The Team: Creating the Enabling Capability to Conduct Net-Centric Operations

Lt. Gen. Robert M. Shea
Command, Control, Communications, and Computer Systems

The ongoing transformation of the Department of Defense demands new capabilities that will enable Network-Centric Operations (NCO). While the Joint Command, Control, Communications and Computer (C4) systems community has been working toward this vision, emphasis has had to shift to a detailed plan to attain it. As a result, a critical task of the Director, C4 Systems Directorate, and the Joint Staff has been to provide the joint C4 community with a unifying strategy that would better integrate and synchronize our collective Joint C4 efforts and staff actions and deliver the C4 capabilities that will enable Joint NCO. After working with and receiving feedback from various Office of the Secretary, Combatant Command, Service (i.e., Army, Navy, Air Force and Marines) and Agency partners, the directorate delivered that strategy in 2004: the Joint C4 Campaign Plan.

2005 focused on the implementation of the Joint *Command, Control, Communications and Computer* (C4) campaign plan. As a result of these efforts, substantial progress has been made toward contributing to the delivery of critical, enabling C4 capabilities and preparing for future Network-Centric Operations (NCO). We are committed to ensuring that 2006 will be an equally productive year.

Accomplishments in 2005

Development of a contextual framework (concept documents) has been critical to supporting the review and approval of new capabilities as they moved through the Joint Capability Integration and Development System (JCIDS) process[1]. In support of this need, in 2005 the Joint Requirements Oversight Council (JROC) approved two critical C4 concept documents: the Net-Centric Environment Joint Functional Concept (NCE JFC), and the Net-Centric Operational Environment Joint Integrating Concept (NCOE JIC)[2]. The NCE JFC defines baseline functional capabilities and attributes required for NCO and will drive capabilities based assessments (CBAs) by identifying network-centric gaps and shortfalls. This analysis will ensure senior decision makers field future C4 capabilities that will *truly be born Joint*. The NCOE JIC will extend the NCE JFC's integrating framework, helping to establish the conditions, tasks, and standards needed to support CBAs that will define the specific net-centric needs of our future joint force. Together, these two concept documents lay the foundation that will support senior leaders as they assess needs and approve the development of solutions that will deliver future Joint C4 capabilities.

U.S. Strategic Command's (USSTRATCOM) Joint Task Force-Global Network Operations (JTF-GNO)[3] is responsible for the policy, guidance, and oversight that will transform today's Department of Defense's (DoD) information assets. We will move from a loose federation of inter-networked elements toward what will become the future capability – a robust Global Information Grid (GIG) Enterprise that will provide information where it is needed, when it is needed, and to those who need it most. Key to this transformation is the continued development of GIG Network Operations (NETOPS) policy and procedures. With the release of GIG NETOPS Version 2.0, JTF-GNO[4], working with the Joint Staff and all the *Combatant Commands* (COCOMs), lays the foundation for improving command and control (C2) relationships for network defense and operations throughout the GIG. JTF-GNO established a disciplined approach to network management that will enable the DoD to *operationalize*[5] the GIG.

The evolving net-centric environment has the potential to make joint networks our *Achilles heel*. Robust information assurance (IA) solutions are critical to providing the end-to-end capability that will deliver secure voice, data, video, and imagery. Trusted information must be accessible at all levels, including out to the *tactical edge* – at the right time, in the right format, and under every circumstance. Throughout 2005, Joint Staff Command and Control (J6) collaborated with the Assistant Secretary of Defense Networks and Information Integration/DoD Chief Information Officer (ASD [NII]/DoD CIO), Defense Information Systems Agency (DISA), JTF-GNO, COCOM, Services and other agencies[6] to improve our IA posture. As a result, department leadership awareness of existing cyber threats was significantly increased, and enterprise-wide security solutions for patching and conducting assessments were implemented (via the DoD IA/Computer Network Defense [CND] Enterprise Solutions Steering Group). The team also developed and implemented an IA annex to the Joint C4 campaign plan that provided the Joint community with a one-stop means for understanding and complying with IA policy and guidance.

The transformational vision of NCO requires a move from *stove-piped* and *interoperable* systems to interdependent systems. To achieve this end, the team focused on numerous information integration efforts. A key example is the partnership with the Office of the Secretary of Defense's Director of Operational Test and Evaluation, DISA's Joint Interoperability Test Command, and U.S. Joint Forces Command (JFCOM) to establish a joint network-centric test environment. By securing funding to conduct testing in a NCE, the process of linking interoperability testing with JFCOM's Joint National Training Capability training efforts was initiated. Another success came in the area of Joint C4 Interoperability Certification Process[7], where the Joint staff assessment was streamlined. By removing unnecessary interoperability certification reviews, COCOM and service staffing time was reduced, yet the net-worthiness of required joint C4 capabilities was still validated. Finally, review of interoperability issues affecting our warfighters in their current operating environments was increased. These reviews resulted in incorporation of Joint Operations lessons learned into interoperability test plans for 10 planned COCOM joint exercises. The work in this area will ensure lessons learned become lessons applied, and not lessons forgotten.

Any discussion of force transformation requires consideration of one of NCO's critical enablers: use of and access to the electromagnetic spectrum. Because spectrum remains a *high demand* but

increasingly scarce resource, the team has worked diligently during the past year with ASD (NII)/DoD CIO, to solve pivotal joint spectrum issues. The first concern related to providing the joint community, Military Services, and defense agencies with coordinated spectrum guidance. The result of this effort was the publication of the Spectrum Annex to Joint C4 campaign plan, an endeavor that provided our warfighting force with a strategy that defines, operationalizes, and will ultimately improve the management and use of the electromagnetic spectrum.

Spectrum-related issues of real-world operations were also examined. Many similar challenges were noted and solutions identified. As a result of this analysis, collaboration among departmental partners resulted in the creation of a dedicated spectrum Web site[8]. By making spectrum-related lessons learned more visible, our joint forces no longer had to waste valuable resources solving identified problems that already had proven remedies. We also went beyond analyzing spectrum issues. Again, working with our ASD (NII)/DoD CIO, COCOM, and service representatives, the team successfully obtained Joint JROC approval and funding for the development of two key spectrum management capabilities. The U.S. European Command sponsored Advanced Concept Technology Demonstration Coalition Joint Spectrum Management Planning Tool. When combined with the Global Electromagnetic Spectrum Information System program of record, spectrum managers at all levels will have the ability to plan and synchronize spectrum use to support operational demands on a near real-time basis, ensuring critical support to all spectrum-dependent missions.

Connectivity remained a 2005 priority and new transport and space capabilities were advocated. One of the lynchpins to successful NCO remains providing our joint forces with interoperability solutions that improve information flow throughout the battlespace. Creating this type of connectivity requires wireless solutions down to the *first tactical mile* with capabilities like the Joint Tactical Radio System (JTRS). Working with the COCOMS and Services, the JTRS program was re-scoped to ensure critical software definable radios will be delivered when needed to support joint warfighters. J6 also worked with ASD (NII)/DoD CIO and DISA to redefine the internet protocol (IP) environment regarding teleports. This effort will improve standardized tactical entry points and facilitate intra-theater and reach-back C4 capabilities for deployed forces throughout the world. Enhancing C2 systems continued to be a priority. J6 worked closely with the operational community to ensure the development of the Joint Command and Control System remains on track and enhancements continue to meet warfighter needs. Finally, worldwide, mobile access to satellite communications is crucial to current operations, as well as future NCO. A great deal of effort went into working with service and COCOM partners to advocate for and defend the funding of critical space capabilities that will be provided by initiatives such as the Advanced EHF system, Mobile User Objective System, and Transformational Satellite Communications System.

In late 2004, J6 met with service and COCOM representatives to discuss how to prepare Joint C4 planners to support real-world operations when deployed. While service C4 training was good, joint C4 training was virtually non-existent. Working with JFCOM and the Services and other COCOMS, the JROC approved development and implementation of a Joint C4 planners course. The course, which will be launched in 2007, will enable future Joint C4 planners to deliver the Joint C4 networks and capabilities that enable NCO.

Agenda for 2006

The key to success in 2006 will be constancy of purpose. Transforming Joint C4 capabilities to support future NCO will continue to be our focus.

The continued efforts of the Net-Centric Functional Capability Board and adherence to the JCIDS processes will ensure the foundational concept documents that were developed and approved in 2005 can be successfully leveraged. The first objective will be to complete the NCOE CBA – an effort that will result in a NCOE Joint Capabilities Document providing the contextual framework for service planners and developers to build the net-centric capabilities our joint forces will need in the year 2015 and beyond. Working closely with ASD (NII)/DoD CIO to complete the NCOE synchronization road map will also be a priority. This important analysis will enable the department to manage the delivery of baseline net-centric capabilities of the GIG and ensure their availability when and where the joint force needs them. Finally, working with USSTRATCOM and the JTF-GNO on improving the NETOPS Concept of Operations, as well as the joint NETOPS architecture, will continue.

As in 2005, 2006 activities will continue to support current and ongoing operations. J6, along with JTF-GNO, COCOMs, Services and agency partners will work to strengthen network command and control and NETOPS. At the same time, policies will be refined and exercises conducted to reflect evolving tactics, techniques, and procedures. Additionally, the entire Joint C4 community will work to improve the overall IA and CND posture in support of ongoing operations and initiatives. Finally, to strengthen current operations, end-to-end joint C4 configuration management will be improved. The focus will be on addressing roles, responsibilities, authorities, and governance structures affecting management control across the GIG.

To strengthen joint network security, the IA staff will continue to improve existing processes as well as work with key staff on critical initiatives in support of joint force IA requirements. For example, the C4 critical infrastructure protection assessments will be combined with IA assessments, creating a more holistic approach to managing initiatives used to protect networks.

In coordination with key department stakeholders, overarching policy in two key areas will be published. The first will streamline the acquisition processes and documentation related to developing security solutions for C4 systems. The second will implement DoD software assurance guidance. Strengthening information protection throughout the joint force will also be addressed. More specifically, the Joint C4 community has decided the time has come to accelerate Public Key Infrastructure (PKI) implementation to include developing and delivering signed and encrypted e-mail, smart card logon, and PKI authentication to Web servers. Senior Joint C4 leadership is committed to addressing concerns of our joint forces operating throughout the world. It is imperative that the problems experienced due to the lack of clear Joint Communications Security (COMSEC) policy and procedures be solved. The management and distribution of joint COMSEC materials used to support our warfighters will be improved.

Finally, two information sharing (IS) initiatives are underway. The first will develop a Joint IS strategy. The strategy must lay the foundation for transformational IS efforts and enable warfighters to make superior decisions in a timely manner. The second area will focus on IS programmatics with the objective of consolidating and standardizing the supportability and interoperability of current multinational systems including the Combined Enterprise Regional Information

Exchange System. The effort will also begin to formalize requirements for future multinational information sharing capabilities via the JCIDS process.

Key to the success of NCO is implementation of a comprehensive data strategy. Information integration was a priority last year and will remain one in 2006. For example, accelerating data strategy initiatives will be pursued in the following ways:

- By improving information sharing among the Services and Joint community on data strategy implementation.
- By promoting an understanding of data strategy guidance.
- By synchronizing Service approaches to facilitate a Joint process for community of interest (COI) governance.
- By establishing a formalized mechanism to coordinate warfighter domain data strategy efforts.
- By identifying gaps or issues in COI support of the warfighting mission area (WMA).

Other information integration areas will include Joint Interoperability metrics, testing, and validation. These efforts are essential for senior leaders responsible for making informed decisions regarding the lifecycle management of Joint C4 capabilities.

Electromagnetic spectrum will continue to be a Joint C4 priority in 2006. Without question, increasing awareness of issues related to spectrum and ensuring spectrum supportability requirements must be addressed early in the JCIDS and acquisition processes. Additionally, continuing to assist key departmental partners is part of the 2006 plan. Emphasis will be placed on establishing spectrum management training programs that prepare service spectrum managers to operate in the joint operational environment. Attention must also be given to creation of policies and methods to foster development and management of a qualified spectrum manager cadre. Finally, the Joint Staff will continue to work with COCOMS, Services and agencies to further the work being done by the Improvised Explosive Device (IED) Task Force including methods to mitigate the effects of IEDs on joint force operations.

Space and transport initiatives will continue to be a priority throughout the Joint Staff. Addressing space support will include reviewing the management process for commercial and military satellite communications. While conducting this review, refinements to software tools and processes allowing for greater accuracy, currency, and relevance of the information contained in the satellite communications database will be evaluated. Improving satellite support to the joint warfighter remains a top priority. Analysis of methods that could augment existing space capabilities will also continue. This will include consideration of new means to provide persistent, responsive, and dedicated *space-like* capabilities at tactical and operational levels to meet our growing joint force satellite communications requirements.

Other initiatives in 2006 will analyze methods to improve discipline in operations throughout the joint network. Since a risk assumed by one is a risk to all, working with JTF-GNO, COCOMS, and Services to ensure the commanders' capabilities to enforce network policy and procedures is essential.

Another area to be addressed is the department's ongoing effort to transition from IP Version 4 to IP Version 6 (IPv6). IPv6 will provide a virtually unlimited ability for the department to service addresses associated with the growing number of IP-enabled capabilities being developed to support NCO. Specifically, the communications-on-the-move capabilities that will be fielded will rely on the quality of service expected from IPv6. With a department goal to become IPv6 compliant by 2008, the staff will work with DISA, ASD NII/DoD CIO, COCOMS and Services to ensure the transition strategy is sound. Since funding constraints will require a phase-in of IPv6 capable assets over time, activities involving tests to ensure new and old systems are secure and compatible will be part of the transition strategy. Vigilance will be required to work with the key stakeholders to ensure our transition to IPv6-enabled capabilities does not disrupt ongoing operations.

Conclusion

The past few years have emphasized an improvement of network capabilities, especially with regard to secure information. Framing issues around operational terms has helped *de-mystify* the effect of C4 vulnerabilities on the warfighter, both now and in the future. We are committed to continuing a dialogue with the operational community to ensure an understanding of how pressing Joint C4 issues apply to and affect them. More importantly, we look forward to continuing to work with our Joint C4 Community partners to deliver the Joint C4 capabilities that will continually move the force closer to the NCO's vision for the future.◆

Notes

1. For more on JCIDS process, go to <www.dtic.mil/cjcs_directives> and see Chairman Joint Chiefs of Staff Instruction 3170.01E.
2. See <www.dtic.mil/futurejointwarfare> and click on JICs.
3. See <www.stratcom.mil> for more on JTF-GNO.
4. See <www.stratcom.smil.mil> for more on GIG NETOPS.
5. *Operationalize the GIG* means treating it with the same kind of rigor and discipline that is applied to other weapons systems and those who control or operate them.
6. See <www.defenselink.mil> to learn more about ASD (NII), DoD Agencies and Combatant Commands.
7. See <www.dtic.mil/cjcs_directives> CJCSI 6212.01C.
8. See <www.js.smil.mil>, J6, MCEB Secretariat, Spectrum Branch.

About the Author

Lt. Gen. Robert M. Shea serves as the Director, Command, Control, Communications and Computer Systems (C4 systems), The Joint Staff. He is the principle advisor to the Chairman, Joint Chiefs of Staff on all C4 systems matters within the Department of Defense. Shea's military service spans 33 years. Prior to his current assignment, he was the Deputy Commander, U.S. Forces, Japan. Shea's command positions include: Commander of the Marine Component to the Joint Task Force Computer Network Defense, Director of the Marine Corps Command and Control Systems School, Commanding Officer, 9th Communications Battalion, and I Marine Expeditionary Force during Desert Shield and Desert Storm. Other assignments include Commanding Officer of two communications companies and the Battalion Communications Officer for 1st Amphibian Tractor Battalion, 3rd Marine Division.

JS J6 DAG
ATTN: Col. Anderson or
Lt. Col. Patricola
The Joint Staff, J6-DAG
Washington, D.C. 20318
Phone: (703) 571-9750
E-mail: john.patricola@js.pentagon.mil or roarke.anderson@js.pentagon.mil