CyberPro

March 10, 2011

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: MAJ. GEN. DALE MEYERROSE (USAF, RET.)

NSCI's Charles Winstead recently had the opportunity to interview General Dale Meyerrose (USAF, Ret.) who currently serves as the Vice President and General Manager for Cyberspace Solutions at Harris Corporation. Gen Meyerrose spent over three and a half decades in public service. The first 30+ years he was in the United States Air Force, the last three years in public service as the first President-appointed, Senate confirmed Chief Information Officer of the Intelligence community. He spent most of that service in cyber communications, information technology, intelligence, command and control operations, and space support. Gen Meyerrose graduated from the United States Air Force Academy in 1975 with a degree in Economics. He also has a Masters Degree in Business Administration from University of Utah.

NSCI: Harris Corporation announced the opening of a Cyber Integration Center in May 2011. Can you tell us a little bit about how that center will help to improve cybersecurity and/or the center's capabilities in general?

MEYERROSE: The information technology world is moving from the network-centric operations to the cloud for reasons of performance, availability, and cost. It's not a matter of if, but when. The Cyber Integration Center is the trusted platform from which Harris will deliver trusted enterprise cloud environments to industry, academia, and government clients. Our differentiation starts from this platform that has both physical and virtual protection built into its every fabric. We will then use hundreds of thousands of virtual machines to provide services and technology that continuously monitors every activity to create explicit trust and exceptional value to those we serve.

NSCI: What key challenges should be tackled over the next year or two?

MEYERROSE: While the professionals working issues in this arena have made remarkable progress over the past several years, the "bad guys" continue to have an unfair advantage in cyberspace. I refuse to accept this condition as unchangeable—particularly for a domain on which so much of the world's economy depends. We need leadership from the public and private sectors to define new responsibilities for government, industry, and consumers. And we need to recognize that technical talent and innovation will be the cornerstones of future growth and prosperity.

NSCI: You've commented before on the need for Cyber standards. What standards do you think would bring the most bang for the buck?

MEYERROSE: The free-lance attributes that created the necessary incubation for the Internet and resultant Information Age will not likely create the environment to reliably support almost every other

aspect of human interaction. I know that when most folks hear the words "standards" and "information technology" linked together, thoughts immediately turn to machine-to-machine specifications. While important, we need to expand our thinking to include legal and business conduct, data and intellectual property rights, and international implications of this man-made, borderless, virtual domain. I believe that we are so nascent with respect to creating even the most basic cyberspace standards, technical and otherwise, that the priority needs to be on moving forward on any aspect rather than arguing which is most urgent. We don't need paralysis by analysis—we need action.

NSCI: The cyber supply chain and the insider threat seem to continue as areas of great concern. Any insight into how Harris Corp. handles these?

MEYERROSE: Our approach to establishing client trust in all Harris products and services starts with supply chain integrity. This understanding not only encompasses traditional concepts of hardware and software, but extends to physical plant, human reliability, and product and service management. From our perspective, particularly regarding the cyberspace supply chain, one has to start with solution architecture, and manage risk through the remaining life cycle of manufacture, distribution, installation, and maintenance. Any short cut in this process potentially negates the technology investment and trust in operations and desired outcomes.

NSCI: The Commerce Department was recently handed the baton regarding Trusted Identity. DHS has the responsibility for protecting critical infrastructure, working with industry and DoD's USCYBERCOM. In general, how would you say we are doing with regards to clarifying cyber-related roles and responsibilities?

MEYERROSE: The attacks of 9/11 have driven our U.S. Government to examine and adjust information technology responsibilities and information sharing roles for the past decade. We are much improved from that baseline, but at the same time the challenges have grown more difficult and complex. There is not an even alignment of cyber talent, expertise, and responsibilities across the Federal agencies—which is perhaps the biggest task at hand. Unfortunately, the only public measurement is the latest breach, intelligence shortcoming, or seemingly exorbitant cost of service. This situation belies the significant progress of the last decade. In my view, we are sufficiently organized and capable of handling more cyberspace roles and responsibilities than most believe, but not all—giving critics sufficient intellectual "ammunition" to build credible fear-based arguments.

NSCI: Pictures of China's J-20 recently surfaced. There was an article in the Wall Street Journal in April 2009 alleging China had hacked into DoD computers containing F-35 design information. How would you characterize our progress in reducing or eliminating future data breaches? Is DoD working more closely with defense contractors, such as Harris Corp, to ensure critical data is protected?

MEYERROSE: The DoD, and most other departments recognize the need to develop new partnerships with contractors supporting the U.S. Government. The most prominent mechanism created in the past half dozen years is the Defense Industrial Board—responsible for forging new accountability processes among the government and DoD contractors. While progress is laudable, there remains much work to

do by all involved. I believe that other agencies within our Government will need to adopt a similar approach in the future with their supporting "cottage industries."

NSCI: We've seen numerous universities ramp up their cyber-related programs for undergraduates and graduates. I think Harris has worked with the University of Florida and the Florida Institute of Technology in this area. How is that going? And how do you think we can also improve the awareness of cybersecurity vulnerabilities, threats, and risks to everyday internet users?

MEYERROSE: Harris has long supported universities and national institutes to develop technical talent to support industry and government needs—the two that you cite are but a couple examples of many. Harris support of the University of Florida programs helped their goal of growing its national reputation as an engineering center of excellence. And our company created the Harris Center for Information Assurance at the Florida Institute of Technology a couple years ago. Not only has that effort developed critical technical talent for Central Florida, but performed needed research in this rapidly developing market sector.

NSCI: Last question, unless you have something to add. If you were still serving as a government official and had "one more dollar" to spend on cyber - where would you put it (e.g. defense, offense, exploitation, situational awareness)? Why?

MEYERROSE: While many focus on the technical elements of cyberspace, I submit that our biggest challenge lies with education of our workforce and talent development. Over 30% of our young people fail to get a high school diploma—and three-quarters of Americans from ages 17 to 24 are unfit for service in the U.S. military. Neither of these statistics provides encouragement about the future of the U.S.'s ability to compete in the future. While I remain optimistic based on my faith in America to rise to the challenge, this is a "high mountain" on which we must focus—and climb sooner rather than later.

NSCI: Is there anything else you'd like to add?

MEYERROSE: I appreciate that your organization puts a spotlight on the ever growing cyberspace industry—and urge you to continue in this endeavor. The workforce is constantly moving the "technology cheese" and demands better access to information through cyberspace. And those responsible for delivering this information capability need to concentrate on staying relevant today, while keeping an eye on the future.

NSCI: Thank you very much for taking the time to visit with us.