-forensics-proposers-day.

government institutions, and conduct counter-insurgency operations. The computer networks of each of these member states were initially isolated and generally unable to communicate with those of other states. As a result, there was no common operating picture for critical warfighting functions such as intelligence, surveillance, and reconnaissance or coordinating artillery strikes.[128] These insulated networks slowed decision-making and command and control and complicated battlefield coordination because information could not easily be transmitted up and down the chain of command. To allow the International Stabilization and Assistance Force to exchange information from the headquarters to the tactical level, NATO planners drafted intelligence sharing agreements and built the Afghan Mission Network.[129]

To be sure, establishing a shared computer network is a far different task from developing interoperable, AI-enabled military capabilities. The Afghan Mission Network, however, demonstrates that a combination of policy and technical fixes can help members of a large, multinational coalition remove barriers to decision-making and operations and enable interoperability and the sharing of sensitive data. Indeed, the Afghan Mission Network was so successful that NATO used it as a foundation for its Federated Mission Network, which helps ensure connectivity and information sharing between NATO members outside the Afghan theater.[130]

The institutional changes described above will take time to implement fully and requirements will evolve as AI technology matures. There are several steps policymakers can take to ensure alliances remain sufficiently flexible and postured to integrate the latest advances in military AI technology. First, alliance member states can work to develop a corps of subject-matter experts with deep technical knowledge about AI and AI-enabled operations. These experts, who gain expertise through graduate education programs or fellowships in the private sector, could staff alliance-run AI centers of excellence, AI development labs, and working groups. Using their knowledge, they would identify where and how AI can best contribute to alliance operations from the tactical through strategic levels and help update alliance doctrine and policies as AI technology evolves. Individual states have already taken some of these steps. The U.S. Department of Defense activated its Joint AI Center in 2018 and, in 2019, the U.S. Air Force and the Massachusetts Institute of Technology launched a jointly staffed organization to develop AI algorithms and systems for military applications.[131]

Second, incorporating AI-enabled capabilities into alliance planning exercises and wargames will help prepare policymakers and commanders to better employ AI.[132] Wargames, for instance, might ask leaders to employ AI-enabled capabilities or respond to a rival's use of AI-enabled weapons. These events allow leaders to test and refine institutional processes in a low-risk environment, while also socializing practitioners to the potential uses, limitations, and risks of AI-enabled warfare.

Conclusion

As additional funding and research drive increases in the effectiveness and reliability of AI, the military use of AI technologies will likely expand. And as more states integrate AI into their armed forces, the United States will find itself working with allies to build and exercise AI capabilities that are interoperable and support alliance decision-making processes. Failure to cooperate early and often on the development and use of AI may leave allies ill-prepared for operations in an era in which AI is an increasingly common fixture in the arsenals of both friends and foes.[133]

Alliances face two broad sets of challenges when integrating AI into operations. First, AI complicates alliance operations. The resource and data requirements needed to build and maintain AI systems pose obstacles to burden-sharing and interoperability. Adversaries can also use AI to launch military deception campaigns that complicate operational coordination. Second, AI can significantly strain alliance decision-making. New AI technologies promise to increase the speed with which allies

[128] Barry Rosenberg, "Battlefield Network Connects Allied Forces in Afghanistan," Sept. 14, 2010, *Defense Systems*, https://defensesystems.com/articles/2010/09/02/c4isr-2-afghan-mission-network-connects-allies.aspx.

[129] Chad C. Serena et al., *Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network* (Washington, D.C.: RAND Corp., 2014), 3–7, https://www.rand.org/pubs/research_reports/RR302.html.

[130] "Federated Mission Networking," NATO Allied Command Transformation, accessed Feb. 20, 2020, https://www.act.nato.int/activities/fmn.

[131] Rob Matheson, "MIT and U.S. Air Force Sign Agreement to Launch AI Accelerator," *MIT News*, May 20, 2019, http://news.mit.edu/2019/mit-and-us-air-force-sign-agreement-new-ai-accelerator-0520.

[132] For an example of how NATO is integrating AI into exercises, see, Patrick Tucker, "How NATO's Transformation Chief Is Pushing the Alliance to Keep Up in AI," *Defense One*, May 18, 2018, https://www.defenseone.com/technology/2018/05/how-natos-transformation-chief-pushing-alliance-keep-ai/148301/.

[133] "Interim Report," 45.

and adversaries conduct operations, decreasing the time partners have to debate potential courses of action. Decision-making can also be disrupted if adversaries use AI to generate misinformation that can degrade trust among allies. To overcome these challenges, allies will need to establish multinational agreements and standardization guidelines that help ensure data is structured in ways that promote interoperability, while technical measures will help preserve data privacy, allow for data sharing, and minimize the consequences of AI use on the part of adversaries.

Whether and how states grapple with these challenges will shape the conduct of multinational operations and has implications for alliance politics and the global balance of power. Alliances that effectively integrate AI technology will be better positioned to counter threats, while those that allow AI to stymie decision-making and operations may find themselves disadvantaged on the battlefield. Within alliances, member states that quickly master the integration of AI into their militaries may gain significant influence, even if they are less powerful than other alliance partners in conventional terms. Because of their AI know-how, these states may play a dominant role in developing the norms, standards, and doctrine for AI use and help set an alliance's AI strategy. In a similar vein, Estonia leveraged its cyber warfare expertise to bolster its position in NATO. Despite being territorially small and weak in conventional military terms, Estonia's specialized expertise allowed it to play a leading role in shaping NATO's cyber doctrine.[134] A state's successful development of AI can therefore increase its voice and sway within complex multinational institutions.

This article represents a first step in understanding how the burgeoning development of AI technologies will affect alliances, and offers a framework for future hypothesis testing. Future work might more systematically explore the ways in which AI-enabled systems influence multinational military decision-making and operations. For instance, do national security decision-makers trust information provided by AI technologies more or less than information delivered by non-AI enabled sources? Under what conditions are decision-makers more or less likely to believe this information? Are military leaders from certain states more willing than those from other states to rely on AI technologies? If so, what drives this variation? Scholars might also try to identify the types of technical or institutional solutions that best promote AI interoperability. Do alliance decision-makers see formal agreements or technical solutions as a more effective means of ensuring data sharing? Scholars can explore these questions using a variety of methodological approaches including experimental research involving alliance decision-makers or in-depth case studies informed by interviews of senior policymakers.

Researchers might also consider the effects of AI on alliances in areas beyond decision-making and interoperability. For example, how does the use of AI affect strategic stability, nuclear deterrence, and alliance reassurance? Does the increased tempo of AI-enabled warfare make it harder or easier for states to deter rivals and reassure allies? Studies that address these questions would not only expand our scholarly understanding of the relationship between emerging technology and international security, but would help policymakers design better processes and institutions for a security environment in which AI use is becoming widespread.

As AI becomes increasingly common in military arsenals around the world, it is crucial for states to understand the potential challenges AI poses to multinational operations and work to overcome them. To prepare for warfare at machine speed, alliances should develop policies and practices that streamline data sharing and decision-making, and take procedural and technical measures to bolster their defenses against AI-equipped rivals.

Erik Lin-Greenberg *is a postdoctoral fellow at the University of Pennsylvania's Perry World House.*

Acknowledgements*: I am grateful to Jonathan Chu, Theo Milonopoulos, Michael Horowitz, Jordan Sorensen, Alexander Vershbow, participants at 2019 Perry World House Global Order Colloquium, and the anonymous reviewers for comments on earlier drafts.*

Photo: Staff Sgt. Jacob Osborne

[134] Josh Gold, "How Estonia Uses Cybersecurity to Strengthen Its Position in NATO," International Centre for Defense and Security, May 27, 2019, https://icds.ee/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/. Estonia now hosts NATO's Cooperative Cyber Defense Center of Excellence.