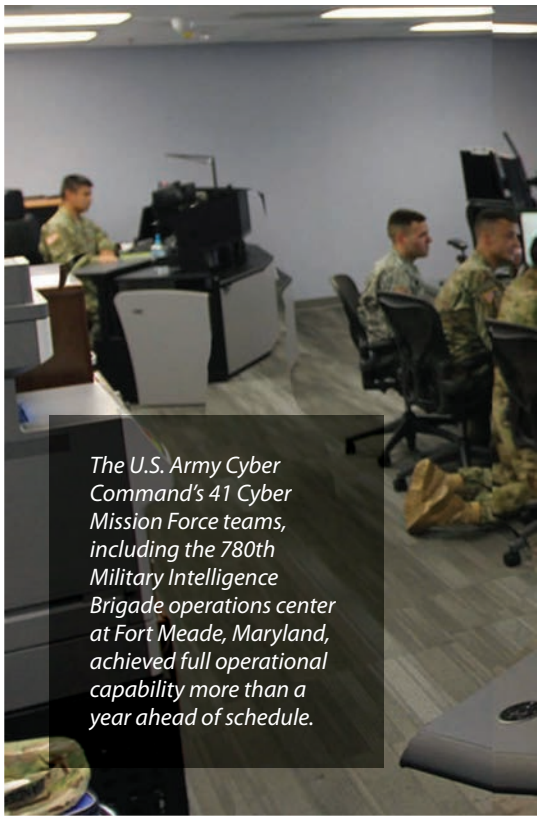
Joint Force Looks For a Leg Up In Cyberspace

U.S. Cyber Command envisions unified capabilities and a way to rapidly integrate emerging technology.

BY MAJ. GEN. GREGG POTTER, USA (RET.), AND CHRIS VALENTINO



The U.S. Army Cyber Command's 41 Cyber Mission Force teams, including the 780th Military Intelligence Brigade operations center at Fort Meade, Maryland, achieved full operational capability more than a year ahead of schedule.

The U.S. Cyber Command's Cyber Mission Force must keep pace with a threat landscape that is evolving at an unprecedented tempo. Cyberthreats are constantly growing in volume, velocity and sophistication, and the force needs a warfighting platform that will allow it to get ahead of attackers. That platform should enable continuous improvement through iterative development at the speed and scale of military operations.

Equipping the Cyber Mission Force (CMF) with integrated full-spectrum cyber capabilities as part of a joint warfighting system is critical. The force, which has more than 6,000 service members and civilians and is expected to reach full operational capacity by the end of this fiscal year, protects the United States from hostile actors and projects power within cyberspace to support combatant commanders and CMF objectives. Cyber Command's vision is to field a system that unifies capabilities across the services and includes the ability to rapidly integrate emerging cyber technology and programs. The command refers to this future state concept as Unified Platform (UP).

UP will provide the means to seamlessly integrate defensive and offensive operations to support the U.S. Defense Department's cyber strategy. Two main elements will create the foundation for this warfighting system: an agile development process to facilitate increases in size and capability, and strong partnerships within the Defense Department and industry to produce capabilities that enable mission success.

While developing UP is a large, complex undertaking, lessons learned from numerous other elaborate software development programs can be applied to the effort. Chiefly, the process to acquire major weapon systems needs to be dynamic enough to deliver capabilities at the speed of need for cyber warfighters now and into the future. This means taking advantage of agile development.

Integrating systems engineering and software development processes enables agile development in "sprints" based on mission threads and operational needs. This method allows speedy development, incorporates user feedback and maintains system capabilities at a level consistent with the rate of change. Partnerships between government and industry are essential to ensure that the process, including priorities and trade-offs, stays on track and that tests and capabilities are done on or ahead of schedule.

An agile approach includes thinking at scale while breaking a problem into distinct mission threads. It gives military commanders the option to deliver capabilities now, even as a program continues to mature.

Using the agile process, coupled with flexibility around requirements, ensures that needed capabilities address current threats while leveraging the latest innovations. This process is not free of requirements but allows for flexibility. The key to success is balancing risk to the government and industry while working as partners

Steve Stover

to develop critical capabilities and accomplish the mission.

Because of the complex nature and scale of the military's cyber operational environmental, capabilities cannot simply be bought off the shelf. They must be developed jointly with input from industry and government experts, which calls for an unprecedented level of collaboration.

With the rapidly changing nature of cyber attacks, this is true now more than ever. Industry's complete understanding of the mission and systems integration, as well as its ability to focus teams on these complex challenges to help solve problems at scale, is essential.

UP necessitates a strong partnership that brings forward the best of industry, academia and government. An effective program structure will unite these critical assets to provide groundbreaking solutions and capabilities to the CMF. This approach not only secures the best talent for the mission but also comprehensively manages risks in this fast-paced, ever-changing environment. Partnerships, if developed with the criticality of this mission set in mind, will make the cyber force stronger and more capable in the face of escalating threats.

U.S. military power has evolved over the decades but continues to be strong and stable. UP, as a military capability in a new domain, will help mature and keep the United States ahead as it operates in cyberspace.

Although creating a warfighting platform that unifies friendly forces across the cyber spectrum might seem daunting, it is imperative to national security. Building a capability that will unify operations faster and can be scaled and repeated at unprecedented levels requires the U.S. military to approach the challenge incrementally but with disciplined tenacity.

The military, government and industry are on the forefront of an effort where organizations and partnerships can make a difference. A mature agile development process, combined with a close working relationship between government and industry, is the best way to address the mission of creating the infrastructure needed to stay ahead on tomorrow's cyber battlefield.

• • • — • —

Maj. Gen. Gregg Potter, USA (Ret.), is the corporate lead executive for Northrop Grumman at Fort Meade and Aberdeen, Maryland. He served in the U.S. Army for more than 32 years as a military intelligence officer and retired as the director of the National Security Agency's Signals Intelligence Directorate. Chris Valentino, director of joint cyberspace programs for Northrop Grumman Mission Systems Cyber and Intelligence Mission Solutions Division, is responsible for development and delivery of full-spectrum cyberspace capabilities to its customers.

To share or comment on this article go to ***http://url.afcea.org/January18***

contact:
signalnews@afcea.org