



### SENIOR LEADER PERSPECTIVE

NSCI's Larry McKee recently had the opportunity to interview Maj. Gen. Kevin Kennedy, director of the U.S. Air Force Joint Capability Development, U.S. Joint Forces Command, regarding the organization's cyberspace capabilities and efforts.

**NSCI: As the lead for the Department of Defense Joint Experimentation, what concepts, organizational structures, and/or emerging technologies is JFCOM looking at to improve the department's cyberspace capabilities?**



**MAJ. GEN. KEVIN KENNEDY:** As the DoD lead for Joint Experimentation, we base our experimentation campaign on support to warfighters. Before we look at concepts, organizational structures, or emerging technologies, we must define what military problem we are trying to solve. That means we must do the necessary research to ask the right questions, or risk getting the wrong answers. Joint Operating Environment 2008, a JFCOM report, outlines a strategic framework and forecasts possible threats that will challenge the future joint force. The exponential growth of cyber and information technologies is one of several trends we've identified and we're addressing that in several ways.

Right now, we have a two-year Joint Concept Development & Experimentation (JCD&E) project to address challenges in cyberspace operations. We want to achieve two things through these efforts: improved integration and synchronization of computer network attack, defense; and exploitation as well as improved integration and synchronization of cyberspace and information operations. We're also working with our partners to provide foundational concepts for joint cyberspace operations.

In examining the cyberspace domain, we must remind ourselves that war is a human endeavor. Adversaries will challenge us in multiple ways; first, by constructing opposing "strategic narratives" distributed throughout multiple networks to change beliefs, perceptions, attitudes, and behaviors in their favor. Additionally, we must assume our networks will be attacked. No matter what technology emerges, it will not be a panacea. We cannot be lured by promises of decision-making machines and perfectly protected networks; instead we must be ready and able to continue operations even with degraded supporting networks.

**NSCI: Can you tell us a little bit about how JFCOM's Global Force Management efforts are, or will be, helping commanders request and receive cyberspace forces?**

**KENNEDY:** Adversaries do not wage discrete land, sea, air, space or cyberspace wars – instead they use all elements of power to wage war. As a global force provider, we need to address each situation on its own terms.



## *Keeping Cyberspace Professionals Informed*

The Global Force Management construct has improved both the efficiency and effectiveness of Combatant Commanders' force requirements identification, submission, validation, force provider assignment and force sourcing processes. Most recently, the implementation of the Joint Capabilities Requirements Manager (JCRM) tool enabled the GFM community to consolidate all force requirements (including Cyber-Space force requirements) into a single Web-based management tool. This facilitated more informed and efficient force sourcing. We will continue to refine these processes and tools. We must improve our ability to provide forces – cyber or otherwise – in a careful and considered manner.

***NSCI: According to JFCOM's Web site, one of the command's goals is to "Design Integrated, Properly Structured Command and Control." Can you tell us about any initiatives JFCOM has underway to integrate the command and control of cyberspace with other domains (e.g. maritime, ground, air and space)?***

**KENNEDY:** One of our areas of emphasis at USJFCOM is to design integrated, properly structured joint command and control. Command and control is not synonymous with network operations or advanced technology. We need to enable joint interoperability from the beginning by sharing information, training, planning and technology. As the Department of Defense portfolio manager for Joint Command and Control, we work closely and transparently with the services and Combatant Commanders to provide needed capabilities.

One initiative JFCOM has underway is a Cyberspace C2 Assessment Team. We formed this team, in support of the National Military Strategy for Cyberspace Operations, to analyze existing command and control processes for their adequacy in conducting operations in the cyberspace domain. The JFCOM-led team then conducted numerous workshops and data calls with Combatant Commands, services and agencies to develop recommendations for improving and integrating command and control of the cyberspace domain with the other domains. Our goal is to integrate cyberspace into joint doctrine, joint training and joint experimentation. Our focus is on empowering commanders at all levels.

***NSCI: The Services appear to be leaning forward to ensure they are positioned to train and equip "cyber warriors" in support of Combatant Commanders. What is JFCOM's role when it comes to training cyberspace professionals?***

**KENNEDY:** The future landscape requires unprecedented levels of flexibility and adaptability. Adversaries will work to blur the line between political conflict and open war. We must build a force that is adaptable, agile and resilient. Joint warfighters demand and deserve improved training/education and integration, as well as robust and agile equipment. Realistic, timely and responsive joint training, along with agile and robust command and control network design, can underpin warfighter success.

At USJFCOM, we provide Combatant Commanders exercise design support to ensure the exercise environments replicate the operational environment (to include supporting command and control networks). Subject matter experts from the information operations and cyberspace operations communities assist in the planning and execution of joint exercises. Cyberspace activities in our training



## *Keeping Cyberspace Professionals Informed*

evolutions include an accurate portrayal of current policies, authorities, threats, capabilities and challenges across all aspects of cyberspace operations.

We will continue to work closely with the Joint Staff, USSTRATCOM, other Combatant Commands and the services to ensure U.S. forces are trained to conduct operations effectively in and through cyberspace.

***NSCI: The Tidewater area of Virginia has long been a DoD leader in areas such as Modeling & Simulation, Command & Control, and Experimentation. Do you have any thoughts on how industry and academia expertise in these areas may be able to help the department with improving cyberspace capabilities?***

**KENNEDY:** We are continually investigating, reviewing and applying the best of current business practices to our DoD processes to ensure the intellectual capital of the business community is leveraged to save U.S. taxpayer dollars. Effective cyberspace capabilities will require the combined efforts of industry, academia and DoD. Industry and academia offer a comprehensive suite of security tools for cyber warfare and can provide solutions for cyber defense and attack by using state-of-the-art technologies that include encryption of data at rest, secure wireless networks, rapid internet protocol traceback and Web-based forensic databases for automatic verification of hardware/software integrity. We want to enable joint interoperability from the beginning through our efforts in establishing standards, sharing information, training, planning and technology.

***NSCI: Given the ongoing cyberspace attacks on DoD and industry networks, what is JFCOM's Joint Center for Operational Analysis (JCOA) doing to collect and analyze cyberspace lessons learned?***

**KENNEDY:** We must capture enduring battlefield innovation and lessons and apply them after rigorous testing and evaluation. The Joint Center for Operational Analysis (JCOA) conducts studies at the request of the Secretary of Defense, the Joint Staff or a supported Combatant Command. To date, JCOA has not been asked to conduct a systematic study of lessons learned for defending against such attacks. One thing that is very clear is the enemy has decided to take us on in the cyber domain, and we will not let him steal a march.