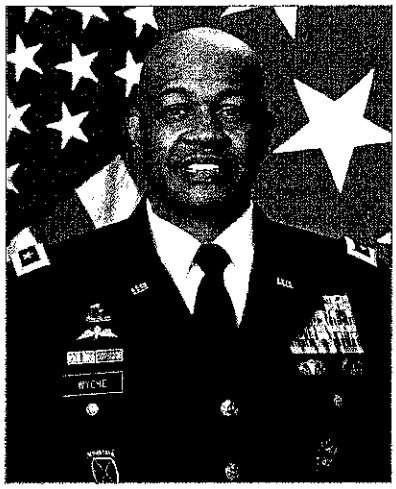
Attacking Cyber: Increasing resilience and protecting mission essential capabilities in cyberspace

Lieutenant General Larry Wyche
Dr. Dawn Dunkerley Goss

We are entering a new era of evolving threats, advancing technologies, and reduced resources. Adversaries continue to exploit weaknesses within interconnected systems, such as the Enterprise Resource Planning solutions that now power the Army's daily operations through the aggregation and analysis of vast amounts of data, sometimes from dozens of sources. Each of these sources brings its own level of threat and vulnerability, leading to an incredibly complex environment ripe for exploitation. Despite these challenges, Army Materiel Command (AMC) is employing an aggressive cyber strategy to ensure our resilience within an increasingly congested and contested domain.

In our growing, sophisticated, and evolving cyber threat environment, we have a particularly complex operational environment based on the global range of our missions coupled with the composite of public and private infrastructure storing and transmitting government and partner data; for example, over a thousand suppliers support the Organic Industrial Base (OIB) alone. From the research and development of cutting-edge materiel solutions to the ongoing Retrograde from Afghanistan, our competencies are facilitated through the use of Information Systems and platforms that are often not under AMC control, sending information across networks that are compromised. This requires us to understand and manage the underlying supply chain, gain the ability to recognize attacks or intrusions when they occur, take immediate steps to mitigate these attacks, and then execute alternate processes as required, as real-time as possible, in order to complete the mission.

Recent events within the cyberspace domain have brought attention to the fact that we must take aggressive steps to better protect our critical data. The AMC Commanding General recently approved a ***Cyber Mission Assurance Plan*** to provide a supporting roadmap to be resilient during a time where all our critical functions rely on networks and access to information. In this plan, well-defined Lines of Effort assign responsibility



Lieutenant General Larry Wyche is the Deputy Commanding General of the U.S. Army Materiel Command, one of the Army's largest commands with 64,000 employees impacting 50 states and 145 countries. He also serves as the Senior Commander of Redstone Arsenal. He began his career in the enlisted ranks and achieved the rank of sergeant while serving as a Calvary Scout leader. He previously served as the Commanding General of the U.S. Army Combined Arms Support Command (CASCOM) and the Sustainment Center of Excellence at Fort Lee, VA. His previous assignments included Deputy Chief of Staff, 3/4, U.S. Army Materiel Command, and the Commanding General of the Joint Munitions and Lethality Life Cycle Management Command/Joint Munitions Command.

Lieutenant General Wyche received his commission as a Quartermaster officer from Texas A&M University, Corpus Christi ROTC, and graduated in 1983 earning a Bachelor of Business Administration. He earned master's degrees in Logistics Management from the Florida Institute of Technology and National Resource Strategy from the Industrial College of the Armed Forces.

within the command and establishes the required objectives and milestones to achieve the desired end state—that we have trusted and resilient infrastructures, systems, platforms, and processes that assure mission performance through improved cybersecurity, increased protection of cyber key terrain and information, strengthened network defenses, and a trained and aware workforce that implements best cyber practices from both government and industry. These objectives are then tracked, along their critical path of implementation, via the use of metrics assessing both the success of implementation and the level of positive effect on the command's cybersecurity posture.

A *Test-Assess-Revise* methodology is required, given the rapid evolution of cyber threats, cyberspace doctrine, and the network environment. As the threats are already so active and are growing, we cannot wait to start these activities until we have the 'perfect' solution. However, given the austere resource environment and the unknown effectiveness and efficiency of some of the proposed actions, we are testing and assessing high payoff and low resource cost activities. We have focused on those activities that increase resilience and are effective, sustainable, and efficient: improved internal and external information sharing, promoting cultural change across the workforce, and pursuing team-oriented solutions leveraging the best of public and private cyber expertise.

Key to success is improved internal information sharing and collaboration across all stakeholders. We are actively engaged with the Department of the Army Staff, Army Cyber Command (ARCYBER), and supported and subordinate commands to ensure cohesive unified action, and to maintain mission assurance and the freedom to operate across the entire enterprise. Enabling greater mission com-

Dr. Dawn Dunkerley Goss is the Chief of the Cyber Division, AMC G-3/4. Her team is responsible for AMC's operationalization of cyberspace to achieve the AMC commander's objectives, facilitate mission command, and maintain AMC's ability to *develop, deliver and sustain* in support of current and future Army and Joint missions.

Dr. Dunkerley Goss received a Ph.D. in Information Systems from Nova Southeastern University in 2011 with a doctoral focus of information security success within organizations. Her research interests include cyberwarfare, cybersecurity, and the success and measurement of organizational cybersecurity initiatives. She holds a number of professional certifications, including Certified Information Systems Security Professional (CISSP), Information Systems Security Architecture Professional (ISSAP), Information Systems Security Engineering Professional (ISSEP), Information Systems Security Management Professional (ISSMP), Certified Secure Software Lifecycle Professional (CSSLP), and Certified in Risk and Information Systems Control (CRISC).

mand and developing cyber resilience across AMC, specifically within the AMC workforce, and facilitates our ability to operate and defend our cyberspace terrain. Legacy processes, methods, and cultural paradigms must yield to a new concept that cyberspace is an operational domain with continuously changing and contested terrain. All operations have risk—it cannot be eliminated, so that risk must be understood and managed actively. We will never 'graduate' from this challenge, and can never stop in onr efforts to improve our cyber resilience.

To meet the challenges of the contested cyberspace environment, a cultural change in the workforce is required to promote all IT users and professionals using best practices in cyberspace in order to operate in a manner that promotes, not hinders, our cyber resilience. The workforce is transforming the way it thinks about cybersecurity. As we continue to train, organize, and equip to take full advantage of cyberspace's potential, we are recognizing that adversaries want to undermine our ability to operate freely within this domain. Every time we enter cyberspace, regardless of where we are, recognizing we are in a contested environment is a fundamental requirement. Anticipating threat attempts to disrupt us, and consider the effects of an adversary's potential ability to destroy friendly networks should be a standard procedure. The protection of information and ability to guarantee its transport though cyberspace will be essential to our operations. Increasing cyber resilience is an imperative at all levels (User, System Administrator, system, network, etc.), as well as additional integration of cyber into all missions to leverage the opportunities of cyberspace and ensure that we maintain future advantage over our adversaries.

Employing a logistics and sustainment enterprise-

level cyber strategy is a total team effort, and requires active participation from all stakeholders, and more broadly across the acquisition community. Both effectiveness and efficiency must be considered within the equation, as well as partnerships with organizations in academia, government, and industry to identify and solve long-term challenges, develop capabilities and capacity for the future, and recruit and retain the best cyber experts.

All operations have risk—it cannot be eliminated, so that risk must be understood and managed actively.

We are the Army's subject matter experts on Materiel Development and Sustainment and will meet the challenge of maintaining our freedom to operate in cyberspace by leveraging the cyber experts and technology needed to execute our mission.

This plan towards resilience in cyberspace has already helped AMC increase our emphasis on cybersecurity and pursue our vision of being ***The Premier Provider of Army and Joint Readiness to Sustain the Strength of the Nation.*** However, we have much more to do, both in assuring situational awareness and protecting our cyber key terrain through innovative solutions in a time of fiscal constraint, remembering that brave Americans around the world continue to depend on us.