COMMENTARY

Seize the Data Initiative

Lt Col Rick Schuessler, USAF

Flexibility is the key to airpower.

—General Giulio Douhet

While General Douhet's observation remains a key tenant of airpower today, superiority in modern warfare requires increasingly complex, data-centric approaches to enhance the decision cycle and amplify the inherent flexibility of airpower. Furthermore, airpower is not alone in this challenge—as the flexibility of a vast number of diplomatic, informational, military, and economic applications are underpinned and enhanced by timely, accurate, and comprehensive data. Therefore, it is no longer adequate for organizations to only look internally when designing improved organization, analytic, distribution, and collaboration data tools or data strategies. Instead, to seize the data initiative and maintain the asymmetric advantages America has enjoyed in past, the United States must develop a holistic approach to data that improves the precision, timeliness, and convergence effects of US, ally, and partner instruments of national power. The technological advancements of the past decades have resulted in incredibly deep data lakes that hold opportunities to deter malicious actions through detection, attribution, and cost imposition. Connecting these data lakes to better cut through the volatile, uncertain, complex, and ambiguous environments of conflict will continue to ensure peace through decision superiority and, ultimately, strength. To that end, this article is intended to provide some historical context for the importance of connecting data, current progress within the Department of Defense, and a vision for future data imperatives.

Historical Context

Discrete, disparate, and fragile information systems have been at the root of too many catastrophic failures throughout history. One of these examples had the potential to change the course of World War II and stresses the importance of data integration and interoperability as key advantages with our allies and partners. On 10 May 1940, German forces swept through France in less than six weeks, culminating in the occupation of France. Despite reports and data indicating otherwise, French Army general Maurice Gamelin expected the German forces to attack through Belgium instead of through the wooded areas of the Ardennes and Sedan.[1] German historian Karl-Heinz Frieser later affirmed, "The air forces of the allies were presented with a unique opportunity on a silver platter to smash a major portion of the German panzer force in the Ardennes but as if by a miracle, the German panzers were not bothered."[2] If an interconnected data and intelligence system had existed at that time, the multisource data would have illuminated the actual German plan, and a game-changing opportunity could have been seized to alter the course of history.

Soon after the Battle of Sedan, the Japanese Naval Forces attacked the United States at Pearl Harbor on 7 December 1941. This horrific attack left the United States stunned, having been dealt a significant blow to the US ability to wage war. However, much like the Sedan case, the buildup leading to the attack on Pearl Harbor presented multiple data and intelligence sources that—if compiled, analyzed, or fused—would have thwarted the Japanese attack. Instead, Pearl Harbor was dealt a significant blow, and tremendous fog and friction ensued at all command echelons, making command and control (C2) of the immediate attack nearly impossible. Decades later, similar shortcomings in intelligence sharing resulted in the terrorist attack on the World Trade Center. This led to clear recommendations from the 9/11 Commission that we must do better. Included in its report were five lines of effort that call for unification of counterterrorism agencies and efforts as well as the following critical observation, "The U.S. government has access to a vast amount of information. But it has a weak system for processing and using what it has. The system of 'need to know' should be replaced by a system of 'need to share.'"[3]

Despite our past failures and the 9/11 Commission's recommendations, our situation today has not drastically improved. We continue to face challenges regarding data sharing, and technological advancements have complicated the decision space through super-saturated, data environments. Contextually, estimates approximate the amount of data stored by 2020 at 40 trillion gigabytes (40 zettabytes), with Internet users generating 2.5 quintillion bytes of data each day.[4] The average Internet user spends 33 percent of their online time engaged in social media,[5] and Twitter users average more than half a million tweets per minute.[6] Described another way, at current download speeds, it would take a single person approximately 181 million years to download the entire Internet.[7] The existence of such large data repositories provides both opportunities and vulnerabilities to any population. Our adversaries are designing government and civilian organizations and systems to weaponize this data for exploitation across all their elements of national power. The cybersecurity firm FireEye, along with Google's Threat Analysis Group and the Australian Strategic Policy Institute, for example, has been tracking hundreds of artificial social network accounts designed for pro-People's Republic of China (PRC) influence.[8] These accounts have attempted to discredit prodemocracy movements and are known to cover more than seven languages.[9] Furthermore, the Department of Defense (DOD) assesses China is moving from an "informationized" warfare and to "intelligentized" warfare.[10] Toward this objective, China is developing advanced capabilities in "artificial intelligence, cloud computing, big-data analytics, quantum information and unmanned systems."[11] The United States and its allies must build capabilities to detect, counter, and, if necessary, defeat these increasingly advanced systems to credibly deter coercion and aggression.

Current Progress within the Department of Defense

A strategist should think in terms of paralyzing, not of killing.

—Basil Liddell Hart

By sowing division, increasing the number antiaccess and area denial capabilities, and stealing intellectual property, we know the PRC is attempting to paralyze those who intend to maintain the rules-based international order and a free and open Indo-Pacific. To remain agile, the US Indo-Pacific Command is working on technological advancements that will create advantage by enabling operations inside an adversary's decision loop. Success in this arena will be contingent on the ability to sense, make sense, decide, and act across multiple domains and in concert with allies and partners. Synchronizing these operations in a contested, degraded environment presents additional challenges. Recognizing those challenges, on 5 May 2021, the United States Deputy Secretary of Defense defined DOD data as a strategic asset and tasked all DOD leaders with ensuring data is "visible, accessible, understandable, linked, trustworthy, interoperable, and secure."[12] Furthermore, the DOD defined five data decrees:

1. "Maximize data sharing and rights for data use: all DoD data is an enterprise resource."[13]
2. "Publish data assets in the DoD federated data catalog along with common interface specifications."[14]
3. "Use automated data interfaces that are externally accessible and machine-readable; ensure interfaces use industry-standard, non-proprietary, preferably open-source, technologies, protocols, and payloads."[15]
4. "Store data in a manner that is platform and environment-agnostic, uncoupled from hardware or software dependencies."[16]
5. "Implement industry best practices for secure authentication, access management, encryption, monitoring, and protection of data at rest, in transit, and in use."[17]

These decrees are designed to move beyond segmented systems and toward a culture of data standardization and sharing. These are necessary steps to set the foundation, formalize, and frame the data architecture toward a Joint All-Domain Command and Control (JADC2) solution. Currently, the services have primarily focused on individual service-specific requirements as their contributions to the overall JADC2 effort. These service programs include the Advanced Battle Management System (USAF), Project Overmatch (Navy), and Project Convergence (Army). Recognizing a greater need for collaboration, Air Force Chief of Staff Gen. Charles Q. Brown and Army Chief of Staff GEN James McConville recently signed a memorandum of understanding to work toward the JADC2 solution while acknowledging the final design must include allies and partners.[18]

The United States is overmatched in labor-intensive systems and is also at risk of losing the advantage in capital and technological superiority. Artificial intelligence (AI), machine learning (ML), and quantum computing will be critical enablers for both JADC2 and maintaining a competitive advantage into the future. One example of a program that must continue to be replicated was the successful "confluence of warfighter, developer, and acquirer."[19] This type of collaboration between academia, industry, and the Air Force successfully integrated AI as a copilot on a U-2 aircraft.[20] Partnerships such as these must continue to grow to innovate at a speed and scale that matches the dynamic threat landscape. It is also critical to recognize that these advancements have data beginnings. Organizing, labeling, and sharing data now can reduce timelines for future innovation by getting that data in the hands of the war fighter to design, experiment, and integrate. Deterrence and competition will also necessitate more efficient and effective data protection. All technologies must be better protected in development, and that starts with ingesting reliable and secure data. The United States cannot continue to fund the enormous research-and-development costs of significant technological advancements only to have them stolen, rendered obsolete, or replicated for a fraction of the cost.[21] Protecting this data and information in development is essential to our ability to defend ourselves, as well as our allies and partners. The United States must ensure all design efforts are adequately protected against data theft, corruption, and manipulation. The stovepiped or air-gapped solutions of the past are no longer adequate.

In addition to C2 advances, there are many new technologies on the horizon with the potential to increase our deterrence effectiveness by detection and, subsequently, by denial. These technologies will increase our ability to sense, plan, decide, and act across all domains. As an example, the Next-Generation Air Dominance program is reported to have implemented cutting-edge advanced manufacturing and digital design techniques to create a networked platform developed with reduced costs and increased interoperability.[22] Moreover, in the integrated air-and-missile defense arena, the hypervelocity gun weapon system is demonstrating capability against a wide range of air threats at a significantly reduced cost per shot when compared to existing contemporary missile defense systems.[23] Integration into the Army's Integrated Air and Missile Defense Battle Command System promises to enhance area air defense and protection of critical assets. Furthermore, remotely piloted aircraft continue to advance their roles and prove resiliency with advancements in survivability, agility, data collection, onboard processing capability, AI integration, and air domain awareness. These are a few of the future tools and countermeasures that, if properly integrated, will promote deterrence through redundancy, multisource validation, self-healing network capabilities, and a layered defense.

Vision for Future Data Imperatives

> *Having a strategy suggests an ability to look up from the short term and the trivial to view the long term and the essential, to address causes rather than symptoms.*
>
> —Lawrence Freedman

Toward this outcome, JADC2 is a desired future state—but not the end state; the journey but not the destination. Due to the amount of data available and limits of human manpower and processing capability, we must build future technology as interconnected pieces of a larger network that ensures interoperability with not only joint and combined forces but also other whole-of-government and industry partners. This requires a common architecture, whole-of-government approach, and a coalition strategy toward information that includes assessment capabilities and a breakdown of the political, physical, and policy barriers to implementation. This concept is an expansion of the current JADC2 concept and goes beyond service components to create integrated deterrence though the entanglement of all instruments of national powers of nations interested in maintaining a rules-based international order.

From a military perspective, ingesting and disseminating nontraditional data sources will be critical in developing strategy and assessing performance and effectiveness in an increasingly expanding role of countering and deterring operations below the level of armed conflict. Autonomously disseminating evidence of sanction, international law, or border violations though industry, military, government, and coalition networks using AI and zero-trust networks to rapidly converge and coordinate effects is just one example of how this new network could aid maneuvers inside an adversary's decision loop. Coordinating humanitarian assistance and disaster relief activities between partner nations and government agencies is another example of where rapid data analysis, augmented or automated decision cycles, and information dissemination could help achieve objectives and save lives. For consideration and design of such a system, the Bretton Woods conference provides a useful model from the past. Readjusted to today's global landscape and focused on peace and stability through conventional deterrence by the convergence of effects across combined national instruments of power.

Conclusion

Creating scalable, integrated networks with adaptive, resilient, and collaborative properties is the key to covering the gaps and seams of our decision loops and to deterring conflict by convincing our adversaries that achieving their objectives by force is not possible. This is the change that will enable the United States and its allies to remain a potent force for freedom across all phases of conflict for decades to come. Technology has accelerated the rate of change for the world, and the US military must keep pace to guarantee it remains relevant in a shifting landscape. Ensuring future investments are networked, adaptable, resilient, overlapping, and secure will create opportunities where discrete and rigid systems break down. Connecting large data lakes to underpin deterrence, to make C2 more resilient, and to bridge partner nations and government agencies will take a strategic approach to data collection and data sharing that will push boundaries. Empowering our people to design, build, implement, and adjust these new capabilities and discover innovative ways to accomplish the mission will be critical. AI, ML, and quantum computing must be employed to complement our strengths and reinforce our weaknesses, to cut through the fog and friction, and to enable our greatest assets—our people—to remain flexible, agile, and inside the enemy's decision-making process. The race to that future is upon us; ensuring a free and open Indo-Pacific will depend on our success. ✪

Lt Col Rick Schuessler, USAF

Lieutenant Colonel Rick Schuessler is the Deputy Division Chief of the Futures Division, Headquarters Pacific Air Forces (PACAF), Joint Base Pearl Harbor-Hickam. He was commissioned in 2003 as a ROTC graduate from Villanova University and earned his pilot wings in 2005 from Vance Air Force Base, Oklahoma. After pilot training, he served as an instructor pilot in the C-21A Learjet and the E-8C JSTARS and as an evaluator pilot in the MQ-9 Reaper. Prior to his current assignment, he was the Commander of the 25th Operations Support Squadron at Shaw Air Force Base, South Carolina where he provided all aspects of MQ-9 Reaper Remotely Piloted Aircraft (RPA) global operations support. He is a command pilot with over 4,900 total hours, 2,700 combat/combat support hours, and has flown in support of Operations Enduring Freedom, Iraqi Freedom, Freedom's Sentinel, Inherent Resolve, and Jukebox Lotus.

Notes

1. Lorris Beverelli, "Why France Lost in 1940," *War Writers*, 11 October 2020, https://warwriters.com/.

2. John T. Correll, "The Fall of France," *Air Force Magazine*, 27 November 2018, https://www.airforcemag.com/.

3. National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, Executive Summary.* https://govinfo.library.unt.edu/.

4. Christo Petrov, "25+ Impressive Big Data Statistics for 2020," *Techjury*, 5 February 2021, https://techjury.net/.

[5] Petrov, "25+ Impressive Big Data Statistics for 2020."

[6] Petrov, "25+ Impressive Big Data Statistics for 2020."

[7] Petrov, "25+ Impressive Big Data Statistics for 2020."

[8] Ryan Serabian and Lee Foster, "Pro-PRC Influence Campaign Expands to Dozens of Social Media Platforms, Websites, and Forums in at Least Seven Languages, Attempted to Physically Mobilize Protesters in the U.S.," *FireEye Threat Research Blog*, 8 September 2021, https://www.fireeye.com/.

[9] Serabian and Foster, "Pro-PRC Influence Campaign Expands to Dozens."

[10] Mark Pomerleau, "China moves toward new 'intelligentized' approach to war-fare, says Pentagon," *C4ISRNET*, 1 September 2020, https://www.c4isrnet.com/.

[11] Pomerleau, "China moves toward new 'intelligentized' approach."

[12] Kathleen H. Hicks, "Creating Data Advantage," *Deputy Secretary of Defense Memorandum*. 5 May 2021, https://media.defense.gov/.

[13] Hicks, "Creating Data Advantage."

[14] Hicks, "Creating Data Advantage."

[15] Hicks, "Creating Data Advantage."

[16] Hicks, "Creating Data Advantage."

[17] Hicks, "Creating Data Advantage."

[18] Theresa Hitchens, "Air Force Chief Seeks Navy Chief's Cooperation on JADC2," *Breaking Defense*, 21 October 2020, https://breakingdefense.com/.

[19] Secretary of the Air Force Public Affairs, "AI Copilot: Air Force achieves first military flight with artificial intelligence," *Air Force News Service*, 16 December 2020, https://www.af.mil/.

[20] Secretary of the Air Force Public Affairs, "AI Copilot: Air Force achieves first military flight."

[21] Terry Thompson, "How Congress Can End China's Theft of U.S. Military Secrets," *RealClear Defense,* 8 October 2020, https://www.realcleardefense.com/.

[22] Valerie Insinna, "The U.S. Air Force has built and flown a mysterious full-scale prototype of its future fighter jet," *DefenseNews*, 15 September 2020, https://www.defensenews.com/.

[23] Yasmin Tadjdeh, "Secretive Pentagon Office Shares Details About Hypervelocity Missile Defense Weapon," *National Defense*, 26 January 2018, https://www.nationaldefensemagazine.org/.