

AEROSPACE



From
the **Top**

By Col. Gregory Brundidge

PACAF Director of Communications and Information

To meet the demands of today's net-centric ops environment or battlespace, we must adapt a much broader construct for Information Assurance. Aerospace dominance, time-sensitive targeting, predictive battlespace awareness, and effects-based operations are now today's essential operational realities. Looking forward, we must further evolve these realities to achieve total battlespace awareness supporting real-time decision-making. At the center of all of these major operational muscle movements is "the net" - the aggregate of all network connectivity (terrestrial, airborne, and space), capabilities and processes. In this net-centric environment, information assurance is not simply ensuring that information is protected, accurate and delivered on time, but it is also ensuring that all the components involved in making that happen are postured, prepared, and ready to do so. To define IA requirements for the "net-centric" environment, we must widen the aperture and include more than the "-icities, -ilities, and -ations" normally associated with information assurance. For the big "IA" we must consider three pillars of technology, processes and people.

DOMINANCE & THE PILLARS OF

INFORMATION ASSURANCE



TECHNOLOGY

Relevant technical capabilities and mission-driven innovation

As industry continues to improve Information Technology capabilities to process, exchange, transfer and store more information, faster and better, we must demand the parallel development of information protection capabilities. The ability to achieve authentication, integrity, confidentiality, non-repudiation, and availability—the traditional elements of information assurance or what we call small “ia”—relies heavily on technologies that are on par with advancing information processing, networking, and storage capabilities. So, it’s not only important for us to be competent with today’s “ia” technologies, but we must always have an eye on the “ia” technologies for tomorrow. **Encryption, intrusion detection, firewall, and authentication tools for our networks must evolve and grow with other network capabilities.** This is especially important as more of these technologies are designed into network components vice the stand alone, add-on boxes. By staying in touch with those who perform network operations and deliver the full spectrum of network services, those who acquire these capabilities can ensure they deliver timely, usable, and relevant technologies for tomorrow’s “ia” demands. Failure to do this will lead to “late-to-need” technology advances, and result in unacceptable vulnerabilities and flaws in the net. **Equally as important as keeping “ia” technologies current, is the need to standardize on vendor solutions or, as a minimum, provide specifications for vendors to meet when providing hardware or software components for the net-centric environment.** This is an essential step to eliminating hard-to-manage, service disrupting variability in our networks and corresponding self-inflicted training and budget challenges in our control centers. We don’t acquire other weapon systems this way and neither do we expect our aircrews, and air, space, and missile operators to have to train for unmanaged variability in the systems they operate.

PROCESSES

CONOPS & TTPs

To achieve the desired product of a fully capable net-centric ops environment, the process for delivering the product is as important as the product itself.

Remember that the net-centric ops environment is the aggregate of all network connectivity, capabilities/services, and processes from the physical layer connections and protocols to net-enabled operational processes and applications. **To effectively command and control this environment there must be well defined CONOPS, policies, and procedures for governance, operation, and sustainment.**

Because NETOPS in the net-centric environment is a young operational discipline, we are in the process of developing many of these governing and guiding documents today.

The process component of big “IA” is critical because it enables optimized use of available technological capabilities. It does no good to have



superior information technology in our control centers if we don't have the processes in place that enable us to leverage its power and transform it into meaningful and relevant operational capability for the warfighter.

How often have we raced to field the latest hardware or software network tool or application only to complete fielding and find that we didn't evolve our ops concepts and procedures so that our net technicians and users could leverage its full capability?

To develop, implement, and sustain viable net-centric processes, it's imperative that we apply strong ops rigor and discipline to current NETOPS policy and Tactics, Techniques and Procedures and adopt a capability-driven model for developing and implementing new network tools.

The advent of a centralized standardization and evaluation program, such as SCOPE EDGE, is a critical first step.

It should form the foundation of a broader stan/eval construct that will assess all critical processes delivering the net-centric environment, to include network management, network administration, network defense and associated NOSC and NCC crew operations.

We will know we've achieved success when the TTP, checklists, bold print, and technical orders that govern these processes are in place.

Today, we routinely bring new capability as technology makes it available and then develop the required CONOPS driven processes and procedures after the fact, if at all.

Instead, **we must use a capability-driven model that brings new network capability as ops requirements dictate and adjusts CONOPS and associated processes and procedures prior to fielding.**

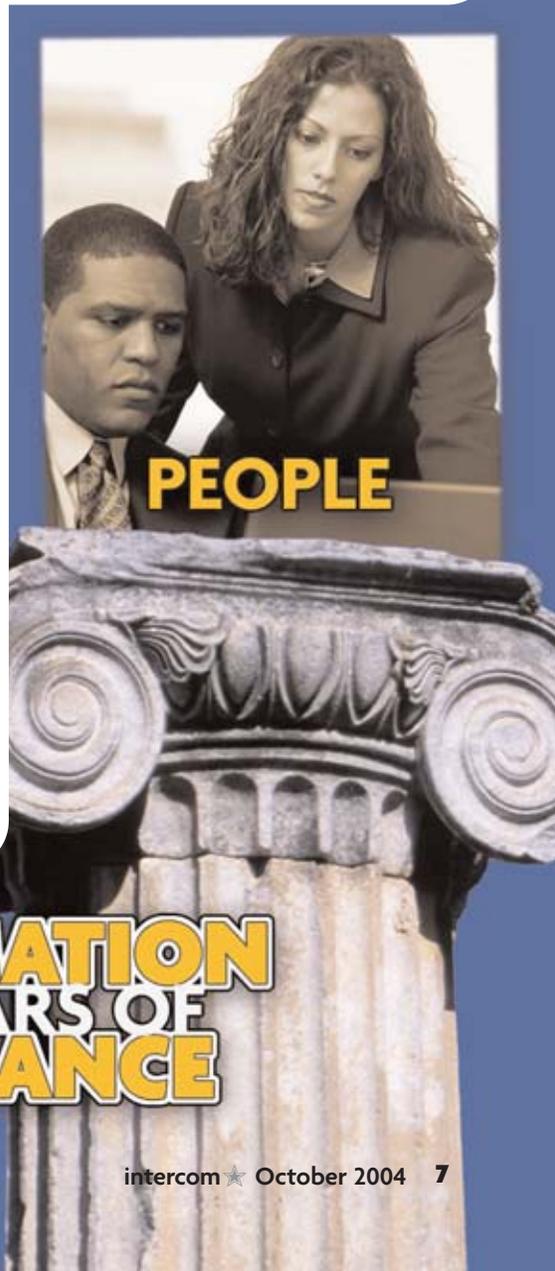
Ideally, we also train our technicians in advance, so we can transparently implement new capabilities without disrupting current NETOPS.

PEOPLE

Indoctrination, Training and Development

Drive-by fieldings, poor or no ops rigor and discipline, constantly changing configuration baselines, training turmoil and deficiencies, and non-standard hardware and software suites are all part of the environment in which we expect our network professionals to succeed. **The mindset of the net professional must be transformed from the world of data processing and specialized computing and messaging centers in which many of our mid-and senior-level technicians grew up.** In the net-centric environment, the essential mindset is one that understands the interdependencies of the net and fully appreciates the importance of standards in our technologies and processes. The transformed net professional realizes that a network risk or vulnerability assumed by one is assumed by all. To complete the necessary mindset transformation, we start with training processes that span the development cycle for the technician. From tech school to 7-level training, the program must be focused on building "interchangeable" net technicians. In addition to standardized training, we should endeavor to "push the envelope" wherever possible and take net warrior training to the next level. In industry, credibility comes from not only being able to deliver capabilities upon demand, but also from the level of certification one brings to the table. We should work toward getting our people mission-driven certifications recognized by the industry but focused on highlighting higher degrees of mission qualification. **Certifications such as "Certified Information Systems Security Professional," "Project Management Professional" and "Security A+" could equate to "specialist," "senior specialist" and "master specialist" ratings.** These ratings would mark the difference between those who dabble in our field and those whom we would consider to be experts. This produces a "win-win" situation for our military, our civilian counterparts, and for the individual. Additionally, it raises the bar for improving net-centric operations across all dimensions of the mission area.

As we standardize hardware and software on our nets, and the TTP we use to employ them, we pave the way for completing the necessary mindset transformation.



**INFORMATION
THE PILLARS OF
ASSURANCE**