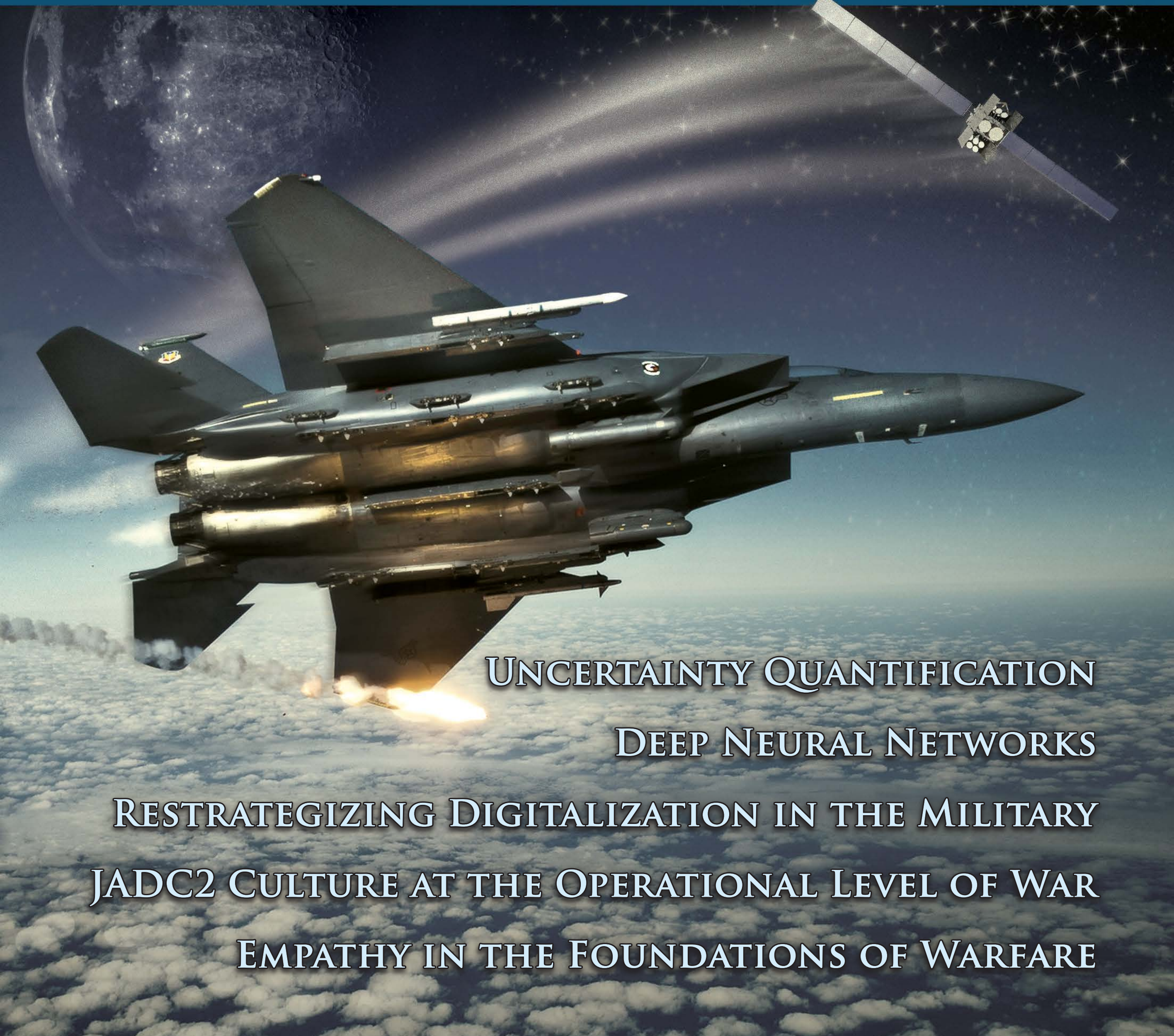
Department of the Air Force

ASOR

Air & Space Operations Review



Uncertainty Quantification

Deep Neural Networks

Restrategizing Digitalization in the Military

JADC2 Culture at the Operational Level of War

Empathy in the Foundations of Warfare

Vol. 2, No. 1 - Spring 2023

DEPARTMENT OF THE AIR FORCE

ASOR

AIR & SPACE OPERATIONS REVIEW

https://www.af.mil/

UNITED STATES SPACE FORCE
https://www.spaceforce.mil/

https://www.aetc.af.mil/

https://www.airuniversity.af.edu/

Air & Space Operations Review

SPRING 2023 VOL. 2, NO. 1

LETTER FROM THE EDITOR

Dear Reader,

Over the past six months, the world has witnessed a profusion of announcements of advances in artificial intelligence by leading global technology firms. The propagation of generative artificial intelligence in the form of chatbots, video, and graphics is another example of the speed with which our national security systems must adapt and change to realities posed by technology and innovation. But to be effective and meaningful, implementing such rapid change demands a close examination of existing processes and organizational cultures to determine what is best retained and what must evolve. Without such examination, we run the risk of embarking on transformation that ignores long-standing lessons learned, leading to the repetition of past mistakes. Above all, technological advances in warfare may even more urgently require that warfighters, serving alone or as humans-in-the-loop of a technological partner, further develop their human capabilities such as empathy and retain key elements of human autonomy in the battlespace.

The first forum in our Spring issue, Artificial Intelligence, Machine Learning, and Digitalization in the Military, leads with an article by Ayla Reed. She argues that quantifying uncertainty in artificial intelligence and machine learning through a process of metadata tagging, bound by military standards, will enable a practical digital implementation of Boyd's OODA loop that also addresses the ethical dilemmas posed by their use. In the second article, Robert Newton and Robert Masaitis present their findings from a study using a deep neural network to improve the efficiency of Air Force Special Operations Command screening and selection boards, creating time for more effective collective consideration of candidates. The forum concludes with an article by Paul van Fenema and Pieter Soldaat. They consider the impacts of digital innovation on the battlefield and propose a reframing of the approach to such technological investments to improve human-machine processes and practices across the boundaries of permissive and nonpermissive environments.

In our second forum, Elements of Future Warfare, Thomas Cantrell examines Joint all-domain command and control from a pyramid framework in which technology and command and control are supported by a foundational cultural layer. For this initiative to be successful, the Air Force must can transform this layer now, focusing on domains, partners, the kill web, and connectivity. Jennifer Rudolph concludes this forum and the issue with findings and recommendations from an Air National Guard study on empathy. The Department of the Air Force can help Airmen prepare for the demands of future warfare by incorporating the skill of empathetic communication into officer and enlisted training programs at multiple levels throughout the service.

Thank you for taking the time to read through our Spring 2023 issue.

~The Editor

Uncertainty Quantification

Artificial Intelligence and Machine Learning in Military Systems

Ayla R. Reed

Instituting a military standard for quantified uncertainty metadata represents a solution to the problems inherent in using artificial intelligence/machine learning (AI/ML) for military advantage. By provisioning for metadata now, the Department of Defense can continue to determine the best policy for using AI/ML in parallel with capability development. This coordination will prevent delays in solving difficult technical problems associated with implementing AI/ML in warfighting systems. Uncertainty quantification can enable a practical digital implementation of the observe, orient, decide, and act loop, addressing ethical issues with employing AI/ML in war and optimizing investment in research and development.

Foundationally, the US military does not need artificial intelligence/machine learning (AI/ML). Yet the military needs to be able to observe, orient, decide, and act (OODA) faster—and better—than an adversary to achieve military advantage.[1] Machines have the capacity to observe, orient, decide, and act at a faster pace than humans and thus enable this advantage. The debate remains open, however, on the appropriateness of allowing AI or ML models to "decide" on the best course of military action, when that decision may result in destruction and death.

The potential pitfalls of utilizing AI/ML for military advantage have been propounded ad nauseam.[2] Three issues remain the most concerning: (1) addressing the moral and ethical considerations for giving an AI the authority to destroy things and people; (2) balancing the cost versus military utility of developing AI/ML capability; and (3) ensuring

Major Ayla R. Reed, USAF, program manager at the Maui High Performance Computing Center, Hawaii, holds a master of science in engineering from the University of Arkansas.

1. John R. Boyd, "Patterns of Conflict," in *A Discourse on Winning and Losing*, ed. Grant T. Hammond (Maxwell AFB, AL: Air University Press, March 2018).

2. Arif Ali Khan et al., "Ethics of AI: A Systematic Literature Review of Principles and Challenges," in *Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022* (New York: Association for Computing Machinery, June 2022), https://doi.org/; Avi Goldfarb and Jon R. Lindsay, "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security* 46, no. 3 (Winter 2021–22): 7, https://direct.mit.edu/; Nick Starck, David Bierbrauer, and Paul Maxwell, "Artificial Intelligence, Real Risks: Understanding—and Mitigating—Vulnerabilities in the Military Use of AI," in *Compete and Win: Envisioning a Competitive Strategy for the Twenty-First Century,* Competition in Cyberspace Project, Army Cyber Institute and the Modern War Institute, January 18, 2022, https://mwi.usma.edu/; and Emre Kazim and Adriano Soares Koshiyama, "A High-Level Overview of AI Ethics," *Patterns* 2, no. 9 (September 2021), https://doi.org/.

an appropriate level of trust in a machine to make optimal use of the investment into the AI/ML components of capability development. Nevertheless, uncertainty quantification (UQ) included as metadata to military information can address these three pitfalls while adhering to DoD ethical principles for artificial intelligence.

The DoD artificial intelligence strategy prioritizes and incentivizes the maturation of AI/ML technology.[3] The result has been a flurry of activity attempting to expeditiously implement capability, accompanied by minimal planning for sustainability of capability growth or the higher-order implications for use of AI/ML. As one defense researcher has observed, "When technological change is driven more by hubris and ideology than by scientific understanding, the institutions that traditionally moderate these forces, such as democratic oversight and the rule of law, can be eroded in pursuit of the next false dawn."[4]

The Defense Advanced Research Projects Agency argues that current AI/ML systems "lack the necessary mathematical framework" to provide assurance in use, which impedes their "broad deployment and adoption for critical defense situations or capabilities."[5] Assurance requires confidence, and confidence requires minimal uncertainty. Such assurance in systems using AI/ML can help address ethical considerations, provide insight into the cost of development versus utility, and allow the locus of responsibility for its use in war to remain with commanders and operators at the lowest possible echelon.

By implementing a military standard for uncertainty quantification in AI/ML systems, the Defense Department can secure the much-needed trust in those systems. Further, there are feasible ways to apply existing mathematical approaches for uncertainty determination and propagation if the Department makes UQ a requirement for developers. Yet as the military applies this standard to information, it must bear in mind the higher-order effects and challenges of uncertainty quantification.

Uncertainty Quantification for AI/ML

To address the three pitfalls mentioned above, uncertainty quantification should be required within and by any military digital system. Uncertainty quantification, which is the process of assigning some number(s) to the imperfect or unknown information in a system, will allow a machine to express in real time how unsure it is, adding critical transparency for building trust in its use. The Department of Defense should implement a military standard that specifies the quantification of uncertainty tagged as metadata to each data or piece of information available in digital systems. Once available, these

3. Department of Defense (DoD), *Summary of the Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity* (Washington, DC: DoD, February 2019), https://media.defense.gov/.

4. Zac Rogers, "Have Strategists Drunk the 'AI Race' Kool-Aid?," War on the Rocks, June 4, 2019, https://warontherocks.com/.

5. Defense Advanced Research Projects Agency (DARPA) Public Affairs, "Progressing towards Assuredly Safer Autonomous Systems," DARPA, January 29, 2020, https://www.darpa.mil/.

metadata can be propagated to higher levels of information usage through functional relationships, providing an AI or ML model the information needed to always express how confident it is in its output.

Understanding UQ as metadata requires understanding foundational concepts in metrology—the science of weights and measures—related to measurement uncertainty. That is, a measurement has two components: 1) a numerical value which is the best estimate of the quantity being measured, and 2) a measure of the uncertainty associated with this estimated value.

Of note, the 2008 International Organization for Standardization (ISO) *Guide to the Expression of Uncertainty in Measurements* defines the difference between measurement uncertainty and measurement error. These terms are not synonymous: "The ± (plus or minus) symbol that often follows the reported value of a measurand [the quantity being measured] and the numerical quantity that follows this symbol, indicate the uncertainty associated with the particular measurand and not the error. An error is the discrepancy between a measured value and the actual or true value. Uncertainty is the effect of many errors."[6]

In military parlance, a "measurement" is any information collected and used during an OODA loop. Each piece of information has been measured by a sensor of some sort and will have some uncertainty associated with it. Uncertainty quantification as metadata will take at least two forms: empirically generated measurement uncertainty (based on the metrology standards outlined above) and statistically postulated uncertainty (determined by some means, of which there are many).[7]

An operator can use the system-reported uncertainty to inform their tactical decision when using a UQ-capable system. Commanders can set predefined levels of trust needed for various categories of military action at the operational or even strategic level using such systems, which can help operators understand what their authorities are when using an AI or ML model. This would also help acquisition professionals make appropriate investment decisions for AI/ML capability development because it would quantify aspects of utility. Moreover, providing quantified minimum levels of certainty required in systems using AI/ML addresses the three pitfalls discussed above.

In terms of the moral and ethical concerns of using AI, there is no single right answer to the question "Is it moral or ethical to allow an AI or ML model to decide on a military course of action that will result in destruction and death?" As with all moral and ethical debates, dealing in absolutes is impossible.

---

6. Ian Farrance and Robert Frenkel, "Uncertainty of Measurement: A Review of the Rules for Calculating Uncertainty Components through Functional Relationships," *Clinical Biochemist Reviews* 33, no. 2 (2012): 50–51.

7. Moloud Abdar et al., "A Review of Uncertainty Quantification (UQ) in Deep Learning: Techniques, Applications, and Challenges," *Information Fusion* 76 (December 2021), https://doi.org/; and Apostolos Psaros et al., "Uncertainty Quantification in Scientific Machine Learning: Methods, Metrics, and Comparisons," *Journal of Computational Physics* 477 (March 15, 2023), https://arxiv.org/.

Consequently, the Department of Defense should categorize military actions into one of the three well-known relative degrees of machine autonomy: things a machine can never do by itself, things a machine can sometimes or partially do by itself, or things a machine can always do by itself. The Department of Defense then can define a minimum level of certainty as a boundary condition for each of these categories and/or can define minimum levels of certainty needed for specific actions. The criticality of the decision or action will drive the determination of a UQ boundary. Using uncertainty quantification embraces the nuance and ambiguity in addressing ethical considerations for systems using AI/ML.

When it comes to balancing the cost of artificial intelligence/machine learning with its use, the Department of Defense's fiduciary responsibility is to ensure the investment in AI/ML development is proportional to its military utility. There is no purpose in developing and procuring a battalion of fully autonomous killer droids if AI/ML policy prohibits the US military from allowing an AI to decide to destroy something or kill someone. Therefore, predefined minimum uncertainty boundaries will allow acquisition professionals to determine how best to spend limited resources for the greatest return on investment.

Optimizing trust in AI/ML during capability development will require safeguards against widespread inexperience in AI/ML acquisition and the relative juvenility of the science of uncertainty quantification in machine learning. "Uncertainty is fundamental to the field of machine learning, yet it is one of the aspects that causes the most difficulty for beginners, especially those coming from a developer background."[8] All aspects of system development should include metadata tags for uncertainty quantification, whether the system is intended to be used autonomously or not.

These outputs might be rolled up into a higher-level digital capability that will then require the UQ data to calculate uncertainty propagation. For example, an F-16 maintainer's fault code reader should have uncertainty quantification metadata tagged to each fault reading, providing this quantification at the source. The reader itself is not intended to incorporate AI or a machine-learning model, and that data may not be used immediately in an AI/ML application, but the fault data might be compiled with fleet-wide fault data and submitted to an external ML model that forecasts depot-level maintenance trends. The metadata would follow that set of digital information through any level of compilation or higher-order use.

Requiring uncertainty quantification metadata as a military standard achieves the intent of the Secretary of Defense's ethical principles for artificial intelligence that encompass five major areas:[9]

- Responsible: UQ informs judgment and provides the empirical basis for developing, deploying, and using AI capabilities.

8. Jason Brownlee, "A Gentle Introduction to Uncertainty in Machine Learning," Machine Learning Mastery, last updated September 25, 2019, https://machinelearningmastery.com/.

9. DoD, "DOD Adopts Ethical Principles for Artificial Intelligence," press release, February 24, 2020, https://www.defense.gov/.

- Equitable: Bias in AI can be measured in the same way that uncertainty is and is based on many of the same statistical principles.[10] Bias can then be addressed and improved.
- Traceable: Requiring uncertainty metadata at every level enables traceability in assurance. Performance issues in machines can be traced back to the culpable component.
- Reliable: UQ allows inspection by developers and allows targeted improvement of the most egregious input factors.
- Governable: UQ as boundary conditions for autonomy trust levels can be used to define guidelines for fulfilling intended functions and avoiding unintended consequences.

These ethical principles were adopted to ensure the Department of Defense continues to uphold the highest ethical standards while embracing the integration of artificial intelligence as a disruptive technology. Uncertainty quantification is a practical way to achieve that goal.

Building Trust in AI/ML

A study by RAND found trust is the root cause of most concerns related to the military use of AI/ML.[11] Department of Defense researchers note that "when it comes to forming effective teams of humans and autonomous systems, humans need timely and accurate insights about their machine partners' skills, experience, and reliability to trust them in dynamic environments."[12] For many autonomous systems, their "lack of awareness of their own competence and their inability to communicate it to their human partners reduce trust and undermine team effectiveness."[13]

Trust in the AI/ML model is fundamentally based on the certainty humans have in the information, whether it be a simple sensor output or the overall competency of an autonomous weapon system. This is supported by MITRE Corporation studies:

> AI adopters often ask about ways to increase trust in the AI. The solution is not for us to build systems that people trust completely, or for users only to accept systems that never err. Instead, lessons point to the importance of forming good partnerships based on evidence and perception. Good partnerships help humans understand the AI's abilities and intents, believe that the AI will work as antici-

---

10. V. Ashley Villar and Michael Little, "Technical Memorandum: Focus Area 3—Uncertainty and Bias," in *NASA SMD AI Workshop Report*, ed. Manil Maskey (Washington, DC: National Aeronautics and Space Administration, September 2021).

11. Forrest E. Morgan et al., *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/.

12. DARPA Public Affairs, "Building Trusted Human-Machine Partnerships," DARPA, January 31, 2019, https://www.darpa.mil/.

13. DARPA Public Affairs, "Human-Machine Partnerships."

> pated, and rely on the AI to the appropriate degree. Then stakeholders can calibrate their trust and weigh the potential consequences of the AI's decisions before granting appropriate authorities to the AI.[14]

By thinking of machines—digital or physical—as partners, the military can make analogies to confidence-building techniques with human partners. Sound partnership requires effective two-way communication and a system to reinforce collaboration.[15] Ipso facto, a measure of uncertainty in the digital system output is not useful unless that uncertainty can be conveyed to the human partner. Once machines can quantify uncertainty and can communicate that quantification, they also enable the evaluation of the output and improvement of the system.

Real-time feedback of a machine's awareness of its own competence will increase transparency into the machine's observe, orient, and decide functions by providing quantification of the uncertainty in each of those loops. This feedback improves trust in that specific system and enables quantification of trust in systems-of-systems via uncertainty propagation. For example, consider remotely piloted aircraft (RPA) video surveillance of a potential target. How certain is it that an RPA sensor is accurate and calibrated, that the video stream has not been compromised, and/or that the operator has been given sound baseline intelligence on where to point the sensor in the first place?

Each of these components of the OODA loop has some associated uncertainty that can and should be quantified so that it can be mathematically propagated to the level of decision-making. In this scenario, it would result in a propagated certainty of *x* percent that the target is correct, giving the mission commander confidence in their situational awareness (observation), and allowing them to orient better and decide faster on whether to engage or not.

By quantifying uncertainty and using it in tandem with predefined levels of confidence needed for various categories of action, decisionmakers can create boundary conditions around those military actions that have little to no moral implications as well as those that have serious moral implications. Defense senior leaders can also set thresholds for proportional investment in developing and applying AI/ML capability and can ensure that investment will be used to achieve optimal military advantage. This would provide assurance in a system using AI/ML through a "quantify–evaluate–improve–communicate" cycle.[16]

Uncertainty quantification allows setting if-then relationships for bounding the allowable space of actions for a machine. In another abbreviated example, a space domain

14. Jonathan Rotner, Ron Hodge, and Lura Danley, *AI Fails and How We Can Learn from Them* (McLean, VA: MITRE Corporation, July 2020), 43, https://sites.mitre.org/; and see also Andrew Lacher, Robert Grabowsky, and Steve Cook, "A Framework for Discussing Trust in Increasingly Autonomous Systems," MITRE Corporation, updated June 2017, https://www.mitre.org/.

15. Rotner, Hodge, and Danley, *AI Fails*, 43.

16. Soumya Ghosh et al., "Uncertainty Quantification 360: A Holistic Toolkit for Quantifying and Communicating the Uncertainty of AI," arXiv, June 2021, https://arxiv.org/.

awareness mission may use infrared sensor data to identify space vehicles. The if-then relationship may look like this: If a sensor data-to-target correlation model has a certainty greater than 95 percent, then that target identification information can be automatically updated in the National Space Defense Center catalog. If a sensor data-to-target correlation model has a certainty greater than 75 percent but less than 95 percent, then the machine can attempt a match to signals intelligence (SIGINT) with a certainty greater than 75 percent, or it can send the information to a human to verify.

Using quantified uncertainty thus allows commanders to root decision trees in parameters usable by AI/ML models and to guide how those AI/ML models may be used. In considering the three relative degrees of machine autonomy, commanders can predefine levels of uncertainty for the inputs to each of these categories of action as guidelines for when and under what circumstances it makes sense to let a machine decide, clearly defining the rules of engagement for using an AI or ML model.

All weapon systems, whether intended to incorporate autonomy or not, should provide uncertainty metadata within their planned user interface. Knowing the uncertainty of all inputs benefits conventional weapon systems users as much as applications of AI/ML. By provisioning for metadata now, DoD senior leaders can continue determining the best governance and policy for using AI/ML without slowing down technical and engineering development. Any such governance can be implemented in the future by referencing the quantified uncertainty within a system at the component level or at the output level.

Mathematical Implementation

Applying uncertainty quantification and propagation to tightening the OODA loop assumes functional relationships can be used to define military situations. Functional relationships are the best mathematical approach for this application because it can generally be shown that a cause-effect relationship exists between the value of the function and the input variables, without specifically identifying the exact mathematical form of the relationship. By assuming these functional relationships exist, a general equation which describes the propagation of uncertainty can be used.[17]

A generic functional relationship with uncertainty terms looks like:

$$y \pm u(y) = f(x_1 \pm u_1, x_2 \pm u_2, x_3 \pm u_3, \ldots, x_n \pm u_n)$$

where y is the output, $u(y)$ is the uncertainty of that output, and there are n input variables with associated uncertainties that affect that output. This shows that y depends on n input variables, and in the style of "imprecise probabilists," that the exact value of y is within the interval $y + u(y)$ to $y - u(y)$.[18]

17. Farrance and Frenkel, "Uncertainty of Measurement."

18. Barry N. Taylor and Chris E. Kuyatt, National Institute of Standards and Technology (NIST) Technical Note 1297, *Guidelines for Evaluating and Expressing the Uncertainty of NIST Measurement Results*, 1994 ed. (Gaithersburg, MD: NIST, September 1994); and T. J. Sullivan, *Introduction to Uncertainty Quantification* (Cham, Switzerland: Springer Cham, 2015), 31.

This direct application of ideas intended to improve medical laboratory research pertains to military decision-making as well. "Uncertainty associated with any measurement and its propagation through a defined functional relationship can be evaluated by differentiation (partial differentiation) and the application of the general equation for the propagation of uncertainty."[19] These mathematical approaches would capture the change in uncertainty as many measurands change in a very complex system. This uncertainty propagation equation can be derived using standard statistical procedures, and most importantly, it is independent of the exact form of the functional relationship.[20]

Those more versed in statistics are invited to submit this approach to further case study and determine the feasibility of calculating propagated uncertainty at very large system-of-systems levels when many input variables need to be included. It has already been shown that "the more complex the problem, the more costly it is to obtain calibrated uncertainty estimates."[21] This approach is probably feasible through operational level AI/ML models (i.e., engagements involving a wing or battalion), but a higher-level strategic propagation of uncertainty (i.e., campaign-level models including political-economic or nuclear factors) may require an infeasible amount of computing power to calculate in real time.

Propagation of measurement uncertainty through a machine learning model as part of the input data set is less common than using statistical methods to estimate uncertainty within the model. Data scientists and AI researchers will be familiar with the mass of studies focused on postulating uncertainty within machine learning models, but much of the historical work does not take an approach of adjusting epistemic uncertainty—an insufficient amount of training data for an ML model—with measurement uncertainty in the training data set.[22]

Uncertainty of measurement can be thought of as noise in data and/or variability in the observation. Other aspects of uncertainty need to be quantified when implementing uncertainty quantification in digital systems, such as the completeness of the coverage of the domain, which is the representativeness of the input data set, and the imperfect modeling of the military problem, which is the result of incorrect baseline assumptions during model development and is ultimately rooted in imperfections in human judgment.[23]

A more modern approach to propagation that may be less computationally intensive may be to use machine learning to postulate uncertainty. Evidence from other disciplines using neural networks shows the inclusion of known input data uncertainty "is advanta-

19. Farrance and Frenkel, "Uncertainty of Measurement," 61.

20. Farrance and Frenkel.

21. Umang Bhatt et al., "Uncertainty as a Form of Transparency: Measuring, Communicating, and Using Uncertainty," in *AIES '21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society* (New York: Association for Computing Machinery, July 30, 2021), 2.4 "Uncertainty Evaluation," https://arxiv.org/.

22. Abdar et al., "UQ in Deep Learning"; and Psaros et al., "UQ in ML."

23. Brownlee, "Gentle Introduction."

geous for making better predictions compared to the case of not using them."[24] These researchers also suggest further investigation into using known input data uncertainty "as the initial values of the uncertainties to be derived" in a Bayesian deep-learning framework, which would be a way to propagate empirical uncertainty in concert with statistically derived uncertainty.[25]

Using the mathematical approach to uncertainty propagation will incorporate and account for the effects of aleatoric uncertainty—the inherent randomness of data that cannot be explained—and epistemic uncertainty. The proposed military standard should enfold the requirement for measurement uncertainty with the requirement of its propagation into higher-order uses, such as machine learning or more abstract modeling and simulation. In military parlance, standardizing UQ by this approach will account for not just the baseline observational data uncertainty, but also data uncertainty related to orientation and action.

Math for Military Utility

To continue the analogy to military strategy, a functional relationship describes how military advantage is gained in the OODA loop, and how uncertainty propagates in that process.

Desired Military Effect ± Uncertainty Success = *f [observation (many variables ± u),*
orientation (some variables ± u),
speed of decision ± u
speed of action ± u]

In this purposely emblematic equation, observation and orientation are constant activities, while decisions and actions are discrete events in time. Probability of success of the desired military effect is based on the propagation of uncertainty of each of the input variables in the loop: how certain is the operator that (a) their observations capture reality, (b) they are orienting in the manner intended, (c) their decision was executed the way intended, and (d) their action has not been disrupted.

The barrier to this approach is that it requires prior knowledge of uncertainties, which is metadata that is currently not available because it is generally costly to determine in the empirical case, and because there are many acceptable methods for its generation in the

24. M. Kiani Shahvandi and Benedikt Soja, "Inclusion of Data Uncertainty in Machine Learning and Its Application in Geodetic Data Science, with Case Studies for the Prediction of Earth Orientation Parameters and GNSS Station Coordinate Time Series," *Advances in Space Research* 70, no. 3 (August 2022): 573, https://doi.org/; and see also Wojciech M. Czarnecki and Igor T. Podolak, "Machine Learning with Known Input Data Uncertainty Measure," in *Computer Information Systems and Industrial Management: 12th IFIP TC8 International Conference, CISIM 2013, Krakow, Poland, September 25–27, 2013, Proceedings*, ed. Khalid Saeed et al. (Heidelberg, Germany: Springer Berlin, 2013), 379.

25. Shahvandi and Soja.

statistical case. This circles back to the recommended solution of levying the requirement and a standard to provide the uncertainties related to each of the input variables as metadata. Once provided, AI/ML systems that compile observational and orientation data can use the metadata for propagation and provide an operator or commander with the overarching quantified uncertainty in the situational picture. When used in real time, this approach intrinsically captures facets of the decision and action steps of the OODA loop.

Higher-Order Effects and Challenges

Fairness in modeling is a well-known issue in the realm of AI/ML capability development, and a large body of work is aimed at ensuring this. Realistically, machines can assist in determining the bias in models by using quantified uncertainty, but a model is only as good as its inputs, and a human will be responsible for determining what those inputs are.[26] Models are "only proxies for the real world and their learning and inference algorithms rely on various simplifying assumptions and thus introduce modeling and inferential uncertainties."[27] Simplistically, the root cause of the uncertainty related to the truthfulness and fairness of a model is based on human psychology. This is problematic for many reasons, but these reasons already exist within executing an OODA loop for military advantage and are not exclusive to using UQ or digital information.

Computers are deterministic in that a developer writes a program and "the computer does what [they] say."[28] If a program is based on bad assumptions, a bad result is not the computer's fault. Trying to quantify how good or bad baseline model assumptions are would still be a problem within this larger UQ framework. This component of uncertainty could be based on any combination of judgment factors during development, such as the choice and preparation of data, choice of training hyperparameters, and the choice of omission. Quantifying uncertainty will only help with fairness in AI/ML models by allowing inspection; it does not necessarily make an AI or ML model fairer.

There are statistical approaches to creating fairness metrics using UQ that can be used to improve models, but the approaches still require human assumptions and decisions in development. Providing uncertainty quantification would allow inspection, and that is the first step needed for improving input assumptions, bias, and output.

Choosing the appropriate mathematical formulae for calculating propagation of uncertainty in a functional relationship requires some baseline assumptions to build the best representation of the partial differential terms. The functional relationship and resulting mapping function may be ambiguous as a result of epistemic uncertainty.[29] Determining

26. Bhatt et al., "Form of Transparency"; and Tongfei Chen et al., "Confidence Scoring Using Whitebox Meta-Models with Linear Classifier Probes," *Proceedings of Machine Learning Research* (*PMLR*) 89 (2019).

27. Ghosh et al., "UQ 360," 1–2.

28. Brownlee, "Gentle Introduction."

29. Bhatt et al., "Form of Transparency."

the correct formulae for uncertainty propagation requires further study, but this challenge does not diminish the value in implementing a UQ military standard.

One analysis has shown that communicating and visualizing uncertainty information to operators of unmanned vehicles helped improve human-AI team performance.[30] But other AI researchers have also shown that "more research is needed into how to best capture and present the developer's [uncertainty quantification] in such a way that is meaningful for the user." They further state, "Giving users seeming control over aspects they don't understand has the potential to give the illusions of clarity and informed control, cause additional automation bias, or simply allow the user to select an option that gives them the answer they want."[31] This finding moves solidly into the body of work on decision theory and psychology. There are statistical approaches that attempt to algorithmically define judgment and decision-making, and there are risks to using those approaches.[32]

A separate analysis provides relevant conclusions from the judgment and decision-making literature that pertain to using uncertainty estimates in decision-making. The study concludes that delivering uncertainty estimates to stakeholders can enhance transparency by ensuring trust formation.[33] A key consideration that the authors cover is the way in which UQ is communicated to stakeholders: "Even well-calibrated uncertainty estimates could be perceived inaccurately by people because (a) they have varying levels of understanding about probability and statistics, and (b) human perception of uncertainty quantities is often biased by decision-making heuristics."[34]

The authors further add that "both lay people and experts rely on mental shortcuts, or heuristics, to interpret uncertainty" and that this "could lead to biased appraisals of uncertainty even if model outputs are well-calibrated."[35] Unsurprisingly, key takeaways on this subject are that chosen methods of UQ communication should be tested first with stakeholders, and that developers should cater their UQ display and user interfaces to different end-user types.[36] For example, the presentation of uncertainty quantification to a data scientist should be different than the presentation of UQ to an operator for wartime decision-making. The Intelligence Community has a long history of determining the optimal method of communicating uncertainty related to military information, so its conventions for "words of estimative probability" may be an appropriate point of departure for the latter type of end user.

---

30. Kimberly Stowers et al., "Insights into Human-Agent Teaming: Intelligent Agent Transparency and Uncertainty," in *Advances in Human Robots and Unmanned Systems: Proceedings of the AHFE 2016 International Conference on Human Factors in Robots and Unmanned Systems, July 27–31, 2016, Walt Disney World, Florida*, ed. Pamela Savage-Knepshield and Jessie Chen (Cham, Switzerland: Springer Cham, 2017).

31. Rotner, Hodge, and Danley, *AI Fails*, 44.

32. Bhatt et al., "Form of Transparency."

33. Bhatt et al., under "4 Communicating Uncertainty."

34. Bhatt et al.

35. Bhatt et al., under "3.2 Uncertainty and Decision-making"; and see also Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185, no. 4157 (1974).

36. Bhatt et al.

When thinking of using propagated uncertainty at operational and strategic decision-making levels, there is a chance that using propagation calculations may make UQ numbers irrelevant and unusable because uncertainty approaches 100 percent of the desired output in very complex systems. Incidentally, this is an interesting conclusion that may point to a mathematical proof of the "fog of war." Further investigation into calculating propagated uncertainty at very large system-of-systems levels may better illuminate this conclusion.

Yet this potential shortfall of the benefits of highly propagated UQ is not a strong enough refutation of implementing a UQ military standard. Including the metadata tags at each level allows operators to inspect what factors are contributing the most uncertainty and what factors a commander can have high confidence in, which is still very useful information. When operator bandwidth is available outside of high-stress engagements, these metadata tags allow operators to examine covariance and correlation between input variables in the functional relationship. These metadata can also be used by acquisition professionals for the evaluate-and-improve tasks, by identifying systemic error and eliminating it and identifying the worst offenders contributing to random error.

The potential for highly propagated UQ to be irrelevant also emphasizes the perpetual importance of developing sound military judgment. As in any military situation where uncertainty is very high, operators and commanders with acumen will be required for achieving military advantage. Using AI/ML to observe, orient, decide, and act faster than an adversary will only lead to victory if the actions are superior. This facet of the theory of victory is distinct from the argument for requiring, propagating, and communicating UQ in a standardized way.

Lastly, AI/ML requires input data that is a "suitably representative random sample of observations" of the domain of interest. Importantly, "in all cases, we will never have all of the observations," and "there will always be some unobserved cases" within the domain of interest.[37] Although it is more common that an AI or ML algorithm has been trained on an insufficient data set, attempting to achieve total observational coverage of the domain in a data sampling is not ideal either.[38]

When applying AI/ML to the OODA loop at a higher ops tempo, improving coverage of the domain does not necessitate more sampling, but should be achieved by more randomization in the sampling with focus on determining accurate measurement uncertainty. The study on known input data mentioned above proved theoretically and empirically that incorporating data uncertainty into the learning process for a range of machine learning models made the models much more immune to the problem of overfitting—an unacceptable ML behavior that occurs when the model fits too closely to a training data set, resulting in inaccurate predictions when tasked to evaluate unknown data.[39]

37. Brownlee, "Gentle Introduction."
38. John R. Boyd, "Destruction and Creation," September 3, 1976, https://www.coljohnboyd.com/.
39. Czarnecki and Podolak, "Known Input Data."

The problem of overfitting is not unique to machine learning and is foundationally caused by a deficient input data set. "Simply stated, uncertainty and related disorder can be diminished by the direct artifice of creating a higher and broader more general concept to represent reality."[40] This results in maximum statistical coverage of the domain with minimal intrusion on the system being observed. It also minimizes the size of the data and metadata set, which increases the computational efficiency of the UQ propagation equation in higher-order usage.

Conclusion

> *"We never have complete and perfect information. . . . The best way to succeed in [this ambiguous environment] is to revel in ambiguity."*
>
> Grant T. Hammond [41]

Implementing a military standard for quantified uncertainty metadata and developing the capability to propagate, evaluate, improve, and communicate that information will provide the most flexibility for continuing to pursue AI/ML capability for military use. Using uncertainty quantification with AI/ML systems enables mutual trust and unity within human-machine teams by developing that trust through communication, transparency, and participation in common experiences. Assurance in using AI/ML systems to achieve military objectives requires quantified uncertainty.

Tying back into concepts of military strategy, this entire framework of uncertainty quantification contributes to a winning organization. By provisioning for UQ metadata now, DoD senior leaders can continue determining best governance and policy for using AI/ML without delaying technical and engineering development. As warfighters use UQ to develop trust in AI/ML partners, the military's ability to observe, orient, decide, and act faster than an adversary will increase and ensure military advantage.

---

40. Boyd, "Destruction and Creation," 7.

41. Grant T. Hammond, "The Essential Boyd," American War: Rediscovering the American School of War (website), n. d., accessed March 6, 2023, https://americawar.wordpress.com/.

Deep Neural Networks

Enriching Leadership Screening and Selection

Robert A. Newton
Robert A. Masaitis

Artificial neural networks mathematically approximate how human neural cells perceive objects. Machine learning has proven valuable as a predictive tool to inform human decisionmakers, although decision authority cannot be completely ceded to algorithmic predictors due to tendencies in such tools to create inequities or promulgate systemic biases based on race, gender, or other measured categories. The deep neural network tested in the study demonstrated a 94 percent accuracy for candidate selection, suggesting the approach could assist Air Force Special Operations Command (AFSOC) during initial sorting. Employing such a model could free senior leaders from spending valuable time reviewing hundreds of records for attributes specified by the command's developmental team. Senior leaders could then better spend collective time applying knowledge of candidates and squadrons to ensure AFSOC selects high-caliber leaders.

Each year, senior leaders in various career fields across the Air Force meet to select officers qualified to fill leadership positions within their respective communities, such as squadron command.*[1] The Air Force Special Operations Command (AFSOC) leadership selection board, Commando Eagle, specifically considers special tactics officers (STOs) at the ranks of senior captain through lieutenant colonel and rated (flying) officers from special operations aircraft at the ranks of senior major through lieutenant colonel.[2]

The current process is labor-intensive, requiring all board members individually review hundreds of officer records. Human capital is AFSOC's stated competitive advantage.[3] Using a deep neural network to score officer records—one that is tailorable to the attributes identified by the command's leadership team—into an initial, rank-ordered list would allow board members more time for deeper discussions about officers on the margins

Lieutenant Colonel Robert A. Newton, USAF, holds a master of science in flight test engineering from the Air Force Test Pilot School and a master of science in operations management from the University of Arkansas.

Brigadier General Robert A. Masaitis, USAF, deputy director of global integration on the Joint Staff, holds a master of science in military national resource strategy and policy from the National Defense University and a master of science in defense analysis from the Naval Postgraduate School.

* The authors would like to acknowledge and thank the Air Force Special Operation Command's (AFSOC) Commando Eagle team, particularly Jeff McMaster and Thomas Outlaw, for the insights and access they afforded the authors throughout this project. Without their thoughtfulness and willingness to challenge conventions, this would not have been possible.

1. Air Force Personnel Center, "2020 AFSOC COMMANDO EAGLE Candidate Selection Board Results," Personnel Services Delivery Memorandum, Joint Base San Antonio-Randolph, TX, June 30, 2020.

2 AFSOC, *AFSOC Strategic Guidance* (Hurlburt Field, FL: AFSOC, 2020), https://media.defense.gov/.

and for the command's officer development efforts. Providing senior leaders this additional time to consider individual leadership placements as AFSOC develops and employs its force improves the long-term health of the command. Moreover, it enables transformational change as the command organizes to compete across the operational spectrum.

Background

Artificial neural networks mathematically approximate how human neural cells perceive objects. Simply put, the neural network processes the input layer through multiple hidden layers, yielding the output layer, which is a classification or score in this case.[4] With small datasets—fewer than 10,000 samples using fewer than 100 input variables—deep neural networks with more than two layers have demonstrated higher accuracy and better generalization in classification/regression applications than many traditional machine-learning methods such as random forest, support vector machine, or shallow neural networks.[5]

In the context of evaluating individuals, machine learning has proven valuable as a predictive tool to inform human decisionmakers.[6] Yet given their "black box" nature, it is inappropriate to cede decision authority completely to algorithmic predictors.[7] Decisionmakers must be aware of the possibility that such tools, due to a lack of direct interpretability, may create inequities or promulgate systemic biases based on race, gender, or other measured categories.[8]

Cognizant of possible shortcomings, the public and private sectors have applied neural networks to synthesize multidimensional human resource data into something more interpretable.[9] The US Army, for example, has experimented with using automated assistance to manage talent in its personnel assignment process through its People Analytics initiative.[10]

---

3. Jürgen Schmidhuber, "Deep Learning in Neural Networks: An Overview," *Neural Networks* 61 (January 2015), https://doi.org/.

4. Shuo Feng, Huiyu Zhou, and Hongbiao Dong, "Using Deep Neural Network with Small Dataset to Predict Material Defects," *Materials & Design* 162 (January 15, 2019), https://doi.org/; and Antonello Pasini, "Artificial Neural Networks for Small Dataset Analysis," *Journal of Thoracic Disease* 7, no. 5 (May 29, 2015), https://doi.org/.

5. Jon Kleinberg et al., "Human Decisions and Machine Predictions," *Quarterly Journal of Economics* 133, no. 1 (2018), https://doi.org/; and Aaron Chalfin et al., "Productivity and Selection of Human Capital with Machine Learning," *American Economic Review* 106, no. 5 (May 1, 2016), https://doi.org/.

6. Michael Luca, Jon Kleinberg, and Sendhil Mullainathan, "Algorithms Need Managers, Too," *Harvard Business Review* 94, no. 1 (2016), https://hbr.org/.

7. Ruha Benjamin, "Assessing Risk, Automating Racism," *Science* 366, no. 6464 (October 25, 2019), https://doi.org/.

8. Eleni T. Stavrou, Christakis Charalambous, and Stelios Spiliotis, "Human Resource Management and Performance: A Neural Network Analysis," *European Journal of Operational Research* 181, no. 1 (August 2007), https://doi.org/.

9. Kristin C. Saling and Michael D. Do, "Leveraging People Analytics for an Adaptive Complex Talent Management System," *Procedia Computer Science* 168 (2020), https://doi.org/.

And to mitigate pitfalls, it is possible to create a tool based on equity and fairness by understanding potential algorithmic biases and maintaining a human-in-the-loop to overcome them.[11]

Air Force Special Operations Command's stated intent to develop human capital and employ automation to realize efficiencies presents an opportunity to leverage machine learning in the Commando Eagle process.[12] Using automation would provide more time for the panel to focus on a smaller group of leadership candidates and hold a richer discussion, theoretically resulting in improved squadron leadership selection matches.

Further, a process that is bias-aware could better inform command leaders of systemic disadvantages to any demographic groups. This article examines the development and testing of a process to automate the labor-intensive portion of the scoring procedures, freeing time for senior leaders to employ their collective experience, candidate knowledge, and judgment—the best use of the command's senior-most human capital—in evaluating potential officer candidates.

The Commando Eagle Panel

The Commando Eagle panel consists of colonels and general officers from across the command—approximately 15 officers in total—who review and score the personnel record of every eligible officer over a period of several days.[13] Relevant core Air Force Specialty Codes include special tactics officers, special operations pilots, combat systems officers, and remotely piloted aircraft operators. Communities represented include special tactics, AC-130, MC-130, U-28, combat aviation advisors, CV-22, nonstandard aviation, datamasked, and remotely piloted aircraft, with the highest representation of eligible officers from the AC-130 and MC-130 communities (73 and 89 officers, respectively, for 2020).

Every Commando Eagle panel member scores each eligible officer's personnel record—a dense collection of duty history, training and performance reports, and decorations received over a career spanning 14 to 18 years—on a scale of 6 to 10. Panel members use criteria defined by AFSOC in the scoring guide provided at the beginning of the selection board regarding the depth and breadth of an officer's experience, education, training, and leadership.[14]

If any panel member scores a record with a difference of two or more points from any other panel member, the "split" in scores is resolved by discussion. The board members

10. David Anderson, Margrét Vilborg Bjarnadóttir, and David Ross, "There Are No Colorblind Models in a Colorful World: How to Successfully Apply a People Analytics Tool to Build Equitable Workplaces" (1st place paper, White Paper Competition, Wharton People Analytics Conference, University of Pennsylvania, Philadelphia, 2021), 10, https://wpa.wharton.upenn.edu/.

11. AFSOC, *Strategic Guidance*.

12. Brandon Webster, Thomas Outlaw, and Nicole Whigham, "2021 SOF Developmental Team Outbrief," AFSOC, June 16, 2021.

13. Robert A. Masaitis, personal experience, January 20, 2021.

discuss the rationale for their scores then adjust them to resolve the disagreement.[15] After the scoring and adjudication process is complete, the board secretariat finds the average of the panel members' scores for each eligible officer and produces a rank-ordered list of the officers reviewed. Based on the projected number of vacant leadership positions, plus a multiplication factor to allow for attrition, AFSOC derives an at-target number of leadership candidates, which becomes the "cut line" number for the rank-ordered list. The command then further considers the officers above the cut line for projected available leadership positions.[16]

With this list of candidates, the panel spends its remaining time discussing the personnel and identifying potential fits for leadership positions. Often, as each member of the panel must review several hundred officer records, only a portion of the conference's final days is available for this nuanced discussion, and the panel does not have sufficient time to discuss every officer.[17]

Developing a Deep Neural Network

To address this deficit, the authors developed a deep neural network using an existing database from within Headquarters AFSOC's personnel system as input to generate a score for each officer's record on a scale of 6 to 10, similar to the score generated by the Commando Eagle board process.

Rated Officer Analysis Report Database

The command maintains and updates entries in the Rated Officer Analysis Report (ROAR) database for all of its officers. The database includes 177 columns of largely categorical data. The authors evaluated each column for unique values, eliminating redundancy in the dataset by using a correlation matrix (see the parametric reduction below). The dataset was otherwise simple to factorize and required minimal preprocessing for use by the deep neural network.

The ROAR database by design captures career details of rated officers. In tuning the network design, the authors found including special tactics officers—who do not hold an aviation rating but are evaluated by the Commando Eagle board—increased average and maximum error in the network. Because of the differences in career timing, community size, and requisite experiences, STOs are often selected for leadership placement at different points in an officer's career length when compared with rated aviators, which creates inconsistency across the two communities during the board scoring process.

---

14 Department of the Air Force, *Officer Promotions and Selective Continuation*, Air Force Instruction (AFI) 36-2501, incorporating through DAF Guidance Memorandum (DAFGM) 2023-01, January 20, 2023, https://static.e-publishing.af.mil/.

15. Webster, Outlaw, and Whigham, "Team Outbrief."

16. Masaitis, personal experience.

In practice, special tactics officers compete for the leadership of special tactics units, which are generally not led by aviators, and the combination of the two communities in a single board process appears to be for ease of process management. The panel usually reviews STO candidates separately after board scoring to ensure sufficiency for projected vacancies.[18] Consequently, the authors elected to remove the STO community from the dataset for this demonstration, applying the neural network to the 332 rated officers.

Additionally, while rated officers reviewed included both majors and lieutenant colonels, eligible majors were senior and soon to be considered for promotion to lieutenant colonel or awaiting their promotion date, based on career timing (14 to 15 years of commissioned service).

Neural Network Design

Utilizing the advantages of deep neural networks while taking care not to create an overly complex model that could overfit, the authors iteratively developed a topology minimizing degrees of freedom and error.[19] As scores were generated on a continuous scale, they used the rectified linear unit (ReLU) activation function in each layer to avoid the vanishing gradient problem with additional layers.[20] Additionally, the ReLU function can accelerate the training speed of deep neural networks compared to traditional activation functions.

The study used mean squared error as a loss function, similar to regression analysis, and mean absolute error as the metric for the model, as this is intuitively interpreted when reporting how close the model was scoring each officer's record. The study also employed root mean square propagation (RMSProp)—a gradient descent optimization algorithm—as the adaptive learning rate method, since RMSProp does not decay the learning rate too quickly and thus prevents convergence.[21] Finally, while the authors set the maximum number of epochs to 5,000, they used early stopping to avoid overfitting with a loss "patience" of 250 epochs.[22]

---

17. Masaitis.

18. Feng, Zhou, and Dong, "Deep Neural Network"; and Nikolai Nowaczyk et al., "How Deep Is Your Model? Network Topology Selection from a Model Validation Perspective," *Journal of Mathematics in Industry* 12, no. 1 (December 2022): 1, https://mathematicsinindustry.springeropen.com/.

19. Gregory Naitzat, Andrey Zhitnikov, and Lek-Heng Lim, "Topology of Deep Neural Networks," *Journal of Machine Learning Research* 21, no. 184 (2020), https://arxiv.org/.

20. Fangyu Zou et al., "A Sufficient Condition for Convergences of Adam and RMSProp," in *2019 Institute of Electrical and Electronic Engineers (IEEE)/Computer Vision Foundation (CVF) Conference on Computer Vision and Pattern Recognition* (Long Beach, CA: IEEE, 2019), https://doi.org/.

21. Lavanya Shukla, "Designing Your Neural Network: A Step by Step Walkthrough," Towards Data Science, September 23, 2019, https://towardsdatascience.com/.

Model Results and Discussion

Parametric Reduction

Among the ROAR database entries for officers considered by Commando Eagle for command positions, 23 of the 177 columns had no unique values. This number included the historical columns no longer in use and columns that would signal ineligibility and were therefore unnecessary to consider: specifically, whether an officer was currently a commander, had an unfavorable information file, and had a processed date of separation from active duty. Other columns found through the use of a correlation matrix were determined to be redundant. An example of this is drone experience, a binary value intuitively correlated with a nonzero entry in unmanned aerial vehicle type, also captured more broadly by values like aircraft last flown.

After considering these redundancies and nonunique columns, the authors eliminated a total of 102 columns as inputs for the neural network. They also removed demographic data as inputs to later use to evaluate the model for bias according to gender, race, and Hispanic/Latino designation. The remaining 75 columns from the ROAR database were inputs in the neural network, followed by two hidden layers each with 53 neurons, and a single output neuron for the predicted score. The study authors arrived at this topology through experimentation, increasing the number of neurons to increase accuracy but without adding so many degrees of freedom to cause overfitting.[23]

Model Accuracy

The authors evaluated the proposed network using a test set of 83 officer records not used in training—25 percent of the dataset. The mean absolute error of the model in this test set was 0.145 points with a maximum error of 0.666 points. The network converged in 1,915 epochs, stopping early to prevent overfitting.

Figure 1 shows the relationship of actual scores from the test set with the predicted scores from the model. As previously mentioned, projected leadership vacancies drive the number of officers selected as candidates, and in 2020, this was 160. While the minimum actual score for candidates selected was 8.230 points, the minimum predicted score required to ensure 160 officers selected was 8.182. With both the actual and predicted officers selected as command candidates, the authors generated the confusion matrix for the test set shown in table 1. From this confusion matrix, they determined the accuracy of the model to be 0.940, precision and specificity both 1.000, and sensitivity as 0.884—based on the five false negatives and zero false positives in the test set.

The vertical dashed line in figure 1 represents the minimum score required for an officer to be on the list and considered as a candidate for squadron command (8.230 points), while the horizontal dashed line represents the minimum score generated by the neural

22. Naitzat, Zhitnikov, and Lim, "Deep Neural Networks."

network (8.182 points). The cutoff score for both ensured 160 rated officers were on the list (43 of whom were in the test set), based on forecasted personnel requirements. The solid black line represents a perfect fit (actual scores equal to predicted scores), and the red arrow denotes the maximum error in the test set (0.666 points).

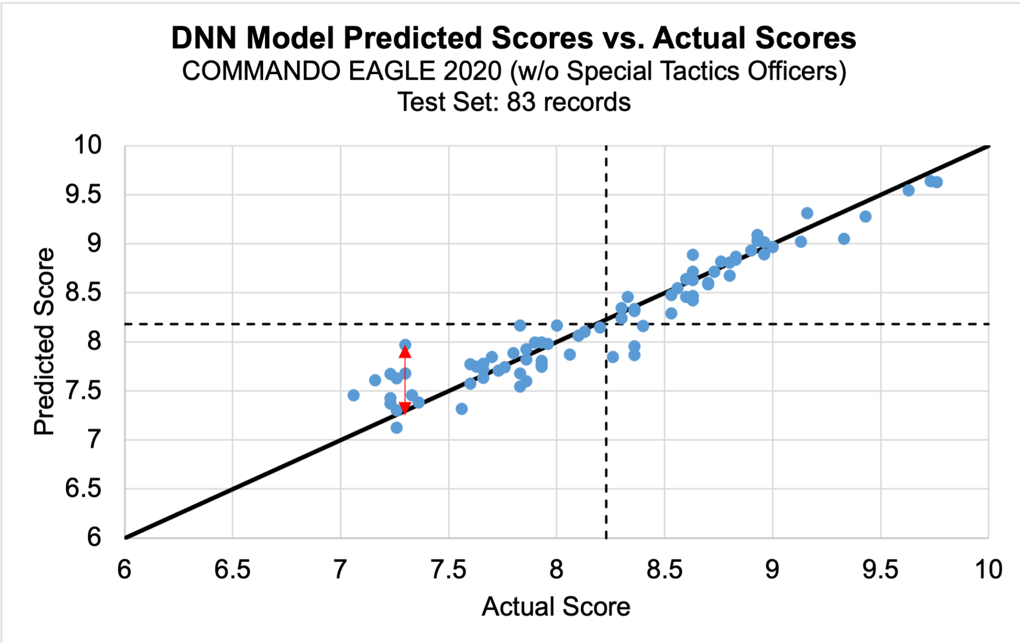


Figure 1. Predicted scores from the deep neural network versus actual scores from the Commando Eagle board

Table 1. Confusion matrix of the 83 records in the test set with actual Commando Eagle 2020 results versus the predicted top officers from the neural network

		Predicted with Neural Network	
	Population = 83	Selected	Not Selected
Actual Board Results	Selected	True Positive = 38	False Negative = 5
	Not Selected	False Positive = 0	True Negative = 40

Given the limited dataset, the authors repeated the fitting of the deep neural network model for over 100 iterations to account for the small size of the randomly selected test set. All but one of the iterations converged, while the remaining iteration was divergent and terminated early after 258 epochs. The maximum error for 99 of the 100 runs was 0.920 points or less with 68 runs less than 0.749 points. The mean absolute error for 99 runs was 0.185 points or less with 95 runs less than 0.175 points, suggesting the use of a deep neural network for Commando Eagle is a repeatable process.

Importance of Factors

Demographic Factors

While the gender, race, and Hispanic/Latino designation factors were not provided as inputs to the deep neural network, the authors tested their significance on the scores using analysis of variance (ANOVA). The dataset, however, was unbalanced demographically in favor of white males who did not identify as Hispanic or Latino (209 of the 332 officers). For example, only 13 females were evaluated, and only two of those females were nonwhite. Only eight officers identified as Hispanic or Latino, and none of those eight were female. As a result, the authors aggregated race to white versus nonwhite for statistical power and did not evaluate intersections with Hispanic/Latino designation.

After the aggregation of race to white versus nonwhite due to sample size, none of these factors were found significant in the actual data or the predicted model nor was the interaction of gender and race (admittedly limited with only two nonwhite females). These results are encouraging in that neither the actual scores nor the model scores appear biased for or against reported demographics. But a dataset with more representation from groups other than male, white, and not Hispanic or Latino would provide greater confidence in this conclusion, particularly with more females.

Nondemographic Factors

The authors also examined the nondemographic data provided to the network to determine significance in the final score assigned to an officer. In the model-predicted scores and actual scores, the study found significant factors in early promotion selection (below-the-zone promotion), year group, weapons school, community, aircraft, core Air Force Specialty Code, professional military education (PME), PME method, academic degree, duty command level, and commissioning source. The authors also looked for interactions informed by the scoring guidance the panel received, with significant interactions between community, aircraft, and Air Force Specialty Code, as well as PME and PME method.

Next, the authors ran regression to determine the relative importance of individual categorical factors in the dataset. Because these categorical data are "one-hot" encoded, they could use the regression coefficients as indicators of importance; that is, a larger coefficient represented a more important factor. The significance of commissioning sources and the communities to which officers belonged revealed by the ANOVA were noteworthy, as these do not necessarily indicate officer performance but are correlated with higher scores. The model predicts officers commissioned through the US Air Force Academy to have slightly better scores on average than officers commissioned through the Reserve Officer Training Corps, the reference population.

The most negative coefficient of the factors found significant was the performance of officers commissioned through the Air National Guard. Additionally, the positive coefficients of every community listed suggest that the reference community, AC-130, on average, received poorer scores than peers from other communities. Even when considering the different aircraft variants of the AC-130 flown by this community—the interaction mentioned above—the differences were generally not large enough to overcome the performance of the other communities that included remotely piloted aircraft, data-masked, combat aviation advisors, U-28, MC-130, and CV-22.

Not surprisingly, based on the knowledge of the scoring criteria, the negative coefficients associated with completing professional military education in correspondence and only having completed Squadron Officer School, versus intermediate developmental education—Air Command and Staff College or equivalent—disadvantaged officers on average. The early promotion selection was the reference population—22 officers in the dataset—and not being selected below the zone had a negative coefficient. This makes sense if one intuitively assumes officers selected for early promotion perform at higher levels and have higher board scores on average.

Conclusion

A deep neural network yielded a command candidate list with 94 percent accuracy and precision, a mean absolute error in scores of 0.145, and a maximum absolute error of 0.666 points. Even with a small dataset with which to train and test, the authors found these results repeatable. In examining for bias among demographic groups, neither the board nor the model exhibited biases, but these results were based on analysis with limited representation from nonwhite and female officers. Including data from multiple years' boards would further increase a network's capacity to model board scores and examine for demographic bias.

That the neural network closely predicted the scores of the actual board suggests AFSOC could find efficiencies in their decision-making/command selection processes by supporting the Commando Eagle panel with a deep neural network. The goal of the Commando Eagle board is to identify the command's most capable officers for future leadership roles. This board and its companion process, the major command developmental team panels, ultimately provide vectors for officers' careers and professional advancement, yet the process of scoring hundreds of individual records currently consumes much of both panels' time.

A hybrid approach, where a deep neural network provides decision support, could give time back to decisionmakers that they can use to create more meaningful, nuanced vectors for the officers evaluated. Further, if future boards manually scored only a subset of 10 to 20 percent of candidates, the command could validate the model while still benefiting from a less labor-intensive process than the current board practice.

To be clear, this proposed process, while bias-aware, does not remove bias from the board. Instead, it provides a method with which to detect potential biases from the human decisionmakers it is attempting to model. Similarly, it is not a replacement for personal knowledge of officers' experiences, skills, behaviors, and talents. This level of insight comes from the human decisionmakers the process intends to support.

Future Work

Air Force Special Operations Command has held subsequent Commando Eagle boards and added additional screening events to its command candidate selection process since generating the data for this review. Adding the actual results from those boards to create a larger dataset with potentially more diverse categorical options as inputs could build an even stronger model for future use. Moreover, it could incorporate any new variables derived from additive screening events such as physical, cognitive, and psychological evaluations. Beyond that, validating the model using current year results trained off previous years' data would further demonstrate utility to the command. Through this practice, senior leaders could become more accustomed to interacting with and applying machine learning, adapting these techniques as needed.

As demonstrated by the authors' removal of special tactics officers from the dataset to reduce model error for aviation-rated personnel, other personnel databases may be more appropriate for nonrated officers. Experimenting with other available personnel databases that capture enough significant details for a wider array of career fields could allow the support from neural networks on a larger scale.

The authors intentionally did not include any natural or human language interpretation in this analysis, looking instead for categorical predictors in officers' records. The language of officer performance reports is often cryptic, particularly regarding stratification statements (e.g., "#1/XX Majors") as guidelines for such statements are inconsistent year after year. A fully informed model for assigning value and weight to stratification statements would be a daunting undertaking in itself. Analysis that included these human language data—potentially scrubbing for word clusters based on previous successful raters and commanders—could enrich a decision-support tool, providing even more nuanced information to decisionmakers in a process the command is already seeking to improve.[24]

Nevertheless, the model's ability to achieve 94 percent accuracy without these data indicates as valid the study's assumption that these discriminators are not independent of other indicators such as below-the-zone promotion and PME method, and that categorical data can adequately provide an initial stratification to the board. ✈

23. AFSOC Public Affairs, "AFSOC Launches Improved Command Screening Process," AFSOC (website), February 10, 2022, https://www.afsoc.af.mil/.

Restrategizing Digitalization in the Military

Paul C. van Fenema
Pieter Soldaat

Digital innovation could lack relevance on the battlefield of the future due to challenges including realism, coherence, and effectiveness. Because the current paradigm is ineffectual, digitalization of the military requires a categorical reframing process. Military leaders must revisit digitalization and its role as a paradigm in enabling military organizations and operations. Three process phases are useful to reframe and reinstitutionalize the digitalization of the military: (1) reflection on the problem; (2) shifting of the framing categories; and (3) construction of the frame. As part of the third phase, four design paradigms will enhance digitalization in military processes: (1) establishing the primacy of nonpermissive ecosystem practices (the operational theater); (2) separating permissive and nonpermissive ecosystem practices; (3) paradoxical coupling of nonpermissive and permissive practices; and (4) investing in communication between humans first with strictly prioritized technological investments.

Military organizations have been investing in innovative concepts and digital technologies since the 1990s.*[1] Military organizations do this because they think they will gain an advantage in reference in terms of temporal and/or capability advantages to an enemy or gain a budgetary advantage for political reasons, basically gaining "more bang for the buck"—or at least the same bang for less bucks. The Dutch Ministry of Defense has already invested substantial amounts of money in digitalization and automatization. It recently published its *Defence Vision 2035*, detailing its move toward an even more data-driven organization.[2] As a result, billions of euros will flow to further digitalization. This trend is happening not only in the Netherlands but also elsewhere in the world.[3]

Dr. Paul van Fenema is a professor of military logistics and associate professor of organizational science at the Netherlands Defence Academy.

Lieutenant Colonel Pieter Soldaat, the liaison officer of the NATO Very High Readiness Joint Task Force brigade, holds a master in military history from the University of Amsterdam.

*The authors want to thank Tim Grant, the editors, and reviewers for their advice and support. We are also grateful to the Future of War Conference 2022 organizers and participants: https://faculteitmilitairewetenschappen.nl/.

1. David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed., rev. (Washington, DC: C4ISR Cooperative Research Program, 2000).

2. Ministerie van Defensie, *Defence Vision 2035: Fighting for a Safer Future* (The Hague, Netherlands: Ministerie van Defensie, 2020), https://english.defensie.nl/.

3. "Chief Digital and Artificial Intelligence Office (CDAO)," CDAO, n. d., accessed March 27, 2023, https://www.ai.mil/.

Digitalization, requiring digital transformation, concerns the phenomenon that "work processes are increasingly intertwined with information technologies, enabling organizations to process large data sets and intelligently subtract and manage information, providing decision-makers with (supposedly) improved knowledge to support analysis and decisionmaking."[4] This article interprets digitalization in the military as a broad concept, affecting strategic processes such as dashboards, business processes such as 3-D printing and digital twins for maintenance and logistics, as well as operational processes such as command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) command and control, and targeting.

These investments are driven by notions like network-centric warfare or the sixth revolution of military affairs.[5] The underlying line of thinking builds on insights like networked military operations, investments in artificial intelligence (AI), and a belief in efficiency, and it resonates with similar ideas in the commercial world—such as Industry 4.0 and its digital transformation and servitization—relying on data, AI, control towers, and cross-organizational interactions.[6]

Specifically, AI has been defined as "scientific discipline, technologies used to realize AI, and AI capabilities."[7] It is also "the frontier of computational advancements that references human intelligence in addressing ever more complex decision-making problems," encompassing facets such as autonomy, learning, and inscrutability.[8] The assumptions undergirding these concepts and technologies tend to promise a novel type of digitalized military organization, preferably with ever fewer soldiers and more combat effectiveness.

But an important conceptual and empirical-professional problem emerges when relating these promises to the actual experiences regarding military digital innovation thus far and the characteristics of military operations in general. It has proven incredibly difficult, especially in the operational theater, to build digital and networked innovation in military organizations that would seamlessly connect enabling and operational processes.[9]

---

4. Therese Heltberg, " 'I Cannot Feel Your Print.' How Military Strategic Knowledge Planners Respond to Digitalization," *Journal of Strategy and Management* 15, no. 2 (April 2022): 220, https://doi.org/10.1108/JSMA-12-2020-0344.

5. Michael Raska, "The Sixth RMA Wave: Disruption in Military Affairs?," *Journal of Strategic Studies* 44, no. 4 (2021), https://doi.org/.

6. Catherine Bucaniec, "Russian Military to Develop Weapons Using Artificial Intelligence," C4ISRNET, August 17, 2022, https://www.c4isrnet.com/; and Johannes W. Veile, Marie-Christian Schmidt, and Kai-Ingo Voight, "Toward a New Era of Cooperation: How Industrial Digital Platforms Transform Business Models in Industry 4.0," *Journal of Business Research* 143 (April 2022), https://doi.org/.

7. Ida Merete Enholm et al., "Artificial Intelligence and Business Value: A Literature Review," *Information Systems Frontiers* 24, no. 6 (2022): 1712; and see also Greg Allen, *Understanding AI Technology* (Washington, DC: Joint Artificial Intelligence Center, Department of Defense, 2020), https://apps.dtic.mil/.

8. Nicholas Berente et al., "Managing Artificial Intelligence," *MIS Quarterly* 45, no. 3 (2021): 1435, 1437, https://misq.umn.edu/.

9. Mikayla Easley, "Skeptics of Services' JADC2 Plans Emerge," *National Defense*, August 15, 2022, https://www.nationaldefensemagazine.org/.

Since the early days of network-centric warfare in the late 1990s, major investments in comprehensive systems for both intra- and extra-theater processes have often been unsuccessful, with limited "power to the edge."[10] After 30 years, progress has been problematic, as shown by Dutch examples including Enterprise Resource Management's Systems Analysis Program Development (SAP), the weapon-storage system COLOR, and operational situational awareness systems such as the Battle Management System (BMS).[11] Even the long-promised paperless office has not materialized.

While such issues have been evident on a national-societal level, no interoperability has occurred on the joint combined interagency level, regardless of the huge investments that have been made. Digital disconnects experienced during international military operations have been reported repeatedly.[12] The build-up and teardown of modern-day command posts takes days, even weeks—much longer than the "analog" command posts of the Cold War. This extensive time commitment was witnessed during the NATO corps exercise Cougar Sword in Wildflecken, Germany, October 7–18, 2022. Indeed, modern military operations require an integrated set of complex digital and energy-providing technologies.[13]

Two questions emerge, one perhaps unpopular: Has the digitalization of the military concerning business and operational practices become trapped in blind optimism? Or has its realization turned into a modern version of the emperor's-new-clothes fairytale? At the very least, the current situation implies that military organizations face a major puzzle with respect to their strategies for digitalization. This is experienced first in the organizations responsible for nonoperational sustainment processes, such as the procurement and maintenance-sustainment organizations. Second, the operational organization at the front line experiences the ramifications of, for instance, choices for products, services, and companies that do not sufficiently lead to operational success.

And at the front line, a vivid concern is the introduction of future technologies that may only function under specific circumstances, with fixed processes and stable infrastructure, and that may collapse when energy, communications, or other vital infrastructure is destroyed.[14]

---

10. Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress*, RL32411 (Washington, DC: Congressional Research Service [CRS], 2007), https://apps.dtic.mil/.

11. Merel Vertegaal, "Development of a Battlefield Management System: How to Use the User" (The Hague, Netherlands: TNO Defense Research, June 1, 2001), https://apps.dtic.mil/; and Jan-Bert Maas, Paul C. van Fenema, and Joseph Soeters, "Post-Implementation ERP Usage: A Longitudinal Study of the Impact of Control and Empowerment," *Information Systems Management* 35, no. 4 (2018), https://www.tandfonline.com/.

12. Erik J. de Waard et al., "Learning in Complex Public Systems: The Case of MINUSMA's Intelligence Organization," *Public Management Review,* November 17, 2021, https://doi.org/.

13. Hind Benbya et al., "Complexity and Information Systems Research in the Emerging Digital World," *MIS Quarterly* 44, no. 1 (2020), https://papers.ssrn.com/; and Paul C. van Fenema et al., "Sustaining Relevance: Repositioning Strategic Logistics Innovation in the Military," *Joint Forces Quarterly* 101 (April 2021).

14. Sebastian Sprenger, "30 Years: Future Combat Systems – Acquisition Gone Wrong, *Defense News*, October 25, 2016, https://www.defensenews.com/.

Concerns about digital communications, digital signatures, and undesirable electromagnetic "presence" abound.[15]

So far, digital innovation as well as digitalization trajectories in military organizations are continuing in an uncoordinated fashion and without awareness of integration challenges.[16] A naive and civilian business-like vision seems to emerge that appears to advocate a mantra of substitution: new digitalized business will replace old business.[17] Moreover, digital innovation proves challenging to materialize cross-level integration, that is, how to relay information across hierarchical levels in and beyond the theater.

This is not to say that military innovations are not necessary. On the contrary, digital innovation runs the risk of lacking relevance in the battlefield of the future due to problems of realism, coherence, and effectiveness. The current paradigm does not work, due not only to practical problems but also for philosophical reasons. Digitalization of the military thus requires a categorical reframing process. This is especially important because given current international affairs, defense budgets will increase substantially in many countries. Such a reframing calls for a revisitation of digitalization and its role as a paradigm in enabling military organizations.

Restrategizing, like any strategic process, involves a process outlining steps to be undertaken and a content side indicating the gist of the strategy's direction.[18] Different views on strategic processes exist, including linear steps and "wayfinding"; this paper adopts the former view to provide an accessible argument.[19] Hence, upon setting the scene, this article proposes processual phases to guide the restrategizing process in terms of reframing. This article then offers design philosophies that operationalize the content side of a new strategy for digitalization in the military. It concludes with implications for research and practice.

Setting the Scene

"Ants and bees can also work together in huge numbers, but they do so in a very rigid manner and only with close relatives. Wolves and chimpanzees cooperate far more flexibly than ants, but they can do so only with small numbers of other individuals that they know intimately.

15. Andrew Eversden, "The Army Wants to Reduce Electronic Signatures of Its Command Posts," C4ISRNET, August 11, 2020, https://www.c4isrnet.com/.

16. van Fenema et al., "Sustaining Relevance."

17. Stella Pachidi et al., "Make Way for the Algorithms: Symbolic Actions and Change in a Regime of Knowing," *Organization Science* 32, no. 1 (2020), https://doi.org/.

18. Robert M. Grant, "Corporate Strategy: Managing Scope and Strategy Content," in *Handbook of Strategy and Management*, ed. Andrew Pettigrew, Howard Thomas, and Richard Whittington (London: Sage Publications, 2006).

19. Robert Chia, "A Process-Philosophical Understanding of Organizational Learning as "Wayfinding": Process, Practices and Sensitivity to Environmental Affordances," *The Learning Organization* 24, no. 2 (2017), https://doi.org/.

> *Sapiens can cooperate in extremely flexible ways with countless numbers of strangers. That's why Sapiens rule the world, whereas ants eat our leftovers and chimps are locked up in zoos and research laboratories."*
>
> Yuval Noah Harari[20]

Since the fall of the Berlin Wall, all militaries have cashed in on the peace dividend, as smaller armies became accustomed to outsourcing and relying on commercial innovation and technologies.[21] For many reasons, military organizations were treated increasingly as if they resembled commercial firms, becoming estranged from the harsh realities of the battlefield and engendering a lack of focus on the psychological and social domains. Assumptions undergirding commercial firms' digitalization then must be reflected upon in terms of how these assumptions apply to military organizations. These assumptions include engineerability; permissiveness of the context in which technology is used; a singular data reality such as shared, single-truth databases; and unidirectional or substitutive transformation toward digitalization.

Engineerability, recognizable in packaged software and business process projects, seems much less feasible in the military. This problem might not have been noticed earlier since many officers and civilian employees working for materiel commands and defense ministries are foremost educated as technicians and/or business managers, as is the case with the Netherlands Defence Academy. This has resulted in a growing tendency to depict the world as a system of systems, where humans are increasingly replaced by digitalization and where they structure their organizations and environment accordingly (fig. 1).

Figure 1 shows from top to bottom an analytics continuum ranging from descriptive use of technologies up to prescriptive use. Human input—light green—gets reduced, for example, shifting to merely checking technology or even being entirely removed from decision-making and action loops. One could also interpret this model using the OODA concept.[22] This is represented as a digital transformation paradigm that assumes an organization is changing at its core unidirectionally and in a substitutive sense toward a digital future (top to bottom in fig. 1).

---

20. "Yuval Noah Harari: Why We Dominate the Earth," *Farnam Street* [*fs*] (blog), accessed March 13, 2023, https://fs.blog/.

21. Ann Markusen, "How We Lost the Peace Dividend," *American Prospect*, December 19, 2001, https://prospect.org/.

22. James Johnson, "Automating the OODA Loop in the Age of Intelligent Machines: Reaffirming the Role of Humans in Command-and-Control Decision-Making in the Digital Age," *Defense Studies* 23, no. 1 (2023), https://www.tandfonline.com/.

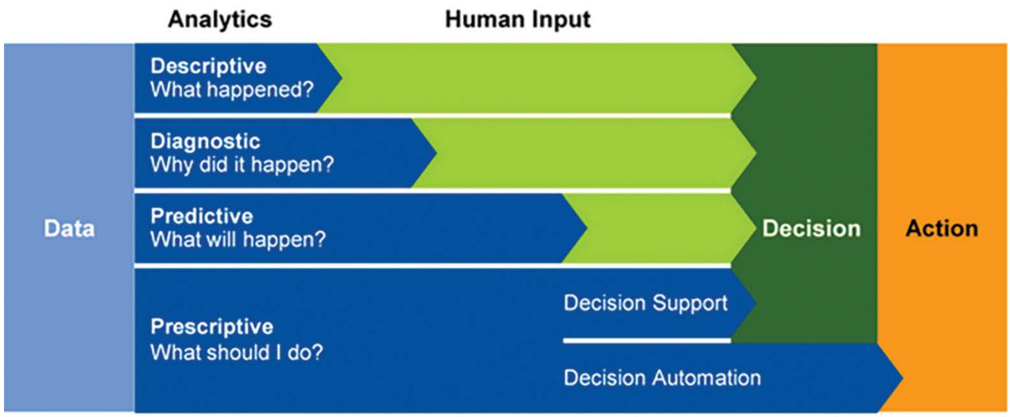


Figure 1. Analytics continuum[23]

This may work for born-digital and incumbent commercial and nonmilitary public organizations. But with a military confronted with real war, assumptions such as one data reality—wherein commercial firms tend to integrate their dispersed operations and rely on shared data and information technology, availability of data, and across-the-board transitioning toward digitalization—are too simplistic.[24] Optimism with respect to advanced digital technologies' capabilities and ignorance of the role of humans require critical reconsideration to avoid building a new military organization that could fail the test of future battle. Digitalization obviously plays a role in the targeting cycle, but this article rejects the ambition of an Internet of Things/Industry 4.0 vision for military operations.

This vision ultimately implies "autonomous decision-making within major functions in an organization. . . . The IT systems within the organization should completely support all the organization processes and they should be fully integrated."[25] After all, many digital technologies come with severe rigidities of routines, built on single-trust data lakes and unlimited connectivity that are rarely possible in operational circumstances.

At the same time, leveraging emerging digital technologies is still important. Military organizations must combine routine business operations with unpredictable theater operations. Therefore, the focus of technology differs across permissive and nonpermissive environments, where the military may or may not have the control or capability to support

23. Gertjan Hendriks and Rick Bouter, "The Analytics Continuum – Data Driven Decisions & Actions," *My Thoughts on Emerging Technology* (blog), February 27, 2018, https://rickbouter.com/.

24. Mary Zhang, "Data Lake: A Single Source of Truth in the Cloud," Dgtl Infra: Real Estate 2.0 (website), November 14, 2022, https://dgtlinfra.com/.

25. Michael Sony and Subhash Naik, "Key Ingredients for Evaluating Industry 4.0 Readiness for Organizations: A Literature Review," *Benchmarking: An International Journal* 27, no. 7 (2020): 10, DOI 10.1108/BIJ-09-2018-0284.

operations. Determining exactly how it differs addresses the challenge of restrategizing digitalization in the military.

A Categorical Reframing Process

Assumptions that apply to commercial firms are inadequate when considering digitalization as it concerns the military, but this can only be understood through a process of reframing.[26] If realities of war are incorporated, consultants, civilian IT professionals in the military, and military leadership can still join forces to digitalize the military but under an altered paradigm. Three process phases are useful to reframe and reinstitutionalize the digitalization of the military: (1) reflection on the problem; (2) shifting of the framing categories; and (3) construction of the frame.

Reflection on the Problem

The first phase reflects on the problem itself. With an increasing reliance on commercial digital innovation, the military has been mirroring in part the civilian need for process optimization, or efficiency, assuming its relevance in the theater. In the civilian world, process optimization might give competitors an advantage, but only because this world is stable, bound by laws and regulations, and therefore almost predictable. Even humans are thought to be dependable and predictable, perceived as cogs in the machinery, as evidenced in their job descriptions.

Yet process optimization supported by digitalization leads to ever more concentration of knowledge of the entire process to ever fewer people. Once digitalized, it will become harder to alter or change the "hardcoded" software for these optimized processes, because too few people know how to adapt these processes and their accompanying software. In fact, advanced digitalization increasingly introduces a paradox and vulnerability for adaptive military operations: pervasive use makes everyone depend on digital technologies, while in-depth expertise is restricted to a limited number of experts. A digital paradigm therefore requires a different view of supply chain logistics and reliability.

Moreover, the upkeep and maintenance of computer systems and especially databases are labor-intensive and require an elevated level of accuracy. Changes are often difficult to make, which is why databases frequently contain old data. This situation can be aggravated because often there is no benefit to the person who enters the data the first time—the data is only reused further up the chain. Feedback loops with the originator are frequently nonexistent, so the data originator does not know how far their input is processed in the chain or what is done with the input.

---

26. Barbara Gray, Jill M. Purdy, and Shahzad Ansari, "From Interactions to Institutions: Microprocesses of Framing and Mechanisms for the Structuring of Institutional Fields," *Academy of Management Review* 40, no. 1 (2015), https://www.jstor.org/.

User interfaces are also often difficult to design and implement, and even the underlying data model does not contain all the possibilities of the real world. Regarding the latter, in the military world, the data model of the NATO Multi-Lateral Interoperability Program (MIP) does not cover all military eventualities that can occur on the battlefield.[27] Moreover, standards for data exchange are often not adhered to, programmers make mistakes, interfaces are faulty, and national military organizations tend to prefer their own national digital technologies at the expense of interorganizational cooperation.[28]

Thus a computer network or a digitalized process can be prone to failure. While technical performance in a permissive environment has been extremely high, the military must increasingly consider kinetic and/or cyber attacks both within the theater and critical data infrastructures outside of the theater.[29] When it fails in practice, it is not uncommon that the user will start to work around these technologies to remedy the problem. For critical issues, a user will find alternative means to achieve a task, such as interpersonal, face-to-face, or remote communications using a repertoire of available technologies—telephone, WhatsApp, or commercial satellite communications. Sometimes users will do this because they know the person on the other end of the line/message. When this happens, the system is lost and will never recover and catch up with reality.

The implementation of digitalized processes already proves difficult in the civilian world, but it is much more so in the military world. For a number of practical reasons digitalization in an operational environment is not so easy. Just-in-time supply chain management—moving materials just prior to needing them for production—will not work because a military environment requires resiliency and redundancy.[30] Another civilian innovation, centralized inventory—with all stock kept in a centralized location—will provide juicy targets for an enemy. Moreover, the end user asking for resupply will have a tough time from a longer distance, since they often can formulate their demands only at an extremely late stage with little time left for supplies to be sent.

In a civilian context, an Amazon.com-style of e-commerce logistics has been extremely successful. It relies on data sharing, analytics, and fast inventory movement based on a flexible, partially outsourced network of individuals and companies. This will not work in the military. However fanciful or nice it would be to have something similar on the battlefield—for example, counting in realtime the ammunition expenditure of a vehicle and sending this in the network—this type of logistics is not necessary and

---

27. Eddie Lasschuyt et al., *How to Make an Effective Information Exchange Data Model, or The Good and Bad Aspects of the NATO JC3IEDM* (The Hague, Netherlands: NATO/OTAN, September 2, 2004).

28. Sebastiaan Rietjens, Erik de Waard, and Paul C. van Fenema, "Employing Comprehensive Intelligence: The UN Experience in Mali," in *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, ed. Paul A. L. Ducheine and Frans P. B. Osinga (The Hague, NL: Asser, 2017).

29. Christian Bueger, Tobias Liebetrau, and Jonas Franken, *Security Threats to Undersea Communications Cables and Infrastructure - Consequences for the EU*, In-Depth Analysis (Brussels: European Parliament, Directorate General for External Policies, Policy Department, April 2022), https://www.europarl.europa.eu.

30. Sandeep Phogat, "The Trouble with JIT in Military Operations: A Review," Line of Sight (Government of Canada), January 26, 2022, https://www.canada.ca/.

more importantly not robust enough. It might equate to giving a fool enough rope to hang themselves.

Digitalization of military operations will need a guaranteed communication layer, but this layer cannot be guaranteed. Furthermore, the improvised nature of this communications layer will require many technicians laying and sustaining the necessary mobile infrastructure. For this reason, numerous supporting communications support—vehicles and personnel—will be visible in the vicinity of command posts, which in itself paradoxically increases the vulnerability of the command posts.[31]

Digitalization also involves physical security demands, ungovernable roll-based access databases due to the high rate of personnel changes in a military outpost, crypto concerns, incompatible software, hardware problems, and significant downtime, so much so that the number of people and amount of effort needed to make this system work will possibly far exceed the advantages, assuming it would ever work. Furthermore, such digitalized processes are vulnerable to enemy action like counterintelligence, surveillance, and reconnaissance or information warfare.[32]

For more philosophical reasons, digitalization in an operational environment will prove difficult as well. The military world finds itself working under a set of paradoxes that is exactly the opposite of what applies to the civilian world.[33] Whereas in commercial firms, success, when repeated, will bring more success, in the military world the enemy learns from their adversary's previous successes, and if a solution is repeated, the enemy expects it, and thus it will likely fail.

The same applies for military solutions in general; the short road—hardcoded processes—to success will prove to be the bloodiest, just because an enemy will also expect this. Every hardcoded process will be watched by the enemy, making the organization vulnerable to enemy intrusion. Thus, it may be better to take the difficult road, which the enemy does not expect. This also calls for flexible and adaptable processes. Due to enemy action, such processes must and will change, and military organizations should therefore steer clear from digital-only and hardcoded process management.

For practical and philosophical reasons, organizations must be incredibly careful with process optimization and digitalization in the military. When the military implicitly mirrors civilian process optimization, it may end up with technologies that are out of touch with its situational needs, as illustrated in the Army's Future Combat Systems Program.[34]

---

31. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985).

32. David Hambling, "GPS Cyberattack Falsely Placed UK Warship near Russian Naval Base," *New Scientist*, June 24, 2021, https://www.newscientist.com/.

33. Edward N. Luttwak, *Strategy: The Logic of War and Peace*, 2nd ed. (Cambridge, MA: Belknap Press, 2002).

34. Christopher G. Pernin et. al., *Lessons from the Army's Future Combat System* (Santa Monica, CA: RAND Corporation, 2012), https://www.jstor.org/.

Shifting Framing Categories

The second phase in the process to reframe the digitalization of military operations concerns the shifting of one category of frames toward another one. A frame is defined as a " 'schemata of interpretation' . . . that actors use to affect the interpretation of events among different audiences"; frames "simplify and condense the 'world out there' by selectively punctuating and encoding events in order to render them meaningful . . . keeping some elements in view while hiding others."[35]

Categories matter as they structure frames people use.[36] Instead of business digitalization as a category, military operations should be an alternative starting point. This resembles a similar shift in military logistics and asset management.[37] The theater poses unpredictable challenges to the military across multiple domains.[38] Engineerability, artifacts, and a systems world—the conceptualization of reality—give way to the harsh reality and experience of warfare.

This argument resonates with the rejection of systemic operational design. Instead, this article advocates a holistic and primarily linear process of designing and planning operations and a preference for improvisational thinking over technical thinking.[39] According to this view, "Military design has particularly emphasized the value of creativity for waging war . . . [and it] connects to longstanding debates in military theory, and particularly to the work of Carl von Clausewitz, who is considered the first to have emphasized chance and creativity as essential characteristics of warfare."[40]

The belief in a "mechanical" worldview was officially abolished in the US military by then Commander, US Joint Forces Command General James N. Mattis (later the US Secretary of Defense) in 2008.[41] He noted the system-of-systems approach led to ever-growing command posts and multiple layers of staff and maintenance personnel yet ultimately produced nothing but "overextension and confusion."[42] He also proposed a return to the

---

35. Peer C. Fiss and E. Zajac, "The Symbolic Management of Strategic Change: Sensegiving via Framing and Decoupling," *Academy of Management Journal* 49, no. 6 (2017): 1774, https://doi.org/.

36. W. Ocasio, J. Loewenstein, and A. Nigam, "How Streams of Communication Reproduce and Change Institutional Logics: The Role of Categories," *Academy of Management Review* 40, no. 1 (2015).

37. van Fenema et al., "Sustaining Relevance."

38. Bradley Cooper, "Precision Logistics: Sustainment for Multi-Domain Operations," *ILW* [Institute of Land Warfare, Department of the Army] *Spotlight* 19-4 (September 2019), https://www.ausa.org/.

39. Milan N. Vego, "A Case against Systematic Operational Design," *Joint Force Quarterly* 53 (2009).

40. Dan Öberg, "Warfare as Design: Transgressive Creativity and Reductive Operational Planning," *Security Dialogue* 49, no. 6 (2018): 494, https://doi.org/.

41. James N. Mattis, "USJFCOM Commander's Guidance for Effects-Based Operations," *Parameters* 38, no. 3 (Autumn 2008), https://apps.dtic.mil/; and see also Mattis, Memorandum for US Joint Forces Command, Subject: Assessment of Effects Based Operations, August 14, 2008, https://smallwarsjournal.com/.

42. Mattis, "Effects-Based Operations," 19.

acceptance of a more complex and chaotic worldview described by von Clausewitz, where people react to people.[43]

New thoughts on military operations include warfare principles and concepts such as surprise, complexity, and nonroutine exploitation of opportunities. Threats can come from any dimension in unpredictably ordered patterns. Successful action depends on breaking patterns and surprising and seeking the unknown, rather than on enacting scripts. Taking military operations as the anchor, military organizations should not advocate only incremental innovations. In fact, disruptive technologies include weapons never envisioned in a linear process, such as atomic bombs and helicopters.[44]

If military operations is a foundational category for framing and designing digital innovation, an open-minded approach is of paramount importance. This starts with strategic mental versatility. This is not surprising given the extreme context of military operations that requires major versatility.[45] Military organizations must have redundancy and holographic modes of organizing to keep functioning under any conditions and avoid easily detectable centers of vulnerability, for example, a single point of failure.[46] That is, organizational modules have their own comprehensive functionality enabling replacement and combination.[47]

This structural redundancy necessitates organizational simplicity. Reflection on framing implies distancing from an institutionalized way of thinking that does not serve the military, specifically the normalized yet problematic crossover between business-type digitalization and the military.[48] This process requires that military organizations "complicate" themselves, rejecting known thought patterns based on previous categories.[49]

Frame Construction

Taking military operations as the category, frame construction becomes the third phase in the process of reframing military operational digitalization. This provides a new take on the interplay of human and technology agency.[50] Starting points are realistic assumptions, such as the unavailability of data, fake data, and lack of energy resources.

43. Antoine Bousquet, "Chaoplexic Warfare or the Future of Military Organization," *International Affairs* 84, no. 5 (2008).

44. We thank one of our reviewers for this insight.

45. Theo Farrell, Frans Osinga, and James A. Russell, eds., *Military Adaptation in Afghanistan* (Redwood City, CA: Stanford University Press, 2013).

46. de Waard et al., "Complex Public Systems."

47. Gene I. Rochlin, Todd R. La Porte, and Karlene H. Roberts, "The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea," *Naval War College Review* 51, no. 3 (1998).

48. Satish Nambisan, Mike Wright, and Maryann Feldman, "The Digital Transformation of Innovation and Entrepreneurship: Progress, Challenges and Key Themes," *Research Policy* 48, no. 8 (2019).

49. Eric-Hans Kramer, *Organizing Doubt: Grounded Theory, Army Units and Dealing with Dynamic Complexity* (Copenhagen: Liber/Copenhagen Business School Press, 2007).

50. Alex Murray, Jen Rhymer, and David G. Sirmon, "Humans and Technology: Forms of Conjoined Agency in Organizations," *Academy of Management Review* 46, no. 3 (2021).

Priority is given to reliable and secure communications and to providing situational awareness to human actors at all levels within and beyond a theater. All humans at all levels are to be capable of thinking for themselves.

In 2022, for the first time, a communication layer was established on which the digitalization of the battlefield could take place. Thousands of Starlink terminals made by SpaceX were deployed over Ukraine in order "to help Ukrainian troops operate drones, receive vital intelligence updates, and communicate with each other in areas where there [were] no other secure networks."[51] Yet widespread outages were reported, leading to "catastrophic" losses of communication in liberated areas and along the front line.[52] Until then, Starlink had proven relatively robust and secure, although it also had to be made jamming-resistant.

With a communication layer established, humans should be able to communicate with each other with whatever digital means are available. Only a connected ring of people working under mission command can adapt and improvise continuously to encountered problems or enemy interference. This idea resonates with literature on high reliable organizations, which stresses, for instance, "heedful interrelating" to understand the context of an evolving crisis and cooperating parties.[53] This should be the orientation of digital innovations and a norm for critically (re)considering efforts in the military to improve or fix automated processes, whether logistical, decision-making, or tactical.

Design Paradigms Starting from Military Theater Operations

As part of the third phase, four design paradigms will help successful digitalization in military processes: (1) establishing the primacy of nonpermissive ecosystem practices (the operational theater); (2) separating permissive and nonpermissive ecosystem practices; (3) paradoxical coupling of nonpermissive and permissive practices; and (4) investing in humans first.

Primacy of Nonpermissive Ecosystem Practices

A first approach acknowledges that while a strategic intent for an operation is likely to be relatively stable, materializing this intent is unpredictable, as the current war in the Ukraine illustrates.

The operational world is chaotic, inducing new forms of military operations. This concept is also referred to as chaoplexity—which acknowledges the order inherent within

---

51. Mehul Srivastava et al., "Ukrainian Forces Report Starlink Outages during Push against Russia," *Financial Times*, October 7, 2022, https://www.ft.com/.

52. Srivastava et al., "Starlink Outages."

53. Karl E. Weick and Karlene Roberts, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," *Administrative Science Quarterly* 38, no. 3 (September 1993): 357, https://www.jstor.org/.

chaos and complexity—as a sequel to networked operations.[54] Military operations in the theater do not rely on process optimization but on unpredictability, asymmetry, secrecy, and obtaining advantage across domains. People will try to outsmart each other, including through electronic warfare and information warfare.[55] Ukraine blows up bridges; Russia will use pontoons. Ukraine destroys ammunition depots with HIMARS rockets; Russia will spread its depots in attempts at decentralization.

In order to be able to adapt and improvise, military operations must prioritize communication between humans. For instance, the authors experienced remote communication challenges during an exercise in Norway, which demonstrated the key role of human-to-human communication. The satellites were just at the horizon, resulting in the satellite dishes pointing into the ground. Military radio signals were dampened by the thick, wet forests, and civil 4G networks had no coverage. Command posts thus had to fall back on military personnel using motorcycles to deliver messages on USB sticks. This manner of communication may seem outdated, but such a measure may be required in the overall repertoire of operations as the situation demands it.

Separating Permissive and Nonpermissive Ecosystem Practices

Civilian corporate resources are mostly prohibited from nonpermissive environments. Their concepts of networked digital services are not likely to play a useful role in such unstable, uncertain environments. First and foremost, under the law of armed conflict, civilians may become legitimate combatants and therefore targets if they assist one side over another.[56] Moreover, commercial sources may also be considered fair game, as indicated by the argument that SpaceX satellites are now a legitimate military target.[57] This article proposes a separation between extra- and intra-theater paradigms, each with their own set of problems. The split is likely to occur between the operational theater supply chain and extra-theater defense industrial base, implying a novel focus for digital innovation: not a highly mature digital network, but a network that keeps working.[58]

This separation between permissive—extra theater—and nonpermissive—intra-theater—applies also to high-tech assets used in military operations in the theater. These technolo-

---

54. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009).

55. Farrell et al., *Military Adaptation*; and Mykhaylo Zabrodskyi et al., "Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022," Royal United Services Institute for Defence and Security Studies (RUSI) (website), November 30, 2022, https://rusi.org/.

56. "The Practical Guide to Humanitarian Law," Medicins Sans Frontieres [Doctors without Borders] (website), accessed March 13, 2023, https://guide-humanitarian-law.org/.

57. Tara Brown, "Can Starlink Satellites Be Lawfully Targeted?," Lieber Institute, West Point (website), August 5, 2022, https://lieber.westpoint.edu/.

58. Raffaele Della Croce et al., *Building Resilience: New Strategies For Strengthening Infrastructure Resilience and Maintenance* (Paris, France: Organisation for Economic Cooperation and Development, 2021), https://www.oecd.org/.

gies increasingly rely on advanced servitization, data-driven analytics pertaining to assets and service logistics, and constant fleet-level learning, such as Tesla's practice of leveraging its large fleet of cars for machine learning. These digitalization trends exemplify the unidirectional and comprehensive transition toward the "cognitive enterprise," relying heavily on integrated computing platforms for operating. Concepts such as platforms, standardization, and visibility optimize multiple business processes outside of the theater. But they must be put on hold in a nonpermissive context.

Artificial intelligence may support units if sufficient data is available, with units flexibly reverting to non-AI modes when deemed beneficial or necessary. This implies a transition in mindset and a check-in/check-out process when units move toward or out of a nonpermissive environment. Their systems may have only partial data collection leaving the nonpermissive environment. This requires the optimization-oriented organization to pick up the pieces and "recharge" advanced technologies in cooperation with industry, as the challenges with standards based on models such as NATO's Joint Command, Control, and Consultation Information Exchange Data Model (JC3IEDM) and earlier Army Tactical Command and Control Information System (ATCCIS) illustrate.

Yet limited maintenance and update facilities are available in the theater. Moreover, relying on data sharing across networks for remote support is risky and often impossible. Hence, to serve military operations, the digital innovations remain concentrated in the asset—such as a weapons system—and on hold until the asset reappears in the permissive environment. Moreover, sustaining capabilities to deal with old technologies remains relevant, as the Ukraine conflict illustrates.

Paradoxical Coupling of Nonpermissive and Permissive Practices

Coupling implies that design is geared toward operations dominating, but it needs to provide room for another type of design.[59] Intra- and extra-theater practices of the digital ecosystem coexist yet not in an equal manner. In addition, they depend on inter-human communications to ensure mutual understanding. Such coupling is paradoxical because the diversity of the two ecosystems—intra-theater versus extra-theater—implies contradictory requirements and paradox management.[60] Figure 2 shows a split between permissive and nonpermissive environments.

As an exception, cyberspace, according to Joint Publication 3-12, *Cyberspace Operations*, is a recognized nonpermissive environment.[61] On the left, efficiency (low stocks), concepts like just-in-time management, and comprehensive technologies rule the game; on the

59. Öberg, "Warfare as Design."

60. Wendy K. Smith, and Marianne W. Lewis, "Toward a Theory of Paradox: A Dynamic Equilibrium Model of Organizing," *Academy of Management Review* 36, no. 2 (2011).

61. Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: CJCS, June 8, 2018), https://irp.fas.org/.

right, redundancy (just-in-case stock management—the storage of large inventories to prevent shortages) and resilience rule.

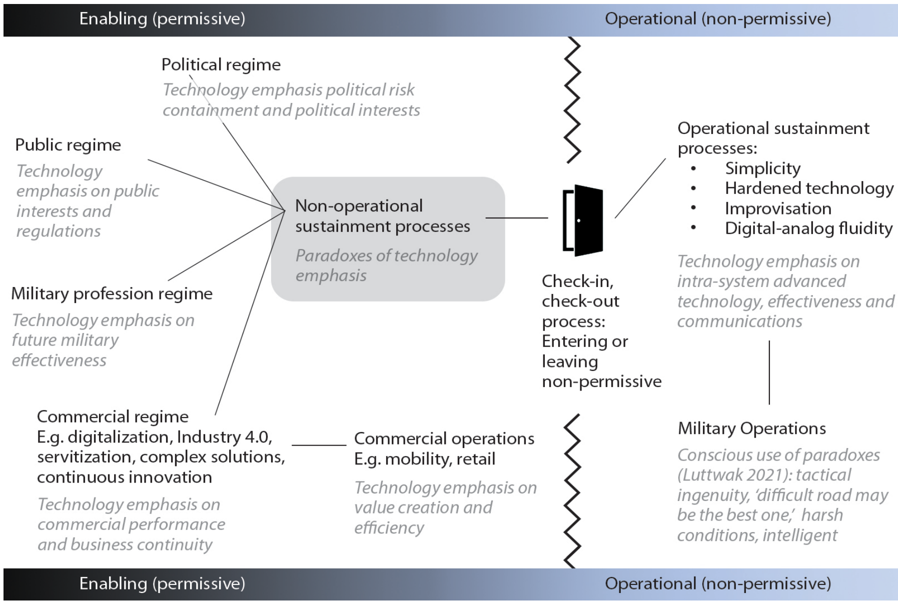


Figure 2. Digitalization in the military

The paradox also applies to complexity-simplicity: in the permissive environment, technical complexity prevails to optimize processes. The coupling is different from coexistence since military operations dominate the overall ecosystem in nonpermissive environments. For instance, this could mean that in the permissive environment, decisions are made that differ from regular business.

Where possible, communications from inside to outside the theater offer chunks of information to be analyzed using digital capabilities outside of the theater. Incomplete information is a starting point rather than a nuisance to a model, assuming single-truth data sets that are complete.

Humans First

In a highly automated world, people are both the problem and the solution. They are the problem because they are forced to improvise in unpredictable ways and they make mistakes, such as software engineers creating faulty software, military units forced to use unreliable equipment due to political/industrial machinations, or maintenance personnel and operators typing errors. At the same time, humans are also the solution. Whereas a computer will signal a system error and halt operations when a mistake or issue is encountered, humans will talk to each other and will attempt to resolve the issue by improvisation, and the process does not stop.

Therefore, militaries must invest in human interaction first in a chaoplexic environment. For example, in 2006, a simple chat program, J-chat, proved to be the most useful and most-used program of all computer systems in the International Security Assistance Force (ISAF) domain in Afghanistan, and it continues to be so in modern-day command posts. Even radio broadcasts were transcribed into written chats so that everyone in theater could subscribe to and read what was happening with platoons operating in other sectors that were normally out of range. Additionally, people would chat to each other when an icon on a screen was distrusted, because, for example, it had not moved for awhile. This interpersonal communication also gave a form of feedback and acknowledgement.

In chaotic environments, only humans can adapt. There is no room for integrated cross-process automation. In the operational environment, processes should be as short as possible and connected to each other by humans. Humans () must interlink multiple processes so that these processes can quickly be rearranged ():[62]

Instead of striving for all-encompassing automated systems, then, one should divide the process into smaller components where humans can intervene, interrelate, and improvise. While humans interlink processes using technologies, this article acknowledges the demarcated usefulness of autonomous data flows. This approach creates overdependence on humans and leverages humans' higher cognitive capabilities. Therefore, the approach has to be nuanced with the idea that AI and automatization can or even must be implemented for short-term processes where the reaction time of human operators may prove to be too long, such as with air-defense systems on ships and Iron Dome-type settings.

In any case, every computer system or automated process should be highly accessible and understandable.[63] These should also be equipped with a manual override button, figuratively speaking. The notion of conceptualized workflows as common in business process design and packaged software does not fit in a nonpermissive operational environment.

There are three final thoughts on process aggregation and AI: On one hand, within demarcated subprocesses, AI may increasingly speed up decision-making and leverage vast amounts of data, if these are available. On the other hand, for aggregated-composed series of subprocesses, military organizations run the risk of AI combining processes in an inaccessible, incomprehensible, and possibly undesirable fashion. Also, thought should be given to how susceptible computer AI is to deception, as compared to humans. At the same time, in the future, they may be able to control interlinked subprocesses and rely on

62. Clay Bartels, Tim Tormey, and Jon Hendrickson, "Multidomain Operations and Close Air Support: A Fresh Perspective," *Military Review* (March–April 2017), https://www.armyupress.army.mil/.

63. Peter Svenmarck et al., "Possibilities and Challenges for Artificial Intelligence in Military Applications," in *Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting* (Bordeaux, France, May-June 2018), https://www.foi.se/.

AI. This applies in particular to theaters combining absence of noncombatants and urgent pressure to transition to extreme levels of warfare speed and span of control. As US Secretary of the Air Force Frank Kendall mentioned in 2021:

> This year, the [Air Force's] chief architect's office deployed AI algorithms for the first time to a live operational kill-chain at the Distributed Common Ground System [DCGS] and an air operations center for automated target recognition. In this case, moving from experimentation to real military capability in the hands of operational warfighters significantly reduced the manpower-intensive tasks of manually identifying targets—shortening the kill chain and accelerating the speed of decision-making.[64]

Conclusion

A categorical shift in strategizing digital innovation for military organizations is needed. This opens space for four design paradigms applicable to service ecosystems, which when combined offer a novel approach to digitalization in the military. Starting from chaoplexity, this article seeks a new mode of engaging multiple specialists in a concurrent fashion with innovative objectives derived from the operational context and future technologies.

Military operations—within an operational theater—represent the primary subecosystem driving design efforts. Such design is separated from extra-theater ecosystems but still (paradoxically) coupled. This research has implications in four areas.

Digitalization in the Theater

Rejecting transposition of commercial concepts as a primary move, future research can start with properties of military operations, both generic ones informed by history and those emanating from the current and upcoming era of partial digital and multidomain warfare. Considering electronic warfare awareness and how to remain unnoticed are starting points for design rather than afterthoughts. Communication is reduced and secrecy is enhanced when units are logistically independent and have a certain number of their own supplies, not needing to ask or communicate a logistical need.

Controlling Networks within and beyond the Theater

Conceptualization has evolved quite separately in different communities of practice such as military academics and nonmilitary business studies orienting toward commercial firms and permissive environments. How is the chaoplexity of the theater coupled with supply chains that operate in a more routine fashion? A gradual transition from nonmilitary business value chains towards boundary spanning military(-ish) supply chain

64. AutoNorms WebAdmin, "Shortening the Kill Chain with Artificial Intelligence," AutoNorms (website), November 28, 2021, https://www.autonorms.eu/.

organizations and onwards to the military operation deserves more research. This includes possibly inevitable public-private frictions.[65]

Moreover, organizations assuming they operate in a permissive environment may have to consider risks in a total-war situation, including cyber attacks and espionage.[66] Digital technologies such as meta and digital twins may overlayer permissive and nonpermissive operations and support conflict resolution across the entire chain. To achieve network control, more insights in the interplay of formal command chains and informal, often lateral, communications are needed.[67]

Human and AI Interplay in the Military Context

Strong military operational validation is paramount; this concerns testing concepts, technologies, processes, and people under nonpermissive circumstances. New insights are needed to enable fluidity of shifting between advanced digital and simple analog ways of working, while acknowledging the importance of simplicity and improvisation.[68] Instead of opting for one digital transformation strategy, as is common for businesses, the military may need many or all of them in the theater, maybe even being "proud to be analog."[69]

Diversity of Communications

Finally, more than process automatization, militaries should prioritize the ability to communicate between human operators with a diversity of means. This effort entails ensuring fall-back options under any circumstances that can deal with complexity and fragmentation and allow for improvisation and adaptation.[70] Accordingly, this article encourages communication technology, but it is hesitant with respect to automation technology, especially in a nonpermissive context. As Yuval Harari noted above, homo sapiens won the race because they communicated. Therefore, digitalization should support the flexible cooperation of strangers relying on swift trust, including technological actors such as AI and robots.[71] ✈

65. Peter Tatham, "An Exploration of Trust and Shared Values in UK Defence Supply Networks," *International Journal of Physical Distribution & Logistics Management* 43, no. 2 (2013).

66. Elad Bengigi et al., *Logistics in Contested Environments* (doctoral dissertation, Naval Postgraduate School, 2020), https://www.academia.

67. Rob Sinterniklaas, "Future of Command Relationships: Lessons from an Ancient Land" (conference paper, The Future of War Conference, Amsterdam, October 5–7, 2022).

68. Carl von Clausewitz, *On War*, Michael Howard and Peter Paret, eds. and trans. (Princeton, NJ: Princeton University Press, 1984).

69. Zeljko Tekic and Dmitry Koroteev, "From Disruptively Digital to Proudly Analog: A Holistic Typology of Digital Transformation Strategies," *Business Horizons* 62, no. 6 (2019).

70. Jeroen Wolbers, Peter Groenewegen, and Kees Boersma, "Introducing a Fragmentation Perspective on Coordination in Crisis Management," *Organization Studies* 39, no. 11 (2018).

71. Steve Curnin et al., "Role Clarity, Swift Trust, and Multi-Agency Coordination," *Journal of Contingencies and Crisis Management* 23, no. 1 (March 2015), https://doi.org/.

JADC2 Culture at the Operational Level of War

Thomas L. Cantrell

Joint all-domain command and control (JADC2) represents a historical transformation in conducting warfare. The changes have manifested through technological advancements and resulting command-and-control reconfigurations, many of which are nascent. While these two levels of JADC2—technology and command and control—are still in development, the Air Force can prepare with changes to the organizational culture, the foundational layer underpinning both. Air components must foster a culture that is truly domain agnostic, engages partners meaningfully in operations, embraces the kill web, and executes daily tasks in a connection-rich environment.

The US Air Force is in the midst of a transformation as it readies itself for a potential great power conflict with a near-peer competitor. One of the most wide-ranging changes will be the implementation of Joint all-domain command and control (JADC2). The US military must consider the implications this change has for the operational level of war, which for the Air Force is embodied in its air components and its air operations centers (AOC).

JADC2 involves establishing a complex amalgam of connected sensors and machine-to-machine interfaces that will integrate service components, Ally and partner nations, and kinetic/nonkinetic domains of warfare. The resulting new asymmetric advantage will preserve US military superiority in the same way the 1980s precision revolution did in the post-Cold War era. As such, JADC2 dialogue has been overwhelmingly technical in nature and has focused on a future state when the architecture will be realized. What receives less attention is the vast human dimension to JADC2 and the cultural change required of Airmen and air components to make this asymmetric advantage a reality.

Air components must pay equal attention to cultural and technical changes within their organizations if JADC2 is to be successful at the operational level of warfare. Truly, JADC2 can be envisioned as a pyramid with the wizardry of promising technology featured at its top. Yet that technology rests firmly on two lower and broader layers: a middle layer of agile command and control (C2) and the critical foundational layer consisting of military personnel and their warfighting culture.

Organizational culture is the collection of values, expectations, and practices that guide and inform the actions of all team members. It must be addressed early for transformation to occur. As one analysis affirms, "it is necessary to educate Airmen early on new

Colonel Thomas L. Cantrell, USAF, Retired, serves as a senior adviser in Joint all-domain operations, intelligence, and strategy with the operational command training program of the 505th Command and Control Wing. He holds a master of science in strategy and Joint campaigning from the Joint Advanced Warfighting School.

concepts in warfare that might require changes to organizational structure and culture, and as JADC2 matures, so should plans for instruction."[1] JADC2's technology may lie in the future, but preparing for this new concept of warfare is today's problem.

To be successful in JADC2, air components must foster a culture that embraces Joint capabilities, understands nonkinetic processes, and sees partner nations as solutions to problems. This is a culture that values horizontal collaboration at the lowest possible level and demands radical sharing of information, so the best shooter will have the best chance to strike the target. Moreover, this is a culture of curiosity, but a curiosity constantly searching for the best ways to ensare the enemy in its kill web.

A pyramid metaphor allows a further examination of JADC2 and its impacts to the air component. The top layer of the JADC2 pyramid represents technology and technological change. The middle layer represents the agile C2 element of JADC2 and how this poses an organizational challenge to air components and especially to their AOCs as they are currently configured.[2] The bottom layer represents the critical foundation of an optimized JADC2 culture.

Incidentally, the significance of this cultural layer is abundantly clear to the Air Force's Operational Command Training Program (OCTP). Part of the 505th Command and Control Wing, this program comprises a group of operational C2 subject matter experts who mentor and advise every air component around the globe via major exercises and real-world contingencies. The views in this article are based in part on conversations with hundreds of senior leaders and practical observations from these complex events that took place from 2019 to 2023.

The Technological Layer

The Department of Defense states that the purpose of Joint all-domain command and control is "to produce the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners to deliver information advantage at the speed of relevance."[3] Put simply, JADC2 is a means to directly tie every sensor to every shooter irrespective of service, domain, or partner.

The Department of Defense highlights the ride-sharing service Uber as an analogy to describe its desired end state for JADC2.[4] In a similar manner that Uber matches riders to the best possible drivers using apps and algorithms, JADC2 will use apps and algo-

1. Timothy Marler et al., *What Is JADC2, and How Does It Relate to Training? An Air Force Perspective on Joint All-Domain Command and Control,* PE-A985-1 (Santa Monica, CA: RAND Corporation, 2022), https://www.rand.org/.

2. Frederick "Trey" Coleman, "Air Operations Center Evolution: A Roadmap for Progress," Wild Blue Yonder, March 14, 2022, https://www.airuniversity.af.edu/.

3. Department of Defense (DoD), *Summary of the Joint All Domain Command and Control (JADC2) Strategy* (Washington, DC: DoD, March 2022), 3, https://media.defense.gov/.

4. John R. Hoehn, "Joint All Domain Command and Control (JADC2)," In Focus 11493 (Washington, DC: Congressional Research Service (CRS), January 21, 2022), https://crsreports.congress.gov/.

rithms to match targets to the best possible weapons regardless of service, domain, or partner nation. The overall effect of JADC2 is to enable high-tempo observe, orient, decide, and act (OODA) loops for rapid C2 decisions, because in great-power conflict, speed and accuracy are paramount.

The Air Force has embraced the advanced battle management system (ABMS) concept to execute JADC2. This concept proposes using cloud environments and new communications methods to share data seamlessly, using artificial intelligence to enable faster decisions among an Internet of Things made of sensors, C2 systems, and shooters.[5] The Air Force has identified four key elements to make ABMS a reality: a sensing grid, advanced networking, decision-making, and authorities and delivery of effects.[6]

Sensing Grid

The sensing grid is envisioned as a network of sensors collecting vast amounts of platform-agnostic, all-domain data to gain and maintain decision advantage. The sensing grid is platform agnostic because it does not care what platform generates the data—it could be an intelligence, surveillance, and reconnaissance (ISR) aircraft, a Navy ship, or a social media account. The grid also is indifferent to the domain that generates the information; whether it is air, land, sea, space, cyber, human, or electronic warfare does not matter. The sensing grid swarm will consist of DoD platforms, willing partner nations, and relevant commercial sources.

Advanced Networking

JADC2 requires an agile and resilient network to transport data in real time across all components and domains. This network must be able to operate in a contested, degraded, and operationally limited environment. This environment will require multiple pathways to resist adversary network attacks, and if it cannot resist degradation, then it must be able to be healed quickly or at least brought to some limited capability. While the network (transport) is key, equally important is the data (content). Data standards are crucial to advanced networking. If nodes from all domains, services, and partner nations are to share warfighting-relevant information, their data must be structured in a way to make it universally compatible.

Decision-Making

This element relies on human-machine teaming to sort large volumes of data gathered by the sensing grid and present it in a way that makes decision-making easier. Joint all-domain command and control envisions reliance on artificial intelligence and machine

5. John R. Hoehn, "Advanced Battle Management System (ABMS)," In Focus 11866 (Washington, DC: CRS, February 15, 2022), https://crsreports.congress.gov/.

6. Headquarters, US Air Force (HAF), "USAF JADC2 Supporting Concept," July 8, 2021, 2.

learning (AI/ML) to enable this process. Some examples might be performing industrial tasks such as plotting real-time order of battle or matching kinetic platforms armed with optimized weapons to take out a dynamic pop-up target. JADC2 also envisions a global and all-domain common operating picture fused with a common intelligence picture to enable rapid decision-making and integration across all echelons supporting or executing the fight.

Authorities and Effects Delivery

The goal of authorities and effects delivery is to match the right weapon to the right target. In an all-domain environment, the right platform and weapon may be cyber, air, maritime, ground fires, or whatever makes the most sense from an effects-based perspective and whatever asset is most readily available given physical reach and connectivity status at that point in time. Mission authorities to leverage capabilities from other domains, services, and partner nations must exist for JADC2 to work. Establishing contracts and mission-type orders to enable these authorities is something that must be accomplished prior to conflict. And authorities also call into discussion how all-domain capabilities are to be controlled at the operational level of war, especially when dealing with Joint counterparts.

The Joint counterparts to the advanced battle management system—the US Navy's Project Overmatch and the US Army's Project Convergence—heavily emphasize common data standards in order to share the targeting data needed for convergent fires. The Navy and the Army are looking for ways to establish common data standards because data sharing continues to be a challenge within and between each service.

Project Overmatch is developing a new fleet architecture using artificial intelligence and manned/unmanned teaming for Distributed Maritime Operations.[7] The Navy is striving to build the Naval Operational Architecture in a way that will enable a common standard for every part of the fleet to exchange data and establish interoperability with other services.[8] Project Convergence is the Army's JADC2 concept designed to integrate artificial intelligence, robotics, and autonomy to improve battlefield situational awareness, connect sensors with shooters, and accelerate the decision-making timeline.[9]

The C2 Layer

The need to address all-domain authorities has emerged as a common theme during recent Tier 1 exercises, US Air Force wargames, and experiments. Joint all-domain command and control's lateral connectivity, where every sensor is connected to every shooter,

---

7. Hoehn, "JADC2."

8. John R. Hoehn, *Joint All-Domain Command and Control: Background and Issues for Congress*, R46725 (Washington, DC: CRS, January 21, 2022), https://crsreports.congress.gov/.

9. 505th Command and Control Wing Public Affairs, "Nellis' ShOC-N Supports Army Project Convergence Experiment," US Navy (website), December 7, 2022, https://www.navy.mil/.

begs the issue of command and control: Who makes the decision to shoot? When, where, and with what? Today's C2 construct puts each service component and domain into its own silo where they work in parallel as deconflicted by the Joint combatant or Joint Force commander. Yet this current C2 construct is seen as antiquated and too slow for the anticipated speed, range, and multidomain nature of a future great-power conflict. In an era where all services and domains are connected and speed is a priority, the question becomes, Who gets to command and control all-domain fires? The answer to this question has huge implications for air component Airmen.

The Air Force transformation includes a change to its mantra. No longer do operational-level warriors tout "centralized control and decentralized execution" as their doctrine but instead offer "centralized command, distributed control, and decentralized execution" as the way forward.[10] The introduction of distributed control is meant to disassociate control from command—indeed, some have taken to calling it "control and command"—as a means to better operate in a JADC2 environment where single C2 nodes are degraded or destroyed and control can actually occur in a multitude of places.[11] Distributed control makes sense where multiple control nodes share a ubiquitous common operating picture/common intelligence picture; where AI/ML assists the matching of targets to weapons; where a single, concentrated C2 node makes for an inviting target; and where speed is of the essence.

The Doolittle Games and Chennault war games executed since 2018 represent an effort to better understand all-domain operations and the associated implications for control and command. That is where new concepts such as agile control and integrated command have been discussed.[12] Agile control leverages multiple nodes to exert air battle management across the operational environment, not just the air operations center or a platform-centric C2 node such as an E-3 Sentry aircraft. Integrated command explores how Airmen could assume authorities over all-domain fires—such as cyber, space, and maritime—at the operational level to prosecute a critical time-sensitive target in the battlespace.

These and similar concepts will turn Airmen from thinking in an airpower-centric way to an airpower-optimized way, a distinction that looks to other domains to achieve airpower goals. Looking at practical means to implement integrated command has led to new organizational concepts such as the all-domain operations capability (ADOC) and to the use of the Common Mission Control Center (CMCC).[13]

---

10. Department of the Air Force (DAF), *The Air Force*, Air Force Doctrine Publication (AFDP) 1 (Maxwell AFB, AL: Curtis LeMay Center for Doctrine Development and Education [LeMay Center], March 10, 2021), 13, https://www.doctrine.af.mil/.

11. HAF, Deputy Chief of Staff for Strategy, Integration, and Requirements (A5/7), *Doolittle 2022: Command and Control Concept Primer* (Washington, DC: HAF, February 2022), 3.

12. HAF, Doolittle 2022 – C2 Workshop and TTX, April 2022, 10.

13. HAF, A5/7, *U.S. Air Force Concept Exchange: Enabling Concept for Integrated Command* (Washington, DC: HAF, June 2022), 10; Miranda Priebe et al., *Multiple Dilemmas: Challenges and Options for All-Domain Command and Control,* RR-A381-1 (Santa Monica, CA: RAND Corporation, 2020), 92, https://www.rand.org/; and Air Combat Command, *Common Mission Control Center (CMCC) Concept of Operations*, December 2022.

In 2021 and 2022, air components experimented with the ADOC concept. For example, Exercise Keen Edge 21—a US Indo-Pacific Command exercise—engaged this concept by standing up the air operations center as an all-domain operations capability to see how an air component could synchronize Joint functions in forward locations.[14] Other air components have explored scenarios where the AOC would become the ADOC and command and control all-domain fires for a specific phase of a Joint operation, such as the takedown of enemy air defense systems during a campaign's opening phase.

Defining future control and command authorities will be critical in identifying ADOC form and function since its ability to direct multidomain and multiservice capabilities will be central to its existence. As both Keen Edge and the Chennault games demonstrated, a solid definition of ADOC structure, its several roles, and its placement within AOC echelons will be important discussion points. For example, will the ADOC merely take the place of the theater commander's Joint operations center? Or could all-domain operations capability be a distributed capability with nodes stretching from the forward edge of battle all the way to sanctuary in CONUS? If control shifts throughout the C2 structure, then how and when control is shifted requires more gaming and testing.[15]

An example of command and control from CONUS is the Common Mission Control Center located at Beale AFB, California. The CMCC was highlighted in recent exercises as a JADC2 enabler, most notably during US Indo-Pacific Command's biennial Joint field training exercise, Valiant Shield 2022. The CMCC is an advanced tactical battle management C2 prototype designed for use in a contested, degraded environment and intended to become a member of the theater air control system, the Air Force's mechanism for commanding and controlling airpower. During Valiant Shield, the center provided capabilities for improving critical C2 and battlespace awareness functions—including maintaining over-the-horizon target custody across distributed C2 nodes, decreasing the time required for electronic order of battle updates, and rapidly disseminating enemy locations to enable convergent fires.[16]

The Common Mission Control Center's access to higher security communication pathways enables it to leverage all-domain capabilities from the US Space Force and US Cyber Command with greater transparency than the AOC or, presumably, a forward-edge ADOC. As such, the CMCC could be a capability working for the air component to task space and cyber in conjunction with air maneuver and launder higher classification information derived from space and cyber in order to integrate it into the lower classification tactical fight as needed.

The reality of a contested, degraded, and operationally limited environment and the capability of new distributed C2 nodes mean the air component now needs to plan for

14. "USAF B-52 Bomber Conducts Simulated Hypersonic Kill Chain Employment," Air Force Technology, May 11, 2021, https://www.airforce-technology.com/.

15. HAF, Doolittle 2022 – C2 Workshop and TTX, April 2022, 10.

16. Air Force News, "Air Force Units Support Navy Valiant Shield Exercise," *Aerotech News* (blog), updated August 9, 2022, https://www.aerotechnews.com/.

C2 as deliberately as it plans for offensive counterair or ISR. The notion of distributed control, sensor-to-shooter connectivity, and integrating cyber and space with kinetics augurs for a reimagination of air operations center functions. Greater attention must be paid to C2 downstream from the AOC and the center's relationship not only to these distributed control nodes, but also to forward-edge Joint and partner-nation capabilities. Joint efforts at common data standards make a Joint integrated fire control network a reality where multiple fires can converge or deconflict at the speed of sensing.

With all this potential capability, it is tempting for many to dismiss the AOC and the operational level of war in favor of envisioned tactical omniscience. While this thinking is shortsighted in the context of a theater campaign plan, it is clear the air operations center has to change with the new environment. Operational-level C2 needs greater emphasis on commander's intent and conditions-based authority. In such an environment, the air component must give significant thought on how to plan C2 deliberately to operationalize distributed control.

AOC Challenges

Critics have pointed to the air operations center as being antiquated and poorly constructed when it comes to its incorporation of JADC2 and distributed control.[17] This line of criticism extends to the air tasking order (ATO) with its 72-hour timeline, often characterized as too slow, inflexible, and a model more fit for the late-twentieth-century Desert Storm fight than the twenty-first-century South China Sea operating environment. While many of these criticisms do not take adequate account of the inherent flexibility resident in the AOC's dynamic targeting and ad hoc tasking methods as well as the foundational importance of operational-level planning, the air operations center does have structural and cultural challenges that must be addressed as the United States embraces a JADC2 future.[18]

Kinetic bias. Air operations center and air component personnel have a bias toward bombs. While nonkinetic targeting certainly occurs today—and improves all the time—the comparative scale of thinking, planning, targeting, and weaponeering in today's AOCs is heavily weighted toward kinetics.[19] The deck is stacked against nonkinetic effects with culture, personnel, doctrine, and processes all weighing in favor of kinetic weapons delivered from air platforms.

Air component leaders are largely selected from fighter backgrounds, which compounds the bias under which knowledge and comfort with space, cyber, and other nonkinetics take

17. Hannah Terino, "Why the AOC Cannot Execute JADC2," Over the Horizon, July 19, 2021, https://overthehorizonmdos.wpcomstaging.com/.

18. David A. Deptula, "A New Battle Command Architecture for Joint All-Domain Operations," *Æther: A Journal of Strategic Airpower and Spacepower* 1, no. 1 (Spring 2022), 53, https://www.airuniversity.af.edu/.

19. *Chennault 2.0 After Action Report: Air Operations Centers and the Targeting Process in the United States Air Force* (Maxwell AFB, AL: LeMay Center, 2020), 4.

a backseat to the kinetic experience that shaped a leader's formative years. Being good at kinetic effects is not a bad thing, but in the context of evolving into an all-domain force, having leaders with such a strong domain bias is a challenge that must be addressed.

Battle rhythms. The kinetic bias is reinforced by the 72-hour air tasking order cycle, which was of course designed with aircraft firmly in mind. All-domain capabilities like cyber, space, and information operations do not necessarily conform to that 72-hour cycle and in most cases have planning timelines that extend well beyond this time frame. For example, the Chennault war games have considered how an eight-day nonkinetic effects (NKE) planning cycle might be merged with the ATO cycle.[20] This type of battle rhythm mismatch contributes to NKE being overlooked and usually not well integrated into air component planning and execution. When one considers Joint, interagency, and partner-nation planning timelines, the challenges of integration and utilization grow exponentially. Alignment of disparate planning processes and timelines will be a crucial task in moving JADC2 forward.

Airpower-centric. Air operations center personnel rarely have the knowledge and expertise to ask questions about Joint, all-domain, and partner-nation capabilities much less how to plan and coordinate their integration. Many Airmen come into the AOC with no Joint experience, and some are junior or even first-term Airmen. Their Joint thinking often consists of how to integrate service or partner aircraft and usually does not stray, for example, into how maritime or ground force operations could be used in lieu of airpower or in support of air maneuver. As a result, understanding of how nonairpower capabilities can achieve airpower goals is often not present or advocated within today's air components.

Lack of authorities. Lack of tasking authority over Joint, all-domain, and partner-nation capabilities is often the reason given for AOC kinetic bias, air-centric battle rhythms, and poor Joint perspective. Air operations center professionals often think in terms of "what is my ALLOREQ (allocation request)?" which comprises those sorties allocated to the air component from other services and partners for tasking on the air tasking order. This line of thinking is of course a single-domain dead end.

But it is certainly a fair point that AOCs should examine what authorities they need to be truly all-domain and where their relationship with nonairpower capabilities could be mission enhancing, given proper planning and synchronization. Many air component Airmen feel they must control something to employ it, but this self-limitation should be minimized. Borrowing authorities from the combatant command for a limited period or engaging in supported/supporting contracts with cyber- or maritime-enabling capabilities

20. *Chennault Event 4: Joint All Domain Operations: Integrated Tasking Order Design and Execution After Action Report* (Maxwell AFB, AL: LeMay Center, 2020), 20.

may be the avenue for greater AOC awareness, understanding, and authorities as the military grows into the JADC2 era.

Human-in-the-loop heavy. Much like the rest of the Department of Defense, the AOC has specialty systems with very few machine-to-machine connections. As a result, there are many humans-in-the-loop who must move information manually from application to application to enable the find, fix, track, target, engage, and assess (F2T2EA) process. This construct is a major contributor to friction and lack of speed in executing time-sensitive activities like dynamic targeting.

New AOC weapons system tools like Kessel Run have enabled the machine-to-machine transfer of data among its own library of applications, but it remains unable to ingest data from non-Kessel Run systems. Data from intelligence-related apps and air-mobility-related systems, all critical to AOC functions, have no machine-to-machine ties to Kessel Run. This gap necessitates human-in-the-loop entry of critical data, a process that is slow and prone to mistakes. The key to making JADC2 a reality will be developing Joint common data standards that allow "single input, multiple outputs." In other words, data is entered once and then proliferated to where it is needed across the system-of-systems via machine-to-machine connection vice human-in-the-loop data entry.

YESFORN. Machine-to-machine issues are further compounded by security and classification. The AOC lives on the Secret computer system, but many all-domain capabilities require the Top Secret or Special Technical Operations (STO) access of the Common Mission Control Center. This exacerbates the problem of integrating capabilities and planning cycles, contributing to what the Chennault series characterizes as "non-kinetic malfunctions."[21] Add partner-nation security, system requirements, and sharing, and the problem becomes exponentially more difficult.

At a minimum, AOCs need to communicate at a Secret-Releasable level to integrate their respective partner nations. As Commander, Air Combat Command General Mark Kelly says, we need to replace NOFORN (no foreign access) with YESFORN.[22] With security and classification there is no elegant or easy solution, but AOCs must strive to deliver a balance.

The Foundational Culture Layer

Joint all-domain command and control is so sweeping and ambitious that it can be overwhelming. The technological top of the pyramid seeks to change sensors, machine-to-machine interfaces, and data structuring, leading to an alteration of the pyramid's middle layer by changing the very nature of operational command and control as it is known. Many air components are well invested in ongoing ABMS technical develop-

21. *Chennault 2.0*, 1.
22. General Mark Kelly, USAF, conversations with author.

ment and working machine-to-machine information flow through a bevy of operational warfare applications. Equally critical will be ensuring the foundational layer by preparing Airmen cognitively and experientially to master the demands of JADC2. Air components can bring their organizations closer to this vision by focusing on people and fostering a JADC2 culture.

Cultural Basics

Organizational culture is the foundational layer to any transformation, including that of the air component. At its heart, JADC2 is intended to embrace Joint and partner-nation capabilities through lateral connectivity that enables practitioners to sense, make sense, and act as a unified whole. The necessity for this is not new. Joint and partner-nation integration was also important in the 2003 invasion of Iraq. But 20 years of low-intensity conflict have ossified conventional forces and created low-tempo stovepipes. The need for Joint and partner-nation integration is as important today as it was in 2003. The only difference now is without truly radical integration, the risk involves not just losing a regional conflict of choice but also losing a great-power war of necessity.

The recommendations below are neither radical nor revelatory when taken separately, but the whole is greater than the sum of its parts and represents a significant shift in approach. The Air Force's Operational Command Training Program often finds organizational excellence is not an act of discovery but one of remembering. Organizations need to be reminded to apply the basics in changing culture. This involves leadership emphasis, training, and a frank commitment to repetition that builds muscle memory.

In particular, the Air Force should focus on building the cultural basics, namely the values, expectations, and practices of the organization. For JADC2, values, expectations, and practices should center on 1) partnering airpower and nonairpower teams and organizations; 2) building all-domain relationships; and 3) conducting frequent battle drills to turn these teams, organizations, and relationships into processes that enable a well-rehearsed kill web. In this way, air components can begin to truly integrate nonairpower capabilities such as space, cyber, and information, as well as Joint and partner-nation capabilities.

Building relationships with those all-domain counterparts, understanding their capabilities and timelines, and practicing how to meld those fires must be done now during precrisis. Attempting to do this as crisis or war develops is simply too late. A JADC2 culture is one that places a premium on curiosity, learning, and engagement with those outside the organization. JADC2 requires air components to be value-embracing and domain-agnostic partners, focusing on the kill web and seeking machine-to-machine connection.

Being culturally partner focused and domain agnostic for JADC2 means first having a Joint outlook. The air component is the Air Force's Joint interface. Despite the importance of this connection, it is rare to find air component Airmen who have Joint experience.[23] This commonly results in staff cultures that think almost solely in terms of Air Force capabilities and kinetic bias. JADC2 demands practitioners think in a multidomain manner, similar to a Joint task force. Airmen must understand Army, Navy, Special Operations, and other capabilities and the tasking processes associated with their platforms, fires, intelligence, communications, targeting, and other aspects:

> Practitioners of [operational-level] C2 must be able to think beyond their tactical "family of origin" weapons systems and understand how the various joint and coalition forces can fit together into a coherent scheme of maneuver. Air planners in the [AOC] are specifically trained in the joint operation planning process for air but also support the parallel joint operation planning process performed by JTF headquarters. Thus, they must be familiar with multiple joint and functional operational-art concepts, doctrine, and terms.[24]

Fostering a culture of JADC2 means fostering a Joint task force culture where land, cyber, and maritime capabilities come to mind just as easily as airpower when working to solve problems. This emphasis must demand face-to-face interaction and relationship building with Joint counterparts; understanding of each other's capabilities and processes; and finding ways, at the lowest possible level, to integrate and synergize together. This could mean establishing dynamic targeting drills, planning multidomain ISR campaigns, or assigning officers from other services to air component billets.

And once Airmen find those points of integration and synergy with nonairpower partners, they should conduct frequent Joint battle drills to build muscle memory among the staffs. The importance of these frequent battle drills conducted alongside Joint partners cannot be overemphasized. Thinking like a Joint task force during precrisis, connecting Joint teams, and having relationships of trust forged over frequent battle drills is a precondition for JADC2 success.

Partner Nations

Being culturally partner focused means embracing key Allies and partners that share US objectives. Partner nations may bring exquisite capabilities and enabling authorities that allow them to achieve common goals easier and faster than the air component. As with Joint counterparts, Airmen must be educated on partner capabilities, understand their tasking (or asking) processes, and build personal relationships that become stronger with frequent battle drills.

Beyond aircraft, air component Airmen should be knowledgeable of partner-nation specialties and accesses, whether that be cyber, human intelligence, maritime, or publicly

---

23. Adam J. Hebert, "USAF Evaluating When Joint Experience Should Equal Command Experience," *Air and Space Forces Magazine*, September 20, 2017, https://www.airandspaceforces.com/.

24. Dave Lyle, "The Rest of the C2 Iceberg," *Air & Space Power Journal* 28, no. 4 (Summer 2014), https://www.airuniversity.af.edu/.

available information. Building this precrisis relationship, however, is complicated by additional challenges of technical interoperability and foreign disclosure. The team building that comes from frequent integration is commonly hampered by inadequate means to collaborate.[25]

Air components should strive to have robust video teleconference and chat connectivity with partners, in addition to common systems, partner networks, and voice lines. Yet having robust communication networks is not merely a checklist item. Those communications must be relevant and used frequently. These partner communication nodes should be persistently energized by Airmen in pushing integration to the lowest level during day-to-day operations and not just during exercise events.

Compounding the problem of partner integration is the difficulty of foreign disclosure. During every single crisis, the imperative to share with partner nations is paramount. Yet the number of foreign disclosure officers and prearranged, fast-moving sharing arrangements are often lacking in such crises.[26]

JADC2 culture will demand radical sharing with partner nations, and this means attacking the sacred barriers that well-meaning security professionals emplace—something that may be prosecuted best when the sharing demand signal emerges locally. The portrayal of Top Secret/Sensitive Compartmented Information on the AOC operations floor with partners working alongside US Airmen, for example, may have been unthinkable in previous times, but this situation will likely become a necessity if the United States is to win a future great-power conflict. The Air Force must thus insist on robust and technically redundant communications that make partner-nation communication routine, low level, and preferably face-to-face.

Domain Agnostic

Nonkinetic effects. The imperative to connect teams, build relationships, and drill battle operations applies especially to the integration of nonkinetic effects. The timelines and authorities for NKE are significantly different than those involved with kinetic effects. Familiarity and practice with these processes must occur in precrisis to be ready for war. Building a platform-agnostic culture familiar with cyber and information warfare requires employing and planning those fires as part of today's real-world, great-power competition, and not just notionally or during exercises.

For example, air operations centers that develop specific offensive cyber operation concepts of operation (CONOPs) during precrisis must assign caveats to their work because air components do not have the authority to approve cyber fires. This authority is retained by US Cyber Command and its subordinate elements and is coordinated through the

25. Lucas Thoma, "There's a Big Problem Limiting US Interoperability with Allies: Here's How to Fix it," Modern War Institute, February 18, 2021, https://mwi.usma.edu/.

26. David Ellison and Daniel Vardiman, "Ukraine Lessons for Naval Intelligence's Next War," *Proceedings* 148, no. 10 (October 2022), https://www.usni.org/.

theater combatant command.[27] Despite this, AOCs that develop offensive cyber CONOPs can create an education tool for air component personnel, a focal point for kinetic and NKE planners, an expected plan of action for combatant commands, and a clear intent for functional elements within the cyber fires chain—all of which will likely result in a cyber capability more readily integrated with air maneuver.

Another example would be air component personnel employing real-world multidomain ISR packages or multidomain flexible deterrence options alongside Joint and partner-nation cyber or information warfare planners during precrisis competition activities. This would build the practical experience and organizational relationships that can be leveraged in wartime. Seeking battle drills in the use of NKE and embedding with partner-nation cells for real-world planning and execution will create well-worn paths for domain-agnostic fires in wartime.

Globally integrated operations. Joint all-domain command and control demand for an all-domain outlook will encourage Airmen to seek solutions to airpower problems outside of the air component and even outside of theater geographical boundaries. Airpower targets may reside in the cyber and space domain, outside the physical reach of airpower kinetic effects, or beyond an area of responsibility. As such, the target may not be prosecutable on that AOC's air tasking order. Many legacy-minded Airmen conclude that just because a target cannot be serviced by their ATO, it is not their job. But in this era of globally integrated operations, all combatant commands (and their air components) work together to target the enemy despite geography or domain.

In the JADC2 culture, an air component working a target of interest that it cannot action by itself will still invest in the detailed analysis of that target's critical vulnerabilities, if only to effectively lobby for its inclusion on another combatant command's or partner nation's Joint target list. JADC2-cultured Airmen will instinctively reach into the realm of globally integrated operations and understand the reach and capability of US Cyber Command or US Space Command as they seek any means necessary to deliver effects to the enemy.

Kill Web

Embrace it. The point of being culturally partner focused and domain agnostic is to obtain greater efficiency and effectiveness in killing the enemy. Embracing the kill web means embracing intelligence, surveillance, and reconnaissance, which for air components means the distributed common ground system (DCGS). Until a few years ago, the DCGS was solely focused on the exploitation of raw intelligence gathered by airborne ISR. In January 2020, the 480th Intelligence Wing launched "DCGS Next Gen," which

27. DAF, *Cyberspace Operations*, AFDP 3-12 (Maxwell AFB, AL: LeMay Center, February 1, 2023), https://www.doctrine.af.mil/.

emphasizes platform-agnostic deep analytical support to the air component.[28] This support comes in the form of analyst exploitation teams that focus on air component intelligence problems requiring deep expertise.

DCGS has leaned into the advanced battle management system and JADC2 writ large by focusing on data services and enabling common intelligence picture and common operating picture capabilities that contribute to rapid OODA loops. The DCGS is also heavily invested in the sensing grid. The system is developing intelligence applications for rapid targeting and long-range kill-chain concepts, making it the fusion engine for JADC2 as the key enabler speeding decisions associated with the kill web. Thus, JADC2-cultured Airmen will be more knowledgeable of DCGS activities and will seek its inclusion in major exercises, battle drills, and flexible response options.

Drill it. Connecting organizations, building relationships, and battle drilling together form the sinews of Joint all-domain command and control. If these are done purposefully and habitually, muscle memory will form and the processes that enable fighting at speed and scale in all domains will come into sharper relief. JADC2 technical development traces the flow of machine-to-machine information from application to application and sensor to shooter. The JADC2 human dimension, however, needs to trace the flow of kill-web information through those processes. By frequently conducting battle drills together, Airmen with all-domain teammates will better identify the most effective paths and flows to integrate the all-domain kill web.

Finding the best paths and flows should be done from the bottom up, but Airmen need repetitions to discover them. Dynamic targeting experiential training, for example, is obtained via Blue Flags or the Neptune series' exercises. But these events are few and far between, taking place every 18 to 24 months. This is too infrequent to build organizational muscle memory. JADC2 cultures are created by air components that develop their own process for frequent battle drills and genuinely test their kill webs. An example of this is the F2T2—find, fix, track, target—which is the first part of the Air Force kill chain F2T2EA, minus the engage and assess. These are self-generated drills that practice an actual, not simulated kill web conducted with, for example, maritime and ground surface fires, partner nations, and all-domain capabilities like cyber.

Some air components employ F2T2s by using multidomain ISR packages against real-world targets, and the intelligence obtained drives multidomain targeting processes. Operational and tactical C2, machine-to-machine data sharing, service component procedures, and all-domain planning considerations are all exercised against a real, breathing, moving target with a mind all its own. The F2T2 drill initiative described above is ingenious because it combines real-world requirements with actual Joint/Allied/all-domain targeting processes and can occur many times a year. This type of frequent battle drill

28. Kelly Borukhovich and Tyler Morton, "DCGS Next Generation: Accelerating Change to Deliver Decision Superiority," Over the Horizon, September 26, 2020, https://overthehorizonmdos.wpcomstaging.com/.

finds JADC2 kill paths that are intuitive. JADC2 technology should not drive these kill-web processes. The lower and middle echelons of the air operations center are perfectly able to determine the right path when informed by all-domain and partner-nation understanding, integration, and frequent battle drills.

Connection-Driven

The sensing grid of the fully formed JADC2 construct assumes machine-to-machine lateral connections sharing data between many platforms at speed and scale, but this is clearly not a reality today.[29] Despite this shortfall, it is critical for Airmen building a JADC2 culture to seek ways for machines to connect and bring down barriers to data sharing. For example, during Joint Task Force Haiti relief operations in the summer of 2021, the Air Forces Southern Joint air component coordination element connected the radar picture emanating from maritime vessels for display in the AOC. Several communicators from both the air and maritime domains had to work together, and within a day or so, the radar picture became completely integrated.[30]

When JADC2 fully matures, this will occur automatically, but today it may require senior leader emphasis in order to happen. It is important for leaders at all levels to set the expectation that Airmen must always strive to identify barriers and work ties with Joint and partner-nation members regardless the topic. Whether it be for radar feeds or intelligence collection, these connections will prove foundational to JADC2 success.

Red dot tests are useful tools that both Pacific Air Forces and US Air Forces in Europe have used to trace machine-to-machine connections in their F2T2EA kill chains. The red dot chart traces the flow of data from ISR sensor to tactical shooter and all the intelligence and operations applications in between. The chart displays every occurrence in which a human-in-the-loop must manually transfer information from one application to another, each annotated with a red dot.

Looking at the number of red dots on the kill web gives a quantitative list of data connections that need automation. Red dots get removed every time machine-to-machine connections are crafted by software developers. The red dot test is an effective mechanism to identify and quantify analog connections, enabling air professionals to think more clearly about the machine flow of their data. Because of this, "single input, multiple outputs" should become the focus for most JADC2 culture-savvy Airmen.

An air component culture that is partner focused, domain agnostic, kill-web embracing, and connection driven will offer the rich soil in which JADC2 can take root. Building culture means taking action, and leaders should focus on ensuring connections, developing relationships, and demanding battle drills as they form the necessary foundational

29. Greg Hadley, "ABMS Will Need 'Continuous Improvement,' Will Never Be a 'Shiny' Finished Product, General Says," *Air & Space Forces Magazine*, September 21, 2021, https://www.airforcemag.com/.

30. Observed by author during Operational Command Training Program mission supporting Air Forces Southern at Joint Task Force Haiti, Homestead ARB, Florida, July 2021.

layer of the JADC2 pyramid. Focusing on building that culture now will help guide development of JADC2 technology and deliberately plan agile command and control in a manner that is most beneficial to the kill web. And building the relationships, knowledge, and muscle memory with the Joint community, partner nations, globally integrated, operations-focused entities, and the distributed common ground system will posture the air component for success in any great power conflict.

Conclusion

Joint all-domain command and control is a pyramid with technology as the capstone. But JADC2 is more than a myriad of technological solutions. To be effective, the technology at the top must have a sturdy middle layer of command and control. This C2 may be both tactical and operational and must deliver agile control and integrated command where Airmen are not constricted to the air domain or tied to a single, platform-centric C2 node.

While these technological and C2 changes may come in the near future, the task the Air Force faces now is to build and mature the foundational layer of the JADC2 pyramid—that of culture. The organizational culture that underlies JADC2 is something Air Force leaders must address today. This change is underway, especially among younger members of today's air components who have generated innovations like F2T2s, all-domain CONOPs, publications that challenge doctrine, and new ways to structure the air operations center. Moving forward, it is incumbent upon the Air Force to build the air component organization in a way that will synchronize airpower with every other domain to make the collective set of OODA loops and associated effects generate in a manner that is markedly faster, flatter, and more efficient.

Empathy in the Foundations of Warfare

Jennifer Lee C. Rudolph

In letters to Airmen and changes to evaluation practices, and in the development of Airman leadership qualities, Chief of Staff of the Air Force General Charles Q. Brown Jr. and Chief Master Sergeant of the Air Force JoAnne S. Bass have charged Airmen to cultivate empathetic communication. Yet a gap exists between service doctrine concerning empathy and its practice through specific behavioral skills. Using a recent study, this article connects a learnable and teachable practice of empathy to improving Airmen's professional and personal lives. Learning and applying empathetic communication to the tactical, operational, and strategic levels of war prepare Airmen for the fast-paced and dynamic contexts of future complex warfare.

War, a complex, multifaceted continuum, consists of many foundational components, both explicit in doctrine and implicit in the large body of work dedicated to understanding how to conduct combat. Yet while comprehensive, the United States Air Force's current framework for future complex warfare lacks a foundation in empathetic behavior. As an ever-modernizing force in the profession of arms, the service must fill the gap between empathy in doctrine and empathy in practice as Airmen prepare for and execute future warfare. Building empathy into the foundation of warfare is important for two reasons. First, learning empathetic behavioral skills will improve relationship building in Airmen's personal and professional lives. Second, an enhanced capacity for empathy is a skill that will be required of Airmen in future complex war.

Understanding and applying empathy pertains to many audiences, from individual Airmen as practitioners, to content developers for resiliency programming, to Air Force senior leaders interested in driving cultural change. Small teams and individual leaders may already be implementing empathetic communication, the practice of interacting with others with an awareness and understanding of their feelings and perspectives. But such an important skill should be more commonly taught, learned, and practiced in the service.

The significance of empathetic communication is demonstrated through a 2022 qualitative research study involving members of the Michigan Air National Guard. The study's findings on reflective listening—a technique used in empathetic communication that involves understanding the speaker and reflecting this understanding back to them—reveal several insights into the benefits of this kind of communication, the

---

Major Jennifer Lee C. Rudolph, USAF, executive officer for the 110th Wing, Kellogg Air National Guard Base, Battle Creek Michigan, holds a master of public administration from American Military University and a master of military art and science as an Art of War scholar from the US Army Command and General Staff College.

potential gap between current Air Force doctrine and the practice of empathy, and the importance of the methods used to train personnel.[1]

While empathetic communication, which includes reflective listening, requires awareness of the situational context, teaching, learning, and practicing this skill could enable effective interpersonal relationship interactions before and when Airmen enter high-stress, high-tempo, and high-visibility situations that require much different communication styles.

The Roots of Empathy in Warfare

Although empathy may seem to run counter to the conduct of war, it is an enduring and universal concept with roots in ancient warfare. Chinese military philosopher Sun Tzu clearly understood the importance of empathy, writing "know the enemy, know yourself; your victory will never be endangered."[2] Sun Tzu's idea of knowing oneself applies to the leader, the troops, and the allies. Moreover, he advises this is half the equation to battlefield success.[3] Successful leaders use their foundation in empathy to know those who serve with, above, and for them to plan and execute war and achieve their missions.

Empathy has many definitions arising from its multidisciplinary use and application. This article is grounded in the military concept of empathy, which the Air Force defines as being "understanding of and sensitive to another person's feelings, thoughts, and experiences to the point that you can almost feel or experience them yourself."[4] This cognitive awareness is the first part of developing a behavioral response to demonstrate empathy toward others, particularly in empathetic communication and relationships.

The connection between empathy in doctrine and empathy in practice existed in previous versions of leadership manuals, even if the service did not explicitly invoke the word itself. The first Air Force leadership manual distinctive from the Army is one such example.[5] The 1948 version of the Air Force Manual 35-15 *Air Force Leadership* states, "To learn [the Airmen's] individual differences and characteristics together with the common desires and aspirations, you must spend much time with them," and "concern for, and assistance with, the personal problems of your men will permit you to know them and will give them recognition."[6]

1. Jennifer Lee C. Rudolph, "Tell Me More: A Qualitative, Bounded Case Study on Reflective Listening" (master's thesis, US Army Command and General Staff College, 2022).

2. Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (London: Oxford University Press, 1963), 129.

3. Sun Tzu, 129.

4. Department of the Air Force (DAF), *DAF Air Force Handbook* (AFH) 1 (Washington, DC: DAF, October 1, 2017), 256, https://books.google.com/.

5. Curtis LeMay Center for Doctrine Development and Education (LeMay Center), *Volume II: Leadership* (Maxwell AFB, AL: LeMay Center, November 4, 2011), 34, https://www3.nd.edu/.

6. DAF, *Air Force Leadership,* AFM 35–15 (Washington, DC: DAF, December 1948), 22–23, https://books.google.com/

Yet although Air Force doctrine has contained references to empathy since 1948, even in the updated 2021 version of the Airman's Handbook, the word itself occurs infrequently.[7] Interestingly, "empathic" communication is "useful when communication is emotional or when the relationship between speaker and listener is just as important as the message," yet somewhat contradictorily, it is the prerequisite to informational or critical listening, the two other types of listening described previously in the document.[8] A junior Airman understandably may view empathic listening as less important as the other two types of listening. The Airman's Handbook could thus benefit from emphasizing and explicitly connecting behavior that demonstrates empathy to solidify this foundation.

One way to break down empathy is through a behavior such as reflective listening. Table 1 provides examples of five reflective listening skills. Reflective listening is a multidimensional skill that enables empathy through attentive behaviors, verbal and nonverbal acknowledgments, phrases to encourage other-centered conversation, silence, and reflective responses to validate understanding.

These specific behavioral skills are learnable and teachable for Airmen at all levels, but behavioral change is not always easy, nor does it occur without creating new habits. Importantly, the term reflective listening is preferred over the term active listening. Whereas active listening requires a response from the listener, reflective listening, in the ways and for the reasons described above, distinguishes and emphasizes repeating and validating the message received in the communication cycle.

Table 1. Reflective listening examples[9]

Behavior	Definition	Example
Attending verbal/nonverbal	Being fully present through posture, gestures, and attention	Eye contact, open body posture, nodding, leaning forward, giving full attention, being present within
Acknowledgments	Verbal and nonverbal communication that assures attention	Verbal: "uh-huh," "really," "no kidding!," "that's interesting...," "yes, I see..." Non-verbal: head nods, expressive eyes
Door openers	Other-centered conversation that encourages the other to talk (not filling the listener's need for information)	"Go on..." "tell me more..." "sounds like you have something to say..." "talk more about it!" "Share more about that...," "I'm listening…"

7. DAF, *Airman* AFH 1 (Washington, DC: DAF, November 1, 2021), 319–20, https://static.e-publishing.af.mil/.

8. DAF, *Airman*, 2021, 320.

9. Adapted from Rudolph, "Tell Me More," 3, table 1; Chapman Foundation for Caring Communities, Our Community Listens training (St. Louis, MO: Chapman Foundation., n. d., accessed March 20, 2023); and see also "Learn to Connect," Chapman Foundation for Caring Communities (website), accessed March 20, 2023, https://www.chapmancommunities.org/.

Behavior	Definition	Example
Silence	Quieting the mind and the voice	Being silent internally and externally
Reflective responses	Conveying understanding facts and feelings to the other as experienced by the other (not inattention, parroting, or paraphrasing)	"Sounds to me like…[facts and feelings of the other]" "What I hear you saying is…[facts and feelings]" "It seems like you are [a feeling word] about [the factor or issue]…"

Empathy across Levels of War

The levels of warfare as defined in Joint doctrine are useful to explore the ways empathy could impact Airmen.[10] Figure 1 depicts how leaders can use empathy as they execute their missions. The applications of empathy at each level listed below are not all-inclusive, and the building-block approach demonstrates that empathetic communication skills can reinforce leadership and relationships at higher levels.

While strategic or operational leaders may have a different focus at the national or campaign level, they rely on their tactical empathetic communication skills to develop their teams and workplace cultures. As the sections below demonstrate, the notion of empathy can be found explicitly or implicitly in service and Joint doctrine, but a gap in implementing successful programs, at least throughout the Air Force, provides opportunities to learn and teach behavioral skills in empathetic communication.

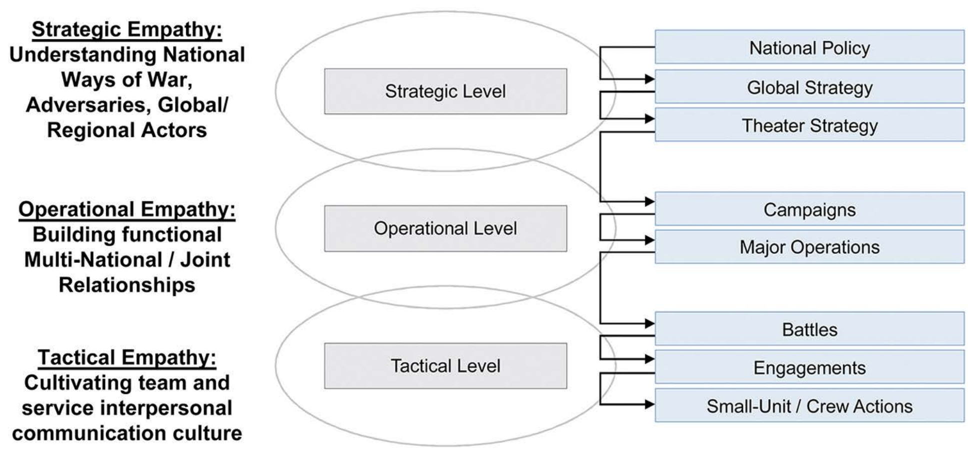


Figure 1. Levels of empathy aligned with levels of leadership

10. Chairman of the Joint Chiefs of Staff (CJCS), *Doctrine for the Armed Forces of the United States*, Joint Publication (JP) 1 (Washington, DC: CJCS, Incorporating Change 1, July 12, 2017), 1-7, https://irp.fas.org/.

Tactical

In the tactical level of war, "battles and engagements are planned and executed to achieve military objectives assigned to tactical units or joint task forces."[11] Here, empathy can arise in the context of the interaction of members on small teams. Empathy may also emerge in interactions between members of a particular military service's culture or between US military service cultures.

Disciplines such as negotiations and psychology employ the concept of tactical empathy. For example, scholars of negotiation have defined tactical empathy as related to accurately understanding and communicating "the emotional obstacles and potential pathways to getting an agreement done."[12] But empathy at the tactical level is not found in common parlance in the military.

As indicated above, the Air Force does address empathy in doctrine and leadership principles.[13] The service's recently revised "Brown Book" is the "foundation for the enlisted force to meet mission requirements and individual Airman proficiency and competency development."[14] Desired leader qualities that help gain respect intentionally include empathy: "credibility, a positive influence on others' self-awareness, cultural awareness, and *empathy* [emphasis added]."[15]

Joint doctrine also discusses the importance of empathy at the tactical level. In the Joint Staff publication *Developing Enlisted Leaders for War*, emotional intellect is defined as "having keen self-awareness with the ability to connect, empathize, and understand people and cultures."[16] This form of empathy is internal—an individually developed quality—and is required within a military organization to accomplish mission success.

Operational

The operational level "links strategy and tactics by establishing operational objectives needed to achieve the military end states and strategic objectives."[17] Operational empathy can include building relationships with multinational Allies and partners and between

---

11. CJCS, JP 1, I-8.

12. Chris Voss and Tahl Raz, *Never Split the Difference: Negotiating as If Your Life Depended on It*, 1st ed. (New York: Harper Business, 2016), 73.

13. Department of the Army (DA), *Army Leadership and the Profession*, Army Doctrine Publication 6-22 (Washington, DC: DA, July 2019), 46, 50, https://armypubs.army.mil/; Department of the Navy (DoN), *Navy Leader Development Framework: Version 3.0* (Annapolis, MD: DoN, May 2019), 7, 10–11, https://media.defense.gov/; and Headquarters US Marine Corps (USMC), *Leading Marines*, Marine Corps Warfighting Publication 6-11 (Washington, DC: Headquarters USMC, November 27, 2002), 31, 69, 96–99, https://www.marines.mil/.

14. USAF, *The Enlisted Force Structure* ("Brown Book") (Washington, DC: DAF, May 16, 2022), 3, https://www.doctrine.af.mil/.

15. USAF, *Enlisted Force Structure*, 8.

16. CJCS, *Developing Enlisted Leaders for Tomorrow's Wars* (Washington, DC: CJCS, 2001), 2, https://www.jcs.mil/.

17. CJCS, JP 1, I-8.

military services. As a NATO report recommends, "the motivation to understand and be understood . . . can create positive attitudes toward other cultures, empathy, and social relaxation, all of which will aid communication."[18] Operational empathy is a lateral empathy necessary to accomplish military goals with Joint and multinational partners and Allies.

Strategic

Strategic empathy is about understanding global actors—adversary or neutral—and includes concepts like national ways of war and "strategic objectives in support of strategic end states."[19] One scholar defines strategic empathy as "stepping out of our own heads and into the minds of others. It is what allows us to pinpoint what truly drives and constrains the other side."[20] Strategic empathy is external empathy required to accurately understand the meaning of what global or regional actors and nations do. Operational and strategic levels of leadership as described above require a foundation in empathy, a skill which can be learned and taught, as demonstrated in the empathy study discussed below.

These tactical, operational, and strategic frameworks create the foundation for examining empathy doctrinally. The next challenge is how to learn it and teach it to Airmen. The results from a 2022 qualitative bounded case study conducted at the US Army's Command and General Staff College provide valuable insights into this process.[21]

Empathy Study

People represent the first priority for most every Air Force commander. While empathy is critical for teams, problem-solving, and organizational relationships, empathy is just as, if not more, important for what it can do for the professional and personal development of Airmen in the service's span of care. Indeed, this critical component of emotional intelligence that meaningfully shapes familial relationship support can be considered one important predictive element of career success.[22]

Between 2017 and 2022, approximately 110 Airmen—4 percent of the Michigan Air National Guard—attended a three-day empathetic communications course offered by a

---

18. NATO and Research and Technology Organisation (RTO), *Multinational Military Operations and Intercultural Factors*, RTO Technical Report, TR-HFM-120 (Neuilly-sur-Seine Cedex, France: NATO Research & Technology Organisation, November 2008), 6-14–6-15.

19. CJCS, JP 1, I-7.

20. Zachary Shore, *A Sense of the Enemy: The High Stakes History of Reading Your Rival's Mind* (Oxford: Oxford University Press, 2014), 2.

21. Rudolph, "Tell Me More."

22. Itziar Urquijo, Natalio Extremera, and Garazi Azanza, "The Contribution of Emotional Intelligence to Career Success: Beyond Personality Traits," *International Journal of Environmental Research and Public Health* 16, no. 23 (November 2019), https://www.mdpi.com/; and Lesley Verhofstadt et al., "The Role of Cognitive and Affective Empathy in Spouses' Support Interactions: An Observational Study," *PLOS ONE* 11, no. 12 (February 2016), https://doi.org/.

third-party nonprofit organization, Our Community Listens. The in-person course sought to teach Airmen specific behavioral skills to demonstrate empathy and provide a framework for effective confrontation.

For the March 2022 study, members of the Michigan Air National Guard who had attended the course shared their experiences, including what learning reflective listening was like, how their reflective listening behavior changed, how reflective listening impacted their demonstration of empathy, how their military work environment changed, and how reflective listening met or did not meet their expectations. The participants provided examples where they used reflective listening or experiences they wanted to share.

Ultimately, their reflective listening yielded a more accurate understanding of others, enabling them to demonstrate perspective taking, or seeing the other person's point of view. When the participants avoided problem-solving as their first response, they realized that reflective listening often provided new and more complete information upon which to make follow-on decisions within their interpersonal interactions. Then, during an other-centered conversation, they found the new information allowed them to conceptualize more effective or different solutions than they had initially envisioned at the outset of the conversation.

Study participants' experiences with reflective listening provided insights into when, where, why, and how Airmen used reflective listening. The semistructured interviews and subsequent cycles of coding revealed relevant themes. One significant insight that emerged from this research is that empathy is a skill that can be taught and learned.

First, facilitators presented common behaviors that might seem like connecting with others: asking questions to satisfy personal curiosity or a need for information, telling one's own story, and giving advice. Although such behaviors appear to promote empathy, they tend to focus the conversation on the listener's needs and not the speaker's. The potential issue is making the conversation self-centered (listener) instead of other-centered (speaker), which is the aim of empathetic communication. Second, the facilitators presented the alternative behaviors surrounding reflective listening, such as attending verbal/nonverbal behavior, and offering attention acknowledgments, door openers, silence, and reflective responses (see table 1).

During the next portion of the course, participants split into small groups for role-playing scenarios to practice the behaviors, while facilitators provided feedback that could demonstrate empathy and put the conversation back in the other person's hands. This experience of learning a behavioral skill and practicing with facilitator feedback led members on a journey experimenting with self-regulating their behavior when listening to others.

At the end of the day, facilitators encouraged participants to practice and experiment with reflective listening with someone in their span of care. Based on end-of-course surveys, reflective listening significantly impacted members during the course. In three sequential iterations of the course, 100 percent of participants identified reflective listening as the most important skill in the course, and 62 percent reported that reflective listening was the skill they made a personal commitment to adopt.

Learning an individual behavioral skill such as reflective listening thus develops a foundation in empathy, creating a practice that an Airman in a leadership position can incorporate while serving at any tactical, operational, or strategic level. This other-centered finding supports the Airmen leadership qualities and foundational competencies found in the Brown Book.[23] Figure 2 situates tactical, operational, and strategic empathy with the leadership performance and developmental areas. The continuum of development implies that qualities and competencies learned at the foundational level contribute to and enhance the advanced level. Training transfer, therefore, is an important component of building a foundation of empathy in warfare.

In the study discussed, participants described transferring their skills from the training environment to various other aspects of their life. They also transferred empathetic communication skills from the classroom to their military and civilian workplaces. Applying these skills outside of a military setting is particularly important to members of the National Guard, who must continuously navigate between military and civilian spheres.

Figure 2. Levels of empathy coupled with the Airmen leadership qualities and Air Force foundational competencies

Reflective listening as a behavioral skill for empathy, therefore, has the potential to impact many different areas of an Airman's personal and professional life. This impact suggests there could be other areas where practicing reflective listening in empathetic

23. USAF, *Enlisted Force Structure*, 23.

communication at the tactical level could be applied, namely to the operational and strategic levels of warfare, creating the empathetic, self-aware, and other-aware Airmen needed for future complex warfare.

Findings and Recommendations

Benefits of Empathy

The participants in the study discussed above became empathy practitioners in their most valued relationships: they demonstrated empathy to the people in their span of care—their coworkers, their families, and their children, and members of their community. Study participants listened when a coworker experienced a death in the family, they released themselves from the burden of solving others' problems, and they had a common language to explain their feelings to their spouses and families. Moreover, participants reported they found others responded by communicating freely in ways that were different than before.

Gap between Doctrine and Practice

Clearly, the time is right to pivot toward including specific behavioral skills for empathy in Air Force resiliency programs, Airmen and family readiness resources, and base- and wing-level programs. Air Force Chief of Staff General Charles Q. Brown Jr. and Chief Master Sergeant of the Air Force JoAnne S. Bass called for empathetic communication in a 2022 memorandum, acknowledging it as a continuous practice and stating that "building trust and belonging is never a one-time event—*it is a daily commitment to those we serve* [italics in original]."[24]

The roots of empathy exist in their ideas to start connecting and engaging with Airmen, such as "shar[ing] perspectives and life lessons." In their directive, CSAF Brown and CMSAF Bass call on Air Force leaders to purposefully incorporate empathy in their interactions: "It must be intentional at every level to create trust and belonging. During these moments, we will continue to be open, show consideration, value differences, and seek to understand multiple perspectives."[25] In order to ensure a daily, long-term practice, the implementation of empathetic communication training must be intentional and consistent.

Teaching and Learning Empathy—Reflective Listening

The study of empathy in the foundations of warfare offers opportunities to further determine and refine how and when empathy can develop Airmen of the future. The Department of the Air Force can benefit from a targeted look into the many current

24. Charles Q. Brown Jr. and JoAnne S. Bass, "Airmen's Time," memorandum (Washington, DC: DAF, April 2, 2022), https://www.resilience.af.mil/.

25. Brown and Bass, "Airmen's Time."

communication courses such as Our Community Listens for ways to implement empathy training. Empathy is a challenging area of interpersonal communication, one that takes personal practice, trial and error, experimentation, and self-regulation of emotion—all added to the current burdens of communication and leadership during today's fast-paced environment. Now is the time to provide tangible, effective training to Airmen at all levels and at all points of their careers to create or reinforce their empathy foundations.

As the Michigan Air National Guard study revealed, reflective listening is one method of teaching empathetic communication. In the 1970s, psychologist Carl Rogers first explored engaging in reflective listening during psychotherapy sessions where he highlighted the importance of validating communicated feelings as both received and understood as the individual has intended.[26] This other-oriented conversation forms the foundation of Rogers' contributions to the field, which extend far beyond psychotherapy and can be traced from his concepts of reflective listening and active listening to many interpersonal and leadership concepts today.

Deconstructing empathy into a behavioral skill is equally as important as the methodology of the training. Participants observed that Our Community Listens was different and unique in concept and practice from other communications training they experienced.

First, members felt attending a communications course focused on listening instead of speaking differed from their previous communication training experiences. Practicing the skill in class with instructor feedback went beyond lecture-style training on leadership concepts, creating a motivational effect among members. Finally, the continuous-learning framework of Our Community Listens facilitated empathetic behavioral skills after the course was over. These insights inform three recommendations for nearly any kind of training the Air Force pursues but are particularly important for teaching empathy.

Recommendations for Empathy Training

Combined Adult Learning Model

During the course, members experienced a combination of interactive and experiential learning when they learned, practiced, and experimented with reflective listening. This combination is the key aspect of successful adult learning models.[27] A combined approach to empathy training could engage the three adult learning theories identified by the US Department of Education's Teaching Excellence in Adult Literacy: 1) engaging andragogy—the art and science of adult learning—to explain why learning empathy is important in a personal and professional context and reinforcing empathy learning with

26. Erik Rautalinko and Hans-Olof Lisper, "Effects of Training Reflective Listening in a Corporate Setting," *Journal of Business and Psychology* 18, no. 3 (March 2004), https://www.jstor.org/.

27. Cynthia Benn Tweedell, "A Theory of Adult Learning and Implications for Practice," paper presented at the Annual Meeting of the Midwest Educational Research Association, Chicago, IL, October 25–28, 2000, https://files.eric.ed.gov/.

skills and feedback; 2) providing a framework for self-directed learning to allow the member to choose what empathy skills to incorporate and how to incorporate them in their daily life; and 3) including concepts from transformational learning to create an environment that encourages learners to explore multiple points of view.[28]

Opportunities to Practice and Experiment

Applying a new perspective to listening means forming new habits. Study participants felt this application of empathy was unnatural at first, because in order to wait patiently and listen reflectively, they had to self-regulate preexisting, entrenched habits. Participants also often felt as though the speaker did not anticipate an other-centered conversation, perceiving that strangers and family members alike were expecting different behaviors from them. Evolving their reflective listening and empathy to a new normal came after practice and feedback both inside and outside the classroom. More interestingly, when participants learned reflective listening and adopted empathy, they felt responsible for demonstrating empathy themselves and became aware of it—or the lack thereof—in others.

As one participant described it, rather than a leadership course providing a to-do list of qualities, Our Community Listens more closely resembled an athletic practice, requiring conditioning in its method of implementing empathy through tangible skills such as reflective listening. An Airman training for an annual fitness test breaks down each event and practices toward the components for the comprehensive assessment. Throughout this process, an Airman practices, self-evaluates, practices again, improves, and continues to practice until the test. This athletic conditioning analogy emphasizes the need to learn how to demonstrate empathy using effective techniques with facilitator feedback as a part of an intentional leadership practice and not just a part of leadership philosophy.

Developing habits and increased proficiency with empathy comes from "reps and sets" through continuous learning for accountability, practice, and feedback. The continuous-learning mindset transforms empathy from an achievable static end state into an infinite goal. To borrow from a business analogy, empathy is a game with an "infinite time horizon" and with "no finish lines" and "no winning."[29] One practices empathy continuously to understand and to seek to be understood.

Small Teams for Follow-Through

One way to encourage continuous learning in the so-called infinite game of empathy is through a small-team approach. In the study, many members struggled to remember the details of the course because it had been two months to four years since they had attended the course. Furthermore, members felt individually stuck with the burden of driving

28. Teaching Excellence in Adult Literacy Center, "Adult Learning Theories Factsheet No. 11: Adult Learning Theories" (Washington, DC: US Department of Education Literacy Information and Communication System, 2011), https://lincs.ed.gov/.

29. Simon Sinek, *The Infinite Game*, 1st ed. (New York: Portfolio/Penguin, 2019), 3–4.

change in a workplace context if they did not have others around with the same common experience and language.

The Air Force should therefore approach continuous learning for empathy from a small-team mindset to provide daily interaction opportunities. As far as can be determined, no program taught throughout the Department of the Air Force relies on an adult learning model to teach and learn empathetic behavioral skills that includes continuous learning and emphasizes small teams.

Empathy in Future Complex War

Practicing empathy in future complex war reinforces strong organizations, effective Joint and multinational partnerships, and accurate assessments of global and regional actors during conflict at the levels of tactics, operations, and strategy. Furthermore, empathy skills enable Airmen to have better relationships at home, at work, and in their communities. The Air Force needs empathetic Airmen, both professionally and personally.

Empathy helps individuals achieve goals and accomplish the mission by providing tools to avoid or manage conflict, sort out messages received versus messages intended, and understand seemingly foreign work center cultures. Operational empathy assists in understanding other perspectives, including those of the sister services and US Allies and partners. Strategic empathy offers the opportunity to consider the values and motives of regional and global actors in better analyzing the appropriate allocation of resources—human and materiel alike—to warfare.

Joint Doctrine Note (JDN) 1-19, *Competition Continuum*, explicitly calls for empathy in relationships with Allies, partners, neutrals, and adversaries during campaigning through cooperation, which is defined as an enduring, continuous activity to maintain policy goals.[30] Accordingly, not only is empathy a required skill for personal relationships and multinational operations, but it is also critical to one of the three elements of the competition continuum.

Competition Continuum further explains that if done well, the resulting relationships can yield immediate tactical or operational benefits, and enduring benefits, such as an increased commitment of a foreign military to the rule of law or a greater willingness to assist US efforts in a crisis. Though the immediate benefits of cooperative relationships are not always apparent, history demonstrates long-term relationships can pay dividends in unanticipated ways.[31]

---

30. CJCS, *Competition Continuum*, Joint Doctrine Note (JDN) 1-19 (Washington, DC: CJCS, June 3, 2019), 7, https://www.jcs.mil/.
31. CJCS, JDN 1-19, 7.

When Empathy Goes Wrong

In the interest of a balanced discussion on empathy, it is necessary to review a few considerations of reflective listening and empathetic communication for Allies, partners, and adversaries, including ethical and moral intent, over-identification, and potential perception of misalignment between empathy and military responsibilities. Even the most well-intended empathetic communication can miss the mark in an inappropriate context, requiring the Air Force to consider deeply the function of empathy in warfare.

First, the service must teach Airmen at all levels to harness empathy for the moral good. It is critical to acknowledge the potential that a person could abuse tactical empathy for manipulative purposes. Some scholars have defined tactical empathy as the connection between "seduction, deception, manipulation, and violent intent," arguing that such empathy can lead to identifying with but also "othering" individuals to dehumanize them.[32] This views the term tactical through a negative lens, which is contrary to the definition of the term used herein.

Other scholars discuss that while most humans can choose to be empathetic, the intent and situational context can lead to overwhelming others, trying to control others or the world, or even empathizing differently between peer managers and employees.[33] Incorporating empathy will require defining the moral boundaries associated with its application. Future discussions on morals should thus begin with learning empathy to connect with Airmen, build relationships with Allies and partners, and accurately assess adversaries.

Second, practicing empathy without care has a wide range of possibilities. It can be as innocuous as leaving a negative review on a travel website or it can be more nefarious as a tool for people with psychopathic tendencies to understand and then manipulate others.[34] Future concepts should explore the balance of teaching empathy to enable organizations while simultaneously understanding the potential risk at overidentifying with adversaries or empathizing but misunderstanding the message.

Finally, empathy can seem contradictory to military responsibilities. This misalignment can manifest as vulnerability for both the listener and the person being reflectively listened to. First, the person listening might have legal or ethical considerations for the information shared, such as a supervisor who is tasked with the mandatory reporting of

---

32. Nils Bubandt and Rane Willerslev, "The Dark Side of Empathy: Mimesis, Deception, and the Magic of Alterity," *Comparative Studies in Society and History* 57, no. 1 (January 6, 2015), https://www.cambridge.org/.

33. Marc J. Schabracq and Iva Embley Smit, "Leadership and Ethics: The Darker Side of Management," in *Research Companion to the Dysfunctional Workplace: Management Challenges and Symptoms*, ed. Janice Langan-Fox, Cary L. Cooper, and Richard J. Klimoski (Cheltenham, UK: Edward Elgar, 2007), 118.

34. Rebecca Pera et al., "When Empathy Prevents Negative Reviewing Behavior," *Annals of Tourism Research* 75 (March 2019), https://doi.org/; Robert I. Simon, *Bad Men Do What Good Men Dream: A Forensic Psychiatrist Illuminates the Darker Side of Human Behavior*, 1st ed. (Washington, DC: American Psychiatric Publications, 2008), 22; and Sara Konrath et al., "The Relationship between Narcissistic Exploitativeness, Dispositional Empathy, and Emotion Recognition Abilities," *Journal of Nonverbal Behavior* 38, no. 1 (March 2014), https://doi.org/.

an employee's sexual assault. Second, the person being reflectively listened to needs to decide on the appropriate boundary for oversharing. For this consideration in particular, the service needs to deliberately explore and practice the nuances of empathetic communication for the military practitioner to help Airmen successfully navigate their empathy practice and their military responsibilities.

Conclusion

The Air Force must look at applying empathy to the levels of warfare to better inculcate a foundational, building-block approach. If empathy helps individual Airmen understand others in personal and professional relationships, it is possible to transfer the skill to Joint and multinational partnerships at the operational level. As a lifelong practice, it can encourage a more thorough and accurate assessment of strategic actors to understand complex, strategic problems. This is within the Air Force's power to achieve. First, the service should incorporate empathy as a learnable and teachable skill that develops leaders capable of future complex warfare. Second, the service should break down empathy into behavioral skills, such as reflective listening, learned at the small-team level with continuous learning for reinforcement, feedback, and accountability. Third, the Air Force should teach the skill using adult learning models that provide practice, experimentation, and feedback.

Consider the fast-paced, overwhelmingly tech-enabled environment of today and imagine a world where the service teaches empathy through behavioral skills, providing an antidote to not feeling heard. As the Brown Book describes, empathy is the catalyst for relationships built on respect, trust, inclusion, and self-accountability for the impact of one's actions on others, and these relationships are what define Airmanship.[35] Imagine a future Air Force where Airmanship is knowing oneself, one's behaviors, and others through empathy—where the infinite game of empathetic communication sharpens the spear of warfare. What would Sun Tzu think of such a force?

35. USAF, *Enlisted Force Structure*, 7.

Mission Statement

Air & Space Operations Review (ASOR), recurring publication 10-1, is the flagship operations professional journal of the Department of the Air Force, published quarterly in an online edition. It serves as an open forum for the presentation and stimulation of innovative thinking on doctrine, force structure, readiness, and other matters of national defense related to air and space operations.

Disclaimer

The views and opinions expressed or implied in *ASOR* are those of the authors and should not be construed as carrying the official sanction of the Department of the Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

Please email comments or address changes to: ASOR@au.af.edu

Article Submission

Air & Space Operations Review considers scholarly articles between 4,000 and 6,500 words from US and international authors. Please see the website for specific submission guidelines and send your submission in Microsoft Word format via email to

ASOR@au.af.edu

Air & Space Operations Review
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112–6026

View and Subscribe for free to *ASOR* at
https://www.airuniversity.af.edu/ASOR/

Follow *ASOR* on LinkedIn, Facebook, Twitter, and Instagram

ASOR (ISSN 2771-7704) is published by Air University Press, Maxwell AFB, AL.

ASOR is indexed in, inter alia, ProQuest, Gale, EBSCO, and DTIC.

Air & Space Operations Review is an open, refereed forum for intellectual discussion and debate on operations, logistics, innovation, doctrine, force structure, readiness, and other matters of national defense relevant to airpower and spacepower practitioners