Information Sharing Is a Strategic Imperative

General James E. Cartwright, USMC
United States Strategic Command

Americans are familiar with the host of new challenges posed by the forces of international terrorism, but one of the greatest threats we face may not be human at all, it may be a virus. John Barry's book "The Great Influenza" *details the flu pandemic of 1918 that killed more than 50 million people around the world. At one point, the flu spread so quickly that some government leaders feared a complete breakdown of civilization was only weeks away* [1]. *The Avian Flu might or might not turn into the next big threat, not only to the United States, but to its adversaries as well. The next big threat could be a natural disaster or something unanticipated.*

As the nation checks its horizon for the unexpected, it must not take its eyes off known threats and continue preparation for them. Both expected and unexpected cases require building a collaborative approach to face any threat America may face. As the realities of warfare and international security constantly evolve, the nation's strategy and willingness to work cooperatively must also evolve. There is a need for a collaborative approach among like-minded individuals and agencies to meet the challenges we face by merging our capabilities. A cultural change needs to take place across all the elements of international security to counter the threats faced today as well as tomorrow.

Successfully combating weapons of mass destruction (WMDs), for example, requires both military and civilian support to share technology and protect infrastructure. Failure to move beyond traditional boundaries risks sub-optimizing the potential for success. There is no alternative to establishing robust, collaborative relationships. The military, civil, and commercial interests of our nation all depend on the willingness to involve one another and fully enhance a shared worldview.

Facing Today's Adversaries

Among the challenges faced today are the unexpected, asymmetric methods that may be used by terrorists or other adversaries. These adversaries will not be reluctant to use WMDs: biological, chemical, or nuclear. Meeting the threat requires the ability to reach across all of the nation's security and defense elements to leverage the potential of America's economic and military infrastructure. This coordinated network must be able to effectively employ capabilities against any adversary.

The nation's economy, quality of life, and defense structures are all linked together in a global tapestry. The price of coffee and oil, a story on Al Jazeera, or a tsunami on the other side of the planet all have direct impact on daily life in this global environment.

Net-Centric Integration

Because America's vital military and economic interests are at stake, net-centric integration of our defense and security options provides a strategic advantage to face asymmetric threats. For its part in developing new approaches to integrate and synchronize actions, empower subordinates, and increase operational speed, U.S. Strategic Command (USSTRATCOM) is moving forward on two fronts. The first is re-tooling organizational and informational structures to make better use of all resources. The second front is actually more difficult. It involves changing the way human beings think about things and the military's basic cultural approaches to problems.

> *"The nation's economy, quality of life, and defense structures are all linked together in a global tapestry. The price of coffee and oil, a story on Al Jazeera, or a tsunami on the other side of the planet all have direct impact on daily life in this global environment."*

USSTRATCOM is transforming both old culture and old structure. One of the command's contributions in the world of information assurance (IA) and net-centric operations involves blogging on the newly installed Strategic Knowledge Integration-Web (SKI-Web) network. On my orders, any airman, seaman, or private first class can blog information on SKI-Web. Contributors buy their way into the blog with the value added – not the rank held. *Stars* and *stripes* are both welcome. Waiting for perfect information that plods through the same old napoleonic structure can make decisions irrelevant in today's world. To be effective, however, culture change also requires altering organizational constructs.

USSTRATCOM is also rebuilding its structure by establishing Joint Functional Component Commands (JFCC) that align responsibilities and authorities, decentralize operational execution, and increase operational speed. JFCCs are manned by STRATCOM planners and operators taken from our headquarters staff. Rather than build new organizations, JFCCs work side-by-side with and take full advantage of already existing centers of excellence that have complementary expertise and authorities.

JFCC Network Warfare (JFCC-NW)

JFCC-NW is collocated with the National Security Agency (NSA), and the commander of JFCC-NW is dual-hatted as the director of the NSA. While the structure has changed, real success requires alterations in culture. Military and government civilian teams must get used to doing business together rather than remaining in their old, comfortable lanes. They must establish

new lines of communication and new lines of authority. Both sides must be onboard to determine what procedures are required for mission execution and their joint role in IA. This effort is critical to supporting efforts to integrate and distribute the data that drives knowledge and ultimately action.

For information capabilities to be of real value today, warfighters must be able to *plug and play* in a joint global environment. Acquiring the ability to plug and play requires revolutionizing the mechanism for consistently incorporating information technology, controlling the configuration of technical components, and ensuring compliance with technical *building codes*. Professionals must constantly review the architectures necessary to provide this vital mechanism as it serves warfighters.

In this endeavor, JFCC-NW has a full partner in Joint Task Force Global Network Operations (JTF-GNO), now collocated with the Defense Information Systems Agency (DISA). The JTF-GNO commander also serves as the Director of DISA. Together they are treating networks as if they were a weapons system because they are certainly an extension of warfighting efforts. That fact is reflected in the training designed today as well as in the standardization of processes. In its current incarnation, JTF-GNO has been around for less than two years. It reflects a belief that the people operating networks should be the same people who defend those networks.

JFCC-Space and Global Strike (SGS)

As for USSTRATCOM's other mission areas, JFCC-SGS is responsible for integrating planning and command and control (C-2) support for the rapid delivery of extended range, precision effects in support of theater or national objectives. SGS mission responsibilities now require the capacity to rapidly and accurately reach any adversary on the planet with kinetic or nonkinetic effects. JFCC-SGS is led by the same three-star general who commands the 8th Air Force – a large part of USSTRATCOM's *global strike* arm. SGS plans global strike activities and serves as lead integrator of joint effects across the range of USSTRATCOM's capabilities. SGS also runs STRATCOM's Global Operations Center and serves as the commander's eyes and ears for situational awareness.

With the merger of the former with Space Command in 2002, the new STRATCOM also directs the deliberate planning and execution of assigned space operation missions. A new Joint Space Operations Center (JSpOC) has stood up, led by the same two-star general who commands the 14th Air Force – the largest part of STRATCOM's space arm. Establishment of the JSpOC and designation of a Commander, Joint Space Operations (JSO), brings true joint perspective and capability to the space operations world. The JSpOC cuts across boundaries to direct all elements of DoD space capabilities from daily space operations through space support to the regional combatant commands.

> *"It will take a team effort to meet challenges on issues as complicated as international treaty interpretation and as basic as the safety of our nation's food supply."*

JFCC-Integrated Missile Defense (IMD)

JFCC-IMD is headquartered in Colorado Springs, Co., to take advantage of missile defense activities located there. The commander of JFCC-IMD is dual-hatted as the commander of Army Space and Missile Defense Command. While the Missile Defense Agency has the specific assignment to develop missile defense systems, it continues to be the job of JFCC-IMD to offer a warfighter's focus and make the system operational by planning, integrating, and coordinating global missile defense operations and support (sea, land, air, and space-based).

JFCC-Intelligence, Surveillance, and Reconnaissance (ISR)

JFCC-ISR plans, integrates, and coordinates intelligence, surveillance, and reconnaissance in support of strategic and global operations and strategic deterrence. This includes coordinating ISR capabilities in support of global strike, missile defense, and associated planning. JFCC-ISR is collocated with the Defense Intelligence Agency (DIA) and the commander of JFCC-ISR is dual-hatted as the director of DIA.

Success in today's environment requires effectively coordinating all intelligence collection capabilities. The information collected must then be made available to a wide range of customers based on a secured *need-to-share* basis rather than the old *need-to-know* threshold.

Combating WMDs

In January 2005, USSTRATCOM was assigned the mission of integrating and synchronizing DoD efforts to combat WMDs and has looked to the Defense Threat Reduction Agency (DTRA) as a partner. The new WMD center is modeled on the other JFCCs, but is headed by a civilian director – in this case, dual-hatted as the director of DTRA. The first priority is rapidly advocating development and implementation of capabilities to support interdicting and eliminating WMD and its related materials. Since terrorists do not distinguish between America's civilian and military establishments, the nation must look at potential military and civilian targets and vulnerabilities alike. The WMD center links military interests with private industry leaders to share information, assess vulnerabilities, and develop deterrent, detection, and response capabilities. It will take a team effort to meet challenges on issues as complicated as international treaty interpretation and as basic as the safety of our nation's food supply. America is truly a nation at war, and private industry is certainly doing its part in supporting USSTRATCOM's newest mission area.

The Challenge of Change

As USSTRATCOM integrates joint, geographically separated, interdependent operations, technical issues must be worked out. However, the greatest challenge to building global integration will be achieving the cultural change referred to earlier in this article. This cultural change is not optional. It must occur in order to build a responsive command that can truly reach across multiple organizations and missions to deliver integrated joint effects. Everyone understands the need for change until it affects him or her personally. But moving further into the 21st century requires replacing *need to know* with *need to share* to achieve the full

strategic potential of net-centric operations. That means partnerships must grow and mature as the military, government, civilian, and industrial communities build on a long history of cooperation to optimize both current and future issues of interoperability. These partnerships must include the nation's best minds and resources in academia and private industry, as well as coalition partners and both the civilian and military sides of government.

Success requires adopting data-tagging standards and IA policies to increase government-wide, trusted information sharing. It requires supporting dynamic, persistent, trustworthy, collaborative planning, with user-defined operating pictures, using distributed, globally available information. The command is not there yet. But thanks to professionals in the military, government service, and private industry, USSTRATCOM is improving its global capabilities. That, in turn, will allow America's defense and security structure to take full advantage of the culture change as it evolves. To deliver the capabilities needed to combat the threats of the 21st century, USSTRATCOM is rebuilding and restructuring America's national C2 apparatus through a growing system of operation centers. Building these joint, geographically separated, interdependent operations meets our imperative need to pursue high capacity, Internet-like capabilities. It creates an indestructible C2 network as it extends the Global Information Grid to deployed and mobile users worldwide. This is vital to maintaining our traditional global deterrence at the same time we move all mission operations at the speed of light through high-capacity, virtual collaborative networks. The men and women who serve this command are aggressively moving out on actions to ensure USSTRATCOM fulfills its full set of global responsibilities, supporting national security needs in peace and in war.◆

Reference

1. Barry, John M. "The Great Influenza: The Epic Story of the Deadliest Plague in History." Penguin Group: New York, NY: 2004.

About the Author

General James E. Cartwright has served as commander, U.S. Strategic Command, Offutt Air Force Base, Neb. since July 2004. He leads an organization involved in the global command and control of U.S. strategic forces to achieve critical national security objectives. During his 35-year Marine Corps career, Cartwright held several operational and staff posts including commanding general, First Marine Aircraft Wing, and director, Force Structure, Resources and Assessment, J-8 the Joint Staff. As a pilot, he has flown the F-4, OA-4, and F/A-18.

United States Strategic Command
Office of Public Affairs
901 Sac BLVD STE 1A1
Offut AFB, NE 68113
Phone: (402) 294-4130
E-mail: hollanju@stratcom.mil

More Online from CrossTalk

CrossTalk is pleased to bring you these additional articles with full text at <www.stsc.hill.af.mil/crosstalk/2006/07/index.html>.

The New Java Security Architecture

Idongesit Mkpong-Ruffin and Dr. John A. Hamilton, Jr.
Department of Computer Science and Software Engineering
Auburn University
Dr. Martin C. Carlisle
Department of Computer Science
United States Air Force Academy

Java's original security architecture was designed to facilitate executing software from remote systems while simultaneously preventing downloaded code from performing unauthorized operations on host machines. The sandbox model of the Java Development Kit 1.0's security architecture was found to be too restrictive; therefore, the model was modified so that remote code could be allowed as trusted code. In the Java 2 platform, the notion of trusted code was removed and security control mechanisms were implemented that could be applied to both application and applet code so the code could be run with configurable trust. Java developers need to understand and incorporate the new Java security architecture into their development process to make certain their applications are secure. This article looks at the implementation of the new architecture and the new mechanisms provided for ensuring security for Java code. It details the motivation for the security changes in a security architecture, gives a general overview of the architecture added, and looks at some of the details of the mechanisms either changed or provided by the new architecture.

Software Cost Estimating: A Cyclical Conundrum

Ellen Walker
Data and Analysis Center for Software

This article describes the dilemma of some organizations in establishing credible software estimates, proposes some guiding principles and practices for improving the process, and addresses how current software best practices may play a role in the journey to achieving accurate software estimations. It seems that in spite of acquisition reform, in spite of our decade-long focus on achieving software process maturity, in spite of our adoption of modern structured development approaches, we (the software acquisition/development community) still have problems achieving success (defined as delivering a quality product on time and within budget). Perhaps the incentives are not strong enough to compel us to deliver quality. Perhaps our focus is skewed in favor of cost or delivery time over quality. Perhaps our cost estimating practices (or lack thereof) are impacting our success with software development. The hundreds of articles on software estimation and software metrics, and hundreds of hours spent in research and development of estimation techniques have not focused on the people and cultural issues surrounding estimating and data collection. Consequently, the reality of cost estimating and perceptions of practioners toward it, are, for the most part, vastly different from what the literature describes.