The Army’s Way Ahead In Cyberspace

By GEN Keith B. Alexander
The United States has become deeply and irreversibly reliant on cyberspace for its major activities: defense, commerce, communications, utilities and governance. The tight coordination of logistics and operations and the reliability of timing and flow are dependent on cyberspace resources and have become indispensable for the order and functioning of our society, economy and military. We communicate in cyberspace and transfer objects such as airline boarding passes that never have to leave cyberspace to be consumed. In cyberspace, we operate the critical infrastructure that underpins the functioning of our society. Cyberspace has also become a place where we store treasure, such as intellectual property and personal wealth. Within DoD, cyberspace resources enable military and business operations to allow the joint force to perform its warfighting functions across all domains.

The efficiency and dependability afforded by cyberspace yield significant benefits. Nevertheless, reliance on highly interdependent networks with ubiquitous access points that are insecure, sensitive to interruption and lack resiliency poses grave risk to our military capabilities, intellectual property, critical infrastructure and diplomatic relationships. This lack of security has turned many of the things we value into targets for our adversaries.

The Coming Cyber Crisis

With its ungoverned space and easy access, the cyber domain has become the newest front for confrontation. Attacks are growing in frequency, scale, complexity and destructiveness. Cyberspace is seen as an advantageous avenue of approach for our adversaries since operations therein often do not require the extensive resources needed for the development and employment of conventional military capabilities. Attacking the United States in the cyber domain is easier than in the land, maritime and air domains, allowing adversaries to avoid challenging the United States in its areas of traditional military dominance. Instead, they can exploit the extensive, essential and often fragile U.S. presence in cyberspace to remotely strike at us and undermine our national interests. Because of the globally interconnected nature of cyberspace, even relatively unsophisticated actors can project power and operate within U.S. “territory.” Potential adversaries can steal intellectual property, conduct industrial espionage, and penetrate networks of governments, the defense industry, critical infrastructure operators and others in the private sector. Adversaries actively conduct intelligence, surveillance and reconnaissance inside U.S. and allied networks, often establishing a persistent presence. They are preparing the future cyber battlefield now.

Defending our nation in cyberspace poses unique challenges because nearly 85 percent of the enabling infrastructure is owned and operated by the private sector, where security is often not the first priority. In the past, the armed services have been focused on defending DoD networks, not those of the country as a whole. This situation is no longer acceptable. Not only do we rely on private sector critical infrastructure for core DoD functions, but U.S. national interests in cyberspace are now so significant that we must accept a greater mission. The services must build the force now to defend our nation and its interests in cyberspace.

Embrace Change

Integration has become both a possibility and an imperative because of significant changes in the operational environment. The biggest change is the convergence of voice, video and data communications onto a single network, which carries massive volumes of data. Ubiquitous networks, mobile computing and an ever-increasing reliance on these systems throughout our daily lives have exponentially increased our vulnerabilities. The increase in the scale and pervasiveness of cyberspace is accelerating. For example, the number of transistors per microchip has increased more than a thousandfold, from 42 million to 5 billion, in just 12 years. Partly as a result, mobile device use went from 740 million subscriptions in 2000 to 6.4 billion in 2012. We expect to see 10 billion mobile devices by 2016—or 1.4 per person on the planet. As cyberspace constantly changes and expands, its complexity increases, the attack surface expands, new vulnerabilities appear and the risk of disaster grows.

The rapid pace of change, however, is not something we should seek to slow down; rather, it is something we must embrace. These developments create opportunities along with the risks. Advances in information technology such as cloud computing, secure mobile communications and high-power computing—when joined with new operational frameworks such as the Joint Information Environment—create the possibility of dramatically improving effectiveness and defensibility.

We currently operate on an architecture built with security as an afterthought. Cloud technology provides the means to build more defensible networks and employ better automated tools and virtualization to secure them. By adopting a cloud architecture, we will be better able to “see” our own networks using automated tools, enhance configuration control and patch systems in near-real time. The shift to a cloud architecture also reduces manpower-intensive tasks because many functions can be centralized and automated, enabling personnel to focus on other important missions. Finally, the movement to a cloud architecture makes data accessible regardless of device or location. Assured, mobile and more secure communications are now possible, with the potential to dramatically empower tactical users.
For intelligence analysts, cloud technology means the ability to automate routine work, leaving more time to discover new intelligence information and provide it to military commanders and other consumers in a timely manner. These advances, along with the networking of analysts across disciplines, promise to improve the quality, timeliness and effectiveness of all intelligence operations. The members of the intelligence community and the military services can utilize big data to meet their needs when the stovepipes are collapsed. Improved intelligence collaboration and an increased capability for discovery can become a foundation for Phase 0 operations to prevent conflicts from escalating, and they can provide critical intelligence that enables our forces to operate more effectively in Phases 1, 2 and 3.

Integration Imperative

To maximize the ability of the joint force to defend the nation in cyberspace, protect DoD information and networks, and conduct military operations in all domains, the services—including the Army—need to integrate their information-related capabilities into a single force. Today, the Army has distinct branches for communications and intelligence. This structure, however, tends to produce one force focused on the operation and defense of information networks and another on information gathering and offense. Given the fact that cyberspace is an increasingly integrated and contested domain, this is no longer tenable. To operate effectively in the current operational environment, we need a single, integrated force to conduct full spectrum cyberspace operations; ensure reliable, secure information flow; and perform intelligence operations across all disciplines.

At the national level, the threat has already forced us to integrate communications and intelligence. In November 2008, in response to the discovery of foreign intelligence malware in our classified networks, then-Secretary of Defense Robert M. Gates placed the Joint Task Force-Global Network Operations under the operational control of the commander, Joint Force Component Command-Network Warfare. Ultimately, both these organizations were merged into U.S. Cyber Command—a critical step reflecting the need to merge cyber security and intelligence in order to obtain threat warning and meet national and joint force commander requirements. DoD has realized that the team conducting cyberspace intelligence, surveillance and reconnaissance is the same team that, when authorized, will deliver combat effects. This principle must guide service force structure as well. Each service needs to combine its information-related capabilities into a single, integrated information corps that can provide assured access to cyberspace resources in a fully integrated manner.

The Way Ahead

We now rely on an information architecture that is difficult to defend and requires a large force to operate. We are not yet postured to use big data to enable cyberspace, intelli-

**GEN Keith B. Alexander** is commander, U.S. Cyber Command (USCYBERCOM), and director, National Security Agency (NSA)/chief, Central Security Service (CSS), Fort George G. Meade, Md. As commander of USCYBERCOM, he is responsible for planning, coordinating and conducting operations and defense of DoD computer networks as directed by U.S. Strategic Command. As director of NSA and chief of CSS, he is responsible for a DoD agency with national foreign intelligence, combat support and U.S. national security information system protection responsibilities.
gence and combat operations. Moreover, the services operate and defend only their own networks, despite joint interdependence. We must move to a more defensible, efficient architecture that relies on a smaller force to operate—the Joint Information Environment (JIE).

The Army must build a force that can access this increasingly capable joint communications architecture for deployed and sustaining base operations. This team must be trained to a single, joint standard and bring the same expertise to the operation and defense of our networks that we devote to exploitation. It should use the power of big data to improve the effectiveness of intelligence operations and provide commanders with assured, secure access to increasingly joint communications. Only a full merger of formerly separate communications, intelligence and other information-related communities will achieve the efficiency and effectiveness gains we need today. With these changes, the Army can become a leading contributor of warfighting capability that will be increasingly important in Phase 0, as well as build a force that will increase the effectiveness of all of the Army’s conventional, special operations and cyber formations.

The innovation needed to realize this vision will not be easy. The Army must transcend traditional barriers between the communications and intelligence communities—between a Signal Corps with an operate-and-maintain focus and an intelligence enterprise that exploits in cyberspace but is not engaged in defense. We need one force that integrates cyberspace operations and defense and offense missions with intelligence operations and support for information requirements of military operations across all operational domains. These changes are even more important in the current budgetary environment. The Army should seize the possibilities provided by progress in information technology to emerge from a period of fiscal constraint as an even stronger force.

The Army has made substantial progress by embracing the advantages of the JIE and building a world-class Military Intelligence (MI) brigade to operate in cyberspace. The Army still lacks a framework, however, for the creation of a force that operates, defends and exploits in cyberspace in an integrated manner.

To move forward, the Army must:

■ Accelerate implementation of the JIE.
■ Develop a road map to unify staffs at all levels, unify force structure, and merge signal and MI organizations at all echelons.
■ Merge current signal and MI communities into a single, integrated information corps that operates across missions.

These steps to build an information corps are both efficient and effective, creating improved capabilities using current or reduced resources. They seize opportunities created by advances in information technology; respond effectively to adversary activities; repurpose forces to provide critical new warfighting capabilities; and provide assured access, confident command and control, and the ability to deliver effects. Together, they will reshape our Army into a 21st-century force that is second to none.