

Ensuring C4 for the Warfighter

By Lt. Col. Karlton D. Johnson, USAF
Commander, Pacific Air Forces Computer Systems Squadron

The Greek mathematician, Archimedes, wrote, "Give me a place to stand and a lever long enough, and I will move the world." In an age where people communicate at the speed of thought across the globe, computer networks are the fabled lever of which Archimedes spoke. Map that against today's battlefield environment and one begins to see exactly how prophetic Archimedes really was.

We live in a dangerous world. As Americans, we do not define ourselves by the attacks of September 11, but those events have shaped our responses to the plethora of terrorist threats against our nation and our way of life. Whether the battlefield is Afghanistan or Iraq, timely information remains a critical component for rapid decision making. And we as communication professionals are the linchpin for projecting that knowledge to the deployed warfighter. In the Pacific Air Forces, we facilitate the management of information flow via the PACAF Network Operations Security Center (NOSC).

NOSC 101

The NOSC's mission is straightforward: Provide the highest level of operational availability and oversight of communications assets within the PACAF theater of operations while maintaining an information assurance emphasis for the PACAF network enterprise. When viewed against the PACAF Senior Communicator (SC) Global Information Construct (see figure below), one can see that the NOSC is the only entity that seamlessly integrates throughout every layer of the model from policy to operations.

The NOSC is the execution arm of the PACAF SC and his primary

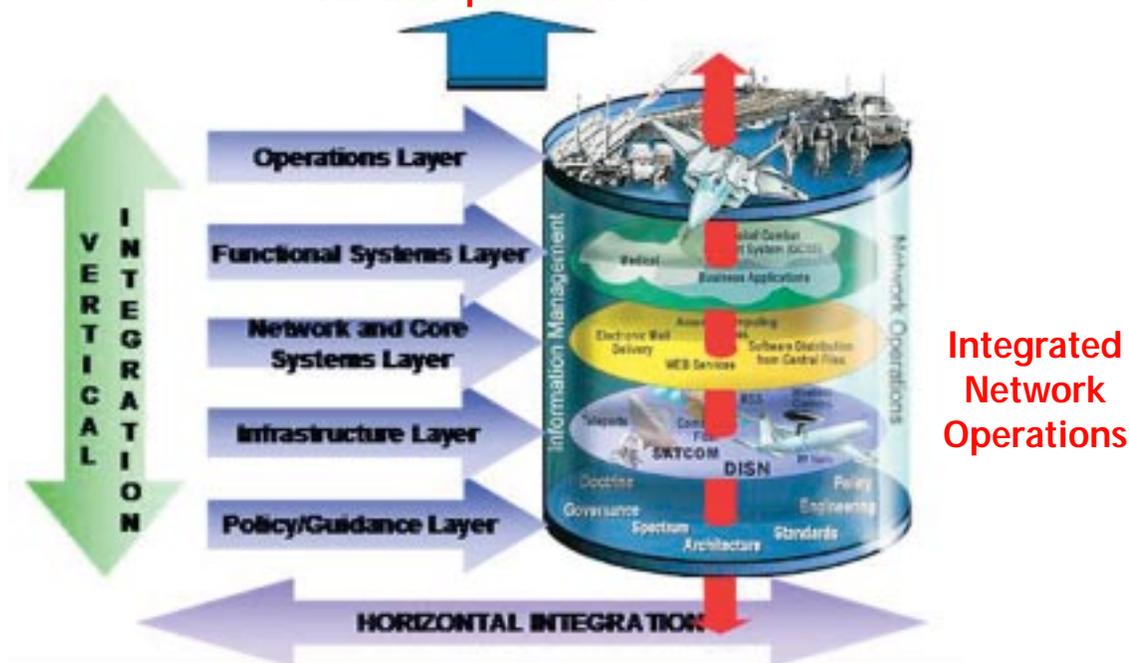
weapon system to ensure the warfighter's communications needs are met.

From an airpower perspective, one might compare the NOSC to the Air Operations Center. The AOC directs airpower for a theater and the NOSC directs Net Operations. In the PACAF construct, the NOSC has operational control over the PACAF enterprise network. This includes what we call "Boundary Protection" services, which is our version of "radar surveillance and integrated air defense systems" for the enterprise. We orchestrate this with Base Network Control Centers. Each NCC provides Tier 1 support for their customers (i.e., core services like e-mail, providing base level C4 support, etc.). They are the first line of network defense and the first level of customer service. When the NCC encounters a problem beyond their capability, they direct the issue to the NOSC, and we provide the next level of support. This includes sourcing support from industry partners who assist with network tools and technology. Additionally, the NOSC facilitates working relationships between various Department of Defense (DoD) organizations such as the PACOM Theater C4 Coordination Center (TCCC) and the Joint Task Force-Computer Network Operations (JTF-CNO) to guarantee enterprise information assurance during normal and contingency operations.

The Defense Department codifies Network-Centric Warfare as the "embodiment of the information age transformation of the DoD."¹ As the cornerstone for 21st-century battlefield dominance, network-centric warfare must be embraced by each Service. The NOSC affects Command-Centric Net Operations via three means: Infostructure Control (maintaining and controlling how we get

PACAF Operations Enterprise Model

Air and Space Power



from point a to b or information transport), Network Defense (how we defend the information) and Operations Support (how we provide day-to-day operations warfighter support).

Infostructure Control. We provide our communications professionals with specific guidance for managing Net Operations. The Special Instructions to Communicators (SINC) Manual provides detailed instructions on how we support communications in theater. Each day, the NOSC publishes the Communications Tasking Order (CTO), which delineates how we will “fly the network” for that day. As events occur, we issue communications Notices to Airmen (NOTAMS) to keep senior leaders informed of significant events. We use the tools at our disposal as our single pane of glass to view the state of the enterprise.

Command Network Defense. Our means of network defense employs a “Defense-in-Depth” strategy using a combination of firewalls, intrusion detection systems, relays and anti-virus protection to protect and defend the enterprise.

Operations/Warfighter Support. In PACAF, we’ve worked hard to integrate the services we provide to warfighters. In addition to monitoring computer network status, our NOSC also provides theater-wide Help Desk support which includes Air Traffic Control and Landing systems oversight, In-Transit Visibility and eventual Theater Battle Management Core System Unit Level (TBMCS-UL) Help Desk support. The NOSC is the one-stop shop — and not just for communications.

The Challenges

We have one major issue that encompasses our focus for taking net operations into the future, and we codify that in a concept we call “Operational Rigor and Discipline.”

What do we mean by Operational Rigor and Discipline? Perhaps a good start is to state what it is not. Imagine for a moment that you need a critical operation that will save your life. Now picture yourself with a doctor who decides to “wing it” rather than follow specific and rigorously defined medical procedures. What are the chances that you will survive? Operational Rigor and Discipline is the systematic process of creating clearly defined and documented procedures for a process. By following this process, we eliminate the “magic” that frequently appears to be the way of doing business in some enterprises, and it provides the platform for ensuring success by doing the same correct procedures over and over with positive results.

Two other significant challenges we are working are:

Configuration Control. Like any other large organization, we purchase services from a diverse group of vendors. The challenge, of course, is figuring out how to integrate these disparate services into a framework that provides the right information to warfighters at the right time.

Malicious Code. Another challenge we face comes from viruses and worms. The entire world recently suffered from the “Welchia.Worm” and “Blaster” virus attacks. Welchia, unlike embedded e-mail viruses, added a new twist by exploiting remote procedure call (RPC) vulnerabilities in networks. The result was degradation of services worldwide. In PACAF net operations, we view virus incidents as the equivalent of a Class B Mishap (loss of an aircraft and its associated loss of life). Without Operational



Above: The PACAF NOSC.

Rigor and Discipline, we needlessly increase our risk to the ever increasing spread of malicious code.

The Way Ahead

The NOSC is undergoing a vector change to enable PACAF “Predictive Network Battlespace Situational Awareness” through a detect-in-depth/defense-in-depth strategy. Additionally, we want to facilitate PACAF’s ability to conduct Capabilities-Based Net Operations throughout the theater of operations.

The PACAF NOSC’s way ahead is simple: lockdown the network. This means we need to facilitate enterprise standardization and provide configuration standards down to the desktop and through the NCCs. It also means we must facilitate the methodical, systematic deployment of new technologies in collaboration with our industry partners to assist in automating data gathering, and reporting and tracking of network status while eliminating unit-level “County Options.” Lastly, it means we must: (1) create new Tactics, Techniques, Procedures (TTP) for our people; (2) identify network processes; (3) focus on filling gaps in guidance; (4) identify training deficiencies; and (5) train to the standard. This entails using personnel with the right credentials to fly the network; codifying well-defined processes and procedures; conducting periodic “check rides”; and erecting strong standard/evaluation functions to sustain the effort over the long term.

In addition to the advanced technology we must leverage for success, we need our partners to provide us with the processes that go along with the tools. It does not help us to get the product first, deploy it and then find out that we need to execute within a specific framework after the fact. The process has to come first, so we can more efficiently leverage technology tools to achieve the desired effect on the enterprise.

We need our partners to continue an open dialogue with us and help keep us current on the latest and best technology solutions. Partnerships are one of the things that define us as Americans — our willingness to work together for a common cause. At the end of the day, each of us has a commitment to protect our troops and bring them home safely. The right technology mix helps make that possible.

Reference

1. Network Centric Warfare Department of Defense Report to Congress. Updated January 25, 2002. (<http://www.defenselink.mil/nii/NCW/>).