Screening Obscuration Module attached to Utility Task Vehicle activates autonomously during Robotic Complex Breach Concept on Yakima Training Center, Yakima, Washington, April 26, 2019 (U.S. Marine Corps/Nathaniel Q. Hamilton)

Transforming DOD for Agile Multidomain Command and Control

By Douglas O. Creviston

Advances in artificial intelligence (AI) and autonomous systems offer enhanced military capabilities to those nations that adopt and operationalize these technologies. Much like the airplane or nuclear weapons, these technologies are so significant that the Department of Defense (DOD) should expect to transform in order to fully realize their benefits. Without data, neither human nor artificial intelligence has a basis for effective decisionmaking. While human intelligence is capable of operating in a sparse data environment, many AI applications require big data sets to come into existence and continuous data flows to effectively operate. Unlike the airplane and nuclear weapons, AI and autonomy will be best operationalized not by a dedicated Service or force structure devoted to their employment, but by their incorporation into the existing forces in all domains. How might DOD need to change policy, leadership structures, and culture regarding data in order to enable the adoption and maximum benefit of AI and autonomous system technologies?

From the academic and business communities, *data science* is defined as a "multidisciplinary field that concerns technologies, processes, and systems to extract knowledge and insight from data and to support reasoning and decisionmaking under various kinds

Colonel Douglas O. Creviston, USAF, is Director of the Comparative Technology Office in the Office of the Under Secretary of Defense for Research and Engineering.

of uncertainty."[1] The field of data science may be divided into two primary activities: managing the data and using (analyzing) the data. Many of the activities of data science use AI and in turn support the development and operation of autonomous systems.

Advances in AI, autonomous systems, and big data analytics are especially relevant to emerging concepts of multidomain battle and associated multidomain command and control (MDC2). Existing C2 systems and concepts should be reconsidered in light of the transformative potential of AI and autonomy. Such a reevaluation should start with proven C2 theory, modify existing C2 doctrine if needed, and redesign C2 concepts and systems in order to gain additional capability.

While the development of data science technologies is important and necessary, it is not sufficient. This article focuses on insights from the academic and business data science communities concerning the process and system changes necessary to transform DOD to adopt AI and autonomy to MDC2. The recently released DOD Digital Modernization Strategy contains objectives to modernize C2 infrastructure and improve allied interoperability.[2] The academic field of data science combines with the theory of agile C2 to provide recommendations to enable agile, integrated MDC2 through the adoption of AI and autonomy. These recommendations suggest policy and cultural changes to transform DOD for cognitive, algorithmic warfare.

Agile C2 Theory Applied to MDC2

According to joint doctrine, "Command is the most important role undertaken by a JFC [joint force commander]. C2 is the means by which a JFC synchronizes and/or integrates joint force activities. C2 ties together all the operational functions and tasks and applies to all levels of war and echelons of command."[3] The function (or action) of command and control is separate from the C2 support systems and structures that enable it:

> *A C2 support system, which includes interoperable supporting communications systems, is the JFC's principal tool used to collect, transport, process, share, and protect data and information. To facilitate the execution and processes of C2, military communications systems must furnish rapid, reliable, and secure information throughout the chain of command.*[4]

Agile C2 theory helps explain the linkage between the function of C2 and the tool of the C2 support system by defining three dimensions that can characterize any approach to fulfilling the C2 function:

- how decision rights are allocated
- how entities interact with one another (interactions)
- how information is distributed (linkages).[5]

The JFC should define these dimensions depending on the objectives, threat, and environment. MDC2 fundamentally asserts that future conflicts will require C2 agility—the ability to alter decision rights, interaction patterns, and information distribution to effectively integrate and synchronize operations across multiple domains—in order to prevail.

Design for Agility in MDC2

C2 support systems should be designed to offer the JFC the maximum design space along the three dimensions of agile C2 theory: decision rights, interactions, and linkages.[6] Design space is here used as the range of possible options for each of the three dimensions. Current C2 support systems constrain the C2 design space; decision rights might not be allocated to the desired subordinate commander because interactions and linkages are either not possible or do not meet requirements for rapidity, reliability, or security. For example, a JFC may want to allocate the decision rights for air defense of a certain sector to a particular field commander, but the interactions and linkages may not support the flow of requisite data to the desired level of field command. Data science can help through infrastructure designs and analytical tools that enable real-time governance of interactions and linkages as determined by the JFC's allocation of decision rights. In addition, data science should be applied to each tenet and subdomain of C2—for example, by using recommender systems (market basket analysis or others) to curate information flows to decisionmakers and operators at every level and in every domain.

David Perkins and James Holmes have described the concept of multidomain battle and the reason it is needed. Historically, each Service has developed federated solutions (weapons, concepts, capabilities) in that Service's operational domain. These were then "synchronized" in a tailored joint response to a specific problem. The time and effort required to synchronize will not support future mission success, and currently possible mash-ups of federated capabilities will still be vulnerable to fracture along Service boundaries.[7] Future C2 systems are already in development, including the Air Force's in-house reboot of the canceled Falconer 10.2 upgrade, as well as the Army's restructuring of the Warfighter Information Network–Tactical program and modernization of the Nuclear Command, Control, and Communication system. As these systems are developed, key performance attributes should include integration and agility in addition to basic network requirements such as cyber security, resilience, and so forth.

Future C2 systems must be integrated and agile. Joint Publication 1, *Doctrine for the Armed Forces of the United States*, posits, "The simplest and most streamlined chain of command can be thwarted by an absence of interoperability among the components' forces and systems."[8] Interoperability is no longer enough, as Perkins and Holmes imply when they state, "We must shift from a model of interdependence to one of integration."[9] Such an integrated architecture would support the improvement they cite as most important: sensor-to-shooter webs. Investment should be made in automated data management tools (for example, a unit assigned a mission will automatically

Seaman uses handheld tablet to request resupply during Office of Naval Research demonstration of Autonomous Aerial Cargo/Utility System, giving capability to helicopters for unmanned flight, Quantico, Virginia, February 25, 2014 (U.S. Navy/John F. Williams)

be routed intelligence feeds related to that mission and operational feeds related to relevant missions in every domain).

As an example, near-future integrated air and missile defense (IAMD) against peer competitors in an anti-access/area-denial environment will rely on improved integration and information-sharing between sensors (often multirole) and shooters (often multiuse).[10] Rear Admiral Archer Macy, USN (Ret.), now a member of the Missile Defense Project at the Center for Strategic and International Studies, identified employment and C2 doctrine as one of the biggest challenges facing IAMD in the transition to a distributed defense approach. When two military Services are shooting using sensor data from four military Services and national agencies, the challenge of allocating information and authority to all the right nodes becomes immense.[11] C2 agility is required to meet this challenge.

Agility is here defined as adaptability (ability to change with the situation) with the added qualities of ease and timeliness of adaptation.[12] Agility is achieved in different ways depending on the attribute that must be changed. Agility in infrastructure may mean procuring multiple pathways for data and designing automated or low-work methods for switching between them. Agility in analysis may come through data management able to provide comprehensive data in an environment populated with open-source or licensed tools and a workforce trained to use them.

The need for tactical and C2 networks to be integrated runs counter to the organizational and funding approaches to developing those networks. The Services develop networks to meet their own needs, on their own acquisition schedules, with interoperability requirements imposed from the Joint Staff. This lack of synchronization in acquisition and development results in integration challenges and reduced C2 capability.[13]

Current C2 systems constrain the JFC's ability to allocate decision rights by limiting the linkages that are possible or permissible and what information can flow over the set of possible linkages. They are not integrated or agile enough to support MDC2. These systems have grown out of organizational, cultural, and security decisions that shaped previous system design and operational use. At the turn of the century, DOD leaders sought to apply network technology and concepts to remake the Armed Forces.

What can we learn from the 2003 DOD Net-Centric Data Strategy and resulting attempts to remake C2 networks and tactical network systems?

Lessons from the DOD Net-Centric Data Strategy

Network-centric warfare was introduced by Vice Admiral Arthur Cebrowski, Dave Alberts, and John Garstka in the late 1990s. It sought to maximize combat power through the effective linking (networking) of geographically dispersed forces, resulting in shared battlespace awareness that enables self-synchronization and synergistic action.[14] The information technology implementation of network-centric warfare inspired the 2003 strategy.[15]

The strategy sought to remake department data flow from prescribed point-to-point transfers across highly controlled interfaces to flexible many-to-many interchanges within a global enterprise data environment. It supported the DOD chief information officer (CIO) goal to "populate the network with all data (intelligence, non-intelligence, raw, and processed)"—a wide goal that has not been realized to this day with separate networks for intelligence and non-intelligence data. Furthermore, the strategy proposed to change the paradigm to "post before processing" rather than waiting to post after completion of a "processing, exploitation, dissemination" cycle. Other features still relevant yet unfulfilled include an enterprise metadata registry, a data catalogue, and establishment of interface standards to facilitate flexible interfaces unforeseen during development of an information system. The strategy defined data attributes essential to meeting performance goals—data was to become visible, accessible, institutionalized, understandable, trusted, interoperable, and responsive to user needs.[16] The goals of the strategy are echoed in recent DOD and Service guidance; they are still relevant and desirable but have proved elusive. The strategy accurately understood important shifts in the global information environment and proposed sweeping changes to adapt. What factors limited the realization of the strategy?

Priscilla Guthrie, a key instigator of the strategy and DOD deputy CIO at the time, identified communication as a central shortcoming. In 2003, data science advocates failed to clearly communicate the business and operational case for implementing the data strategy. The theory of information, semantic technology, technical capabilities of information technology, and computer science jargon was meaningless to most DOD senior leaders, military and civilian alike.[17] Private-sector examples of effective data science existed, but they were nascent. In this respect, the situation is somewhat better in 2020 as private-sector success stories abound in the business results of data-centric companies such as Google, Amazon, Microsoft, and Facebook, and popular interest in AI/machine learning is captured by public demonstrations from AlphaGo to autonomous package delivery.

Leadership support in 2003 was neither sustained nor strong due to leadership transitions and lack of understanding. According to Guthrie, DOD did not have the human resources to effectively acquire, implement, and operate a modern data infrastructure and failed to develop viable contract vehicles to remedy the shortfall.[18] Implementation of the data strategy also stalled because of the failure to field a viable metadata registry and data catalog, necessary to any effective execution of data science. DOD failed to enact a viable resourcing plan to support the strategy. As a cross-cutting, foundational capability, data infrastructure needed a single champion to advocate for investment and a stable, multiyear funding stream.

The 2003 strategy was a forward-thinking document that failed to achieve the desired result. The primary reasons for that failure were lack of leadership support due to lack of understanding; failure to make necessary cultural, organizational, and policy changes; inadequate in-house human resources and failure to acquire adequate external human resources; and inadequate financial resources due to a flawed funding strategy.

DOD problems with implementation of the strategy have cost billions of dollars, years of effort, and lost combat effectiveness. As a foundational step toward effective MDC2, senior leaders should address the key factors contributing to that failure. The strategy was not a perfect document, and network-centric warfare was not a perfect concept, but those imperfections will be an inherent part of current and future strategy and concept development. The new DOD Digital Modernization Strategy outlines a strategic plan for resource investment in fiscal years 2019 to 2023 and continues with many themes evolved from network-centric warfare and the 2003 data strategy, but with greater specificity of mission objectives and a plan for incorporating cutting-edge information technologies. To effectively execute digital modernization of DOD, senior leaders will need to resolve important cost-benefit tradeoff decisions that were and will be inherent to any major policy, organizational, and resourcing shifts. Data science as an academic discipline offers insights that can guide leadership decisions. Individual applications will pose unique challenges and require unique solutions, but data science provides the theoretical principles and disciplined process by which the department can adopt AI and autonomy to turn data into military capability.

Data Science Defined

To reiterate, data science is "a multidisciplinary field that concerns technologies, processes, and systems to extract knowledge and insight from data and to support reasoning and decisionmaking under various kinds of uncertainty."[19] This field may be divided into two primary activities: managing the data and using (analyzing) the data. Data management encompasses the collection, storage, cleaning, engineering, and monitoring activities required to give data the desired attributes that make it useful.[20] To be useful, data must be visible, accessible, understandable, trustworthy, and interoperable.[21] Data is used through data analytics in activities also known as business intelligence

Fourth-year Ph.D. student Mark Velednitsky, University of California, Berkeley, discusses his research during Naval Postgraduate School Operations Research Department's second annual Day of Data, Decisions, and Defense, Monterey, California, August 27, 2018 (U.S. Navy/Javier Chagoya)

and big data analytics and encompasses descriptive, predictive, and prescriptive analytics. This article includes within the definition of *data science* the management and organizational processes and systems necessary to enable the application of data management and analytics technologies—sometimes also referred to as the "digital transformation" or "digital modernization" of an organization.

Data Science: Forcing, Enabling, and Enabled Technologies

Forcing technologies push data science by creating data problems requiring data science to solve. The proliferation of sensors, storage and computing power, and network connectivity has resulted in substantial growth in the volume and variety of data that must be managed. Practicing data analytics creates new data about data. The Internet of Things promises penetration of this sense/store/compute/network structure into previously data-sparse environments. The resulting flood of data renders legacy human-centered approaches to analysis and decisionmaking ineffective; the dominant challenge has changed from one of sensing and collecting data to one of processing, cataloguing, searching, and verifying useful data. These forcing technologies have combined to increase the volume, velocity, and variety of relevant data beyond the capability of legacy infrastructure and analytic capabilities.

Data science often uses statistical methods that are old concepts applied in new ways. The key enabling technologies have been increased computing processing power and memory at decreased cost, increased data generation throughout the environment, and massive parallel data architectures that enable efficient storage and processing of data at the point of storage (virtualization). These advances combine to make statistical concepts that were prohibitively expensive in either time or money practical for a wide range of users.

Data science enables one to sense reality in many ways and then perform computationally expensive but conceptually simple algorithms to allow an intelligence (human or artificial) to understand reality more fully and accurately. Technologies enabled by data science include descriptive, predictive, and prescriptive analytics, AI, and autonomy. Major technological trends have dramatically changed the volume, variety, and velocity of data available for MDC2 as well as the operational benefit that may be gained from that data. Extracting that operational benefit requires overcoming the obstacles that derailed full implementation of the 2003 data strategy.

Recommendations for Agile MDC2

Proposals to enable effective MDC2 are derived from historical examples and civilian literature on digital transformation of complex business operations. DOD has repeatedly fallen short of strategic goals relative to data and network-centric warfare, in part due to excessive focus on the technology and acquisition thereof. The Defense Innovation Board captured the link between the first three recommendation areas when it stated, "Since many of the Department's challenges with data are cultural (that is, DOD organizations are not used to collecting or sharing data), the Secretary's role in this endeavor is critical, particularly because new policy and legal frameworks will be necessary to change the status quo."[22] None of these recommendations are binary; each requires leadership judgment to select an approach that balances present and future risk, funding limitations, statutory authority, and so forth. Leandro Dallemule and Thomas Davenport have discussed how leaders can define the overall posture of an organization relative to "offensive" and "defensive" uses of data and show how different governance, organizational structures, and resourcing approaches are best suited to each set of uses.[23] The foundational concept behind these recommendations, born out of a reading of the civilian literature on data science and digital modernization, is that senior leaders should take a holistic approach to transform DOD for the application of AI and autonomous technologies, for both MDC2 and other mission areas. The 2019 DOD Digital Modernization Strategy outlines ambitious and much-needed goals and objectives to transform DOD. What are the difficult policy, cultural, and organizational tradeoffs leaders should expect to make, and what resources are available to support those decisions?

Recommendation One: Senior Leaders Should Implement Data Science as a Multidisciplinary Field to Guide Transformation of Policy, Organization, and Resourcing Decisions. Leaders must make foundational decisions to achieve coherence among data management, data analytics, and the overall strategy and trajectory of DOD as AI and autonomous technologies are acquired and fielded. At the department level, leaders can learn from civilian management experiences of transforming companies and institutions to inform difficult tradeoff decisions. Transitioning C2 from an industrial-age approach to an AI-enhanced one will require leaders to initiate and sustain the transformation with a changing threat environment and emerging multidomain battle concepts. This includes the development and acquisition of C2 support systems that maximize the design space available to JFCs and that are delivered integrated and agile to support joint and coalition operations. The acquisition of such systems may require a different allocation of acquisition resources and/or oversight in order to synchronize disparate efforts. Instead of viewing data science (or AI or autonomy) as a tool to be bought, commanders should recognize data science as a discipline practiced to enable better decisionmaking.[24] This recognition should include experimentation with different allocations of decision rights, interactions, and linkages to explore the effects of different concepts in contested peer conflict. Without senior leader support to initiate and persistently support the application of data science, the existing conflicts among policy, organizational priorities, and parochial interests will continue to forestall system design, acquisition, experimentation, and operational execution of MDC2.

Recommendation Two: DOD Senior Leaders Should Promote Cultural Values of Data Collection, Evidence, and Cooperation (Data-Sharing). DOD does not appropriately value data. Data is valued relative to the primary purpose for which it is collected. One tenet of data science is that data is inherently valuable and may be used to extract value in many ways beyond the purposes for which it was originally collected.

The dominant DOD cultural value regarding data is one of protection within organizations on the smallest level—except where forced by leader action or policy. Leaders from the top down should recognize the value of sharing data and require open analysis, including the sharing of underlying data as well as analytic methodologies to support evidence-based decisions. To support and encourage a culture of data-sharing, policy should be shaped to promote the needed analysis to generate decision-quality evidence with the minimum interference required for governance and security needs.

Recommendation Three: Leadership Should Issue Clear, Consistent Policy Promoting Data Availability at Acceptable Risk. Senior leader calls for innovation and rapid acquisition are sometimes undercut by data governance policy (or lack thereof) that allows compartmentalization to persist. This is a problem that subordinate units are unable to solve in a timely manner. Governance policy should cover data ownership, access, use, protection, and disposition. In addition, governance could extend to validation of data sets as authoritative or of analysis as technically sound. Data sets will have unique risk/reward characteristics based on their content and potential uses. As with any policy, data governance policy should be clear and consistent to define the boundaries of acceptable action and promote freedom within those boundaries. In addition to clarity and consistency, policy should be evaluated over time to determine effectiveness. This evaluation should be an explicit part of joint exercises and operations; if data-sharing policy does not support mission success, the policy must be changed.

Recommendation Four: Develop a Methodology for Assessing the Value of Sharing Data. For classified and compartmented data, "need to know" is a policy, not only a cultural mindset. Security policy is authoritative, communicating leadership decisions about the acceptable risk/reward ratio for data access. To support those decisions, estimates should be developed for the damage to national security due both to information escape and ill-informed decisions or to operational failures because of incomplete information. A well-structured data science effort should consider

Army UH-60 "Blackhawk" flies in formation over Yamaguchi Bay, Japan, during premier U.S. Army and Japan Ground Self-Defense Force bilateral field training exercise Orient Shield 2019, September 9, 2019 (U.S. Army/Jacob Kohrs)

a means of quantifying these two estimates (loss due to sharing and loss due to not sharing) into a decision support system for information-sharing decisions. Such decisions may include lowering the classification level of information over time, sharing information with certain allies or coalition partners, or removing a compartmentation or special access program caveat to allow wider awareness and incorporation of an operational capability. Leadership statements about the importance of concepts, such as sensor-shooter networks in multidomain battle and technologies such as AI, to victory in future conflict must be converted into security policy changes that permit adoption of those concepts and technologies with appropriate, accepted risk to information flows. There are technologies to improve the risk/reward ratio of information-sharing decisions, but these do not fully resolve the inherent reduction in information security that comes with increased access to the information.

Recommendation Five: Vest Security Decision Authority Where Risk and Reward Meet, at an Appropriate Level Within the Chain of Command. Commanders at every level should be given clear, expanded "right to share" authority over information and information systems. In addition to providing a decision support system for information-sharing decisions, policy should be changed to vest those decisions in the chain of command. Existing policy puts operational effectiveness at risk by endowing security professionals outside and disconnected from the chain of command with final authority for information-sharing decisions, at both the infrastructure level (network infrastructure authority to connect/authority to operate) and the operational level (the ability to disclose a particular element of operational or intelligence data to a subordinate decisionmaker or operator). Furthermore, some intelligence and acquisition agencies restrict the range of possible information linkages available to the operational commander through compartmentalization or special access programs. The chain of command should be given a right to share authority over all information the commander has access to for all members, U.S. and coalition, under his or her command. This right to share will likely require limits to protect strategic interests and/or prevent the present chain of command from reaping current rewards at the cost of increased future risk.

As an example, a joint task force commander may be given authority to share classified information not specifically cleared for foreign disclosure with a coalition partner who possesses a comparable security clearance. As an additional

example, a combatant commander may be given authority to grant access to special access programs to members of his or her command deemed necessary, but subject to the limitation that those members have a clearance at the overall classification level. There are existing processes for both of the above examples that reflect a certain static risk/reward tradeoff decision, but those processes and the underlying tradeoff decision should be reevaluated in light of the accelerated pace of warfare, knowledge, and information flows required for successful implementation of AI and autonomous technologies.

Recommendation Six: Contract for Partnership to Build Government Capability in C2 Support Systems. Agile C2 support systems likely cannot be acquired as traditional vendor-supplied systems with proprietary architecture, both because contracting (and associated legal) timelines are too long and because DOD human resources with intimate understanding of the C2 support system are required. DOD has inadequate capability and capacity of human resources to implement data science in command and control, so contractor support will be required for some time. Contractor personnel could provide support services with appropriate contract vehicles that avoid proprietary solutions, produce data and tools that are government property, and surge human resources in areas the government is lacking. The Air Force approach to developing C2 applications in-house seeks to deliver both needed C2 capabilities now and the capacity for agile development of future capabilities. Active-duty Air Force programmers are teamed with those of Pivotal Labs to produce software that is wholly government-owned and may be iteratively developed as requirements change.[25] DOD should recognize the need for in-house capability to adapt C2 support systems in the combat zone and invest in equipment and training to develop that capability.

Future warfare will incorporate two broad trends: multidomain battle and AI/autonomy. Both trends demand a higher level of interoperability, even integration, of data networks to be successful. Across the range from competition to conflict, joint force commanders will need maximum design space in the three agile C2 dimensions of decision authorities, interactions, and linkages to develop effective multidomain C2 approaches. DOD has pursued transformation to a network-centric force before, but with limited success. Learning from the implementation of the 2003 data strategy, senior leaders should apply data science theory from the civilian world to evaluate what deep cultural, organizational, and policy changes may be necessary to adopt the transformative technologies of AI and autonomy. Future multidomain battles will be complex, and that complexity cannot be eliminated with technology. Developing agile and integrated C2 support systems may enable future JFCs to prevail over the enemy despite the complexity. **JFQ**

Notes

[1] National Academies of Sciences, Engineering, and Medicine, *Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions* (Washington DC: National Academies Press, 2017), 1–2.

[2] *DOD Digital Modernization Strategy* (Washington, DC: Department of Defense, June 5, 2019), available at <https://media.defense.gov/2019/jul/12/2002156622/-1/-1/1/dod-digital-modernization-strategy-2019.pdf>.

[3] Joint Publication (JP) 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013, incorporating change 1, July 12, 2017), xxiii.

[4] Ibid., xxiv.

[5] David S. Alberts et al., *C2 by Design: Putting Command and Control Agility Theory into Practice*, version 2.0, NS D-5614 (Alexandria, VA: IDA, 2015), 14.

[6] David S. Alberts, Reiner K. Huber, and James Moffat, *NATO NEC C2 Maturity Model* (Washington, DC: DOD Command and Control Research Program [CCRP], 2010), xvii.

[7] David G. Perkins and James M. Holmes, "Multidomain Battle: Converging Concepts Toward a Joint Solution," *Joint Force Quarterly* 88 (1st Quarter 2018), 54–57.

[8] JP 1, V-19.

[9] Perkins and Holmes, "Multidomain Battle," 54–57.

[10] Thomas Karako and Wes Rumbaugh, *Distributed Defense: New Operational Concepts for Integrated Air and Missile Defense* (Washington, DC: Center for Strategic and International Studies [CSIS], January 2018), available at <http://missilethreat.csis.org/wp-content/uploads/2018/01/Distributed-Defense.pdf>.

[11] Remarks from January 25, 2018, release of the *Distributed Defense* report at CSIS.

[12] Alberts et al., *C2 by Design*, 6.

[13] Brian K. Bass et al., "Overcoming Joint Interoperability Challenges," *Joint Force Quarterly* 74 (3rd Quarter 2014), 136–140. See figure 2.

[14] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare* (Washington, DC: CCRP, 1999), 88.

[15] *DOD Net-Centric Data Strategy*, memorandum, May 9, 2003, available at <http://dodcio.defense.gov/Portals/0/Documents/DIEA/Net-Centric-Data-Strategy-2003-05-092.pdf>.

[16] Ibid.

[17] Priscilla Guthrie, interview by author, December 7, 2017.

[18] Ibid.

[19] National Academies of Sciences, Engineering, and Medicine, *Strengthening Data Science Methods for Department of Defense Personnel and Readiness Missions*, 1–2.

[20] Ibid., 2.

[21] *DOD Net-Centric Data Strategy*. These five attributes were identified in the 2003 DOD Data Strategy and are repeated verbatim in the 2017 Navy Data Strategy and 2016 Army Data Strategy. The Air Force substitutes the phrase *link context* for the term *interoperability* to form the acronym VAULT (visible, accessible, understandable, linked, and trustworthy), but it retains the essential attribute characteristics.

[22] Defense Innovation Board, *Practices and Operations—Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis*, March 19, 2018, available at <http://innovation.defense.gov/Recommendations/>.

[23] Leandro Dallemule and Thomas H. Davenport, "What's Your Data Strategy?" *Harvard Business Review* (May–June 2017), 112–121. The authors characterize the overall posture of an organization relative to "offensive" and "defensive" uses of data and show how different governance, organizational structures, and resourcing approaches are best suited to each set of uses.

[24] Defense Innovation Board, *Practices and Operations*.

[25] Mark Wallace, "The U.S. Air Force Learned to Code—and Saved the Pentagon Millions," *Fast Company*, July 5, 2018, available at <www.fastcompany.com/40588729/the-air-force-learned-to-code-and-saved-the-pentagon-millions>.