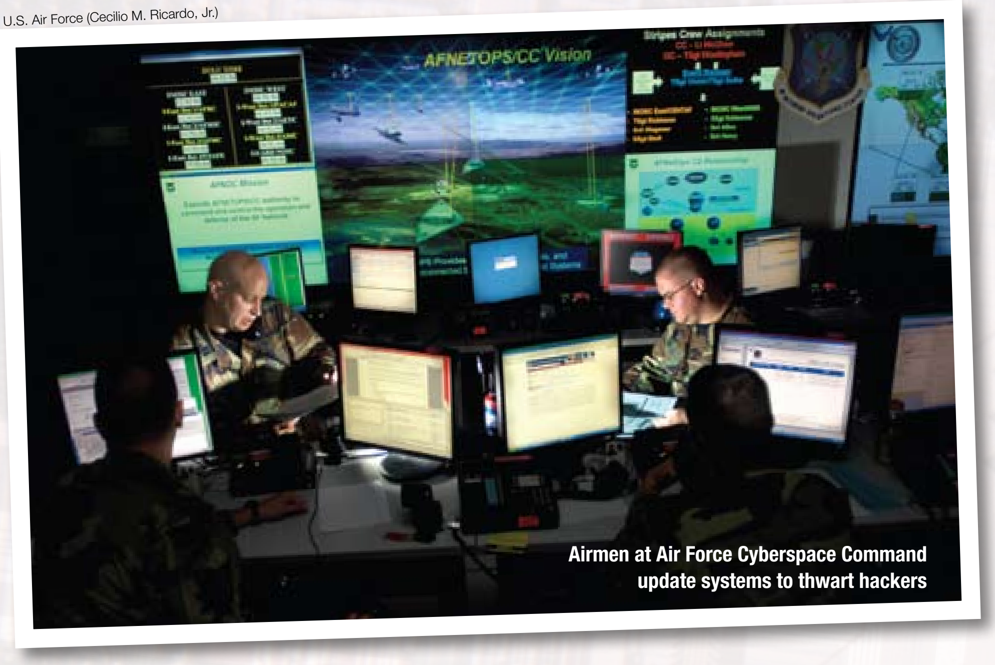
Data Transparency
Empowering Decisionmakers

By MICHAEL W. PETERSON

U.S. Air Force (Cecilio M. Ricardo, Jr.)



Airmen at Air Force Cyberspace Command update systems to thwart hackers

Today's U.S. Air Force operates in a world of diverse threats marked by the proliferation of weapons of mass destruction, unconventional warfare, enemy countermeasures, and cyberattacks moving at the speed of light. We have taken many small steps over the last 10 years to migrate stovepiped systems that do not share information toward an environment where we can fuse and use data on demand. In the end, it is all about the data—at least when it is presented as decision-quality, actionable information.

During the Gulf War, we failed to destroy any Iraqi Scud missiles during the launch preparation phase. We tracked every launch, but even then we were unable to respond and destroy the transporter-erector-launch (TEL) vehicles they relied on. We simply had not built the supporting tactics, techniques, and procedures and, more importantly, could not move information from sensor to shooter quickly enough to kill the TELs. During the air war over Serbia, we struggled for more than 4 hours to turn data into a "destroyed" SA–6 surface-to-air missile, thereby protecting the skies near Pristina, Kosovo. In that case, Serbian air defense forces were certainly operating inside our observe, orient, decide, act loop. In 2003, intelligence indicated that Saddam Hussein entered a restaurant in the Mansur suburb of Baghdad. A B–1B Lancer was diverted and flattened the target with a precision-guided munition. Unfortunately, Saddam had only used the restaurant to enter an underground tunnel system and was already gone when the strike occurred. Even though we compressed the decision cycle time from countless hours in 1991 to 35 minutes in 2003, it was not enough to operate inside the enemy's execution cycle.

We now collect more battlespace information than ever before. Global Hawks, Predators, and on-orbit assets are continuously collecting data and sending it around the world. The combined sensor data create a virtual flood of battlespace information—possibly too much information if it is not carefully managed. Increasing speed and precision on the battlefield demand unprecedented knowledge. Turning data into knowledge requires advanced data management strategies.

We are making great progress in reducing our decision cycles, exemplified by the time-sensitive targeting operation that killed Abu Musab al-Zarqawi in June 2006. However, our work is far from over. Even today, two-thirds of the time required to prosecute a time-sensitive target is allocated to manual communication processes—not machine to machine, not automated, but rather someone making a voice call, writing something down, or manually entering data. To continue evolving the delivery of decision-quality information to the warfighter, the Air Force is focusing on automating manual processes and employing advanced data management strategies.

Overview

The need for a Department of Defense (DOD)–wide strategy to manage data was formalized in 2001 through the DOD Net-Centric Data Strategy Initiative, which seeks to expose decisionmakers at all levels to authoritative data. The Air Force's implementation of this strategy, called Data Transparency, will eliminate the need for these time-consuming, labor-intensive activities and ensure that authoritative information reaches the decisionmaker. This means that battlefield commanders and their support staffs get the best, most current, and most accurate data available.

The lack of authoritative data means that battlefield commanders may actually operate with different information than what is accessible by headquarters elements. When users collect data, store it locally, and then share it with other systems, the data quickly become redundant, dated, and potentially inaccurate. This problem manifests itself when decisions are made based on inconsistent or old data. For example, our unit deployment managers (UDMs), who oversee the readiness and deployment of Airmen, must access training, medical, and equipment readiness information from multiple sources. Some of these sources include spreadsheets, databases, and paper reports that are days if not months old. When inconsistent or inaccurate information is used to make decisions, unqualified Airmen could

Lieutenant General Michael W. Peterson, USAF, is Chief of Warfighting Integration and Chief Information Officer for the Office of the Secretary of the Air Force.

initially be tasked to deploy. Once the error is discovered, we have tripled our workload since we must dedicate time and resources to finding a suitable replacement, resulting in short-notice deployment taskings.

The Technical Approach

To remedy such situations, the Air Force is transforming the current paradigm of developing and supporting isolated information systems connected by myriad interfaces to a network-centric approach based on the development and use of services, known as a service-oriented architecture (SOA). In an SOA environment, core services such as security, discovery, collaboration, and others are reused across multiple users and domains. In the previous scenario, a service-oriented approach would enable our UDMs to access the authoritative sources as soon as the data are available—without running manual reports or individual queries against multiple databases.

This service-oriented environment requires a robust, secure, singularly managed infrastructure. To support this requirement, the Air Force is developing a capability module approach to share information across functional communities. These capability modules are determined based on the community's needs and will be built gradually and affordably.

For example, an Air and Space Operations Center (ASpOC) capability module would support global and theater ASpOC command and control capabilities and require a secure connection to joint and coalition infrastructures. A combat support capability module would support business processes and require secure connection to the Internet for Airmen, their families, and retirees. An intelligence capability module would support intelligence processes and require secure connection to the defense intelligence backbone. These capability modules will operate through verified relationships to control the direction and nature of information exchanges and provide the necessary access rules.

A critical component of this strategy is the metadata environment, which is the set of technologies and business rules that allows users at all levels to find the information they are looking for—from the commander of a combatant command to the Soldier, Sailor, Marine, or Airman at a desk or in the field.

Today, when a Predator captures imagery over Iraq or Afghanistan, the data are sent both to the ASpOC in Qatar for immediate use and to the Distributed Common Ground System for analysis. The data are manually catalogued and stored in various intelligence databases. Finding the authoritative data becomes time-consuming and difficult for intelligence analysts because the data are stored in multiple locations.

With the implementation of the metadata environment, the Predator's video feed and imagery will be automatically tagged with the location, date, and other relevant information. Metadata (information about data) are important to making the information discoverable by users through search services, catalogues, and registries. In this scenario, intelligence analysts could discover and retrieve the Predator video using keyword searches, drastically reducing the time spent searching through multiple databases and file servers.

We will tackle larger and more complex problems as our Data Transparency initiative evolves. For example, one of our most critical products is the air tasking order (ATO), currently maintained as a large file formatted in United States Message Text Format. The result is an ATO that is difficult to parse and reuse for other mission planning and execution activities. Through metadata tagging, commanders could quickly and easily access historical ATO data to analyze the effectiveness of different ATOs or simulate different scenarios in an adaptive planning process. Data Transparency moves a future concept like this much closer to reality.

Governance Model

In August 2006, the Secretary of the Air Force, Michael Wynne, chartered the Transparency Integrated Process Team (TIPT) to govern the Data Transparency initiative. The TIPT addresses the need to rapidly share information with DOD, allies, and coalition partners by requiring the Air Force to make data visible, accessible, and understandable through a common vocabulary.

This governance body has already paid dividends. The TIPT recently identified significant overlaps among three joint initiatives requiring readiness data: the Global Force Management Data Initiative, the Force Management Integration Project, and the Deployment Readiness Recording System. The TIPT will ensure that each of these initiatives receives Air Force data from the authoritative source, resulting in an accurate representation of our capabilities. The TIPT also identified ways to reduce development costs by ensuring that the information for each of these joint initiatives came from a single set of interfaces.

The Next Steps

The Air Force's Data Transparency initiative supports all three of our leadership's priorities—winning the war on terror and preparing for the next war, caring for Airmen and their families, and recapitalizing and modernizing our air, space, and cyberspace systems. Data Transparency helps operational commanders make more informed decisions by providing them access to authoritative, timely, and relevant information. It gives Airmen needed tools to accomplish their missions and frees up resources for recapitalizing by slashing the cost of developing and sustaining redundant legacy systems.

The lifeblood of any decisionmaking process is access to the right information at the right time. Over the next year, we plan to implement our first true service-oriented architecture infrastructure and begin planning the enterprise-wide deployment of that infrastructure. We will deliver our first Data Transparency capabilities, exposing mission critical data to our flight schedulers and unit deployment managers. Our roadmap is dependent on working closely with our Federal, Department of Defense, and coalition partners to ensure that we deliver timely and accurate information to decisionmakers. **JFQ**

Electronic warfare officers aboard RC–135 Rivet Joint detect and locate signals

U.S. Air Force (File Photo)