Viewpoint

Creating a More Agile Defense Department Info-Tech Enterprise

BY TERI TAKAI

Secretary of Defense Leon Panetta in January released guidance that outlines a plan for shaping U.S. defense strategy. The purpose is to achieve a joint force that "will be more agile, more flexible, ready to deploy quickly, innovative and technologically advanced."

However, in order for the joint force to change, the Defense Department's information technology environment must change.

The Defense Department's chief information officer is responsible for overseeing the enterprise and ensuring that the department's networks and information sharing are as secure, effective and efficient as possible and that the technology is accessible and dependable in the face of any threat — physical or cyber — by any adversary.

The current Defense Department information technology environment is vast and complex. The approximately $37 billion requested by the department for fiscal year 2013 includes funding for a range of products such as desktop computers, tactical radios, identity management technology, human resource applications, commercial satellite communications and financial management systems. On the unclassified network alone, it has more than 3.6 million users on more than 7 million computers.

Currently, each military service builds its own information infrastructure. These infrastructures are connected by a common network, and all share certain core information services. However, there is ample room for improvement. The complex interconnected nature of the networks means that it is difficult, or in some situations impossible, for a joint commander to obtain accurate situational awareness of all of the networks supporting his or her mission.

The joint force described in the secretary's new guidance will be smaller than before, but no less formidable. The keyword is "agile." The new joint force will be able to respond to threats and meet objectives while engaged in larger operations elsewhere. It will be technologically superior and better networked than before. Improving communications and infrastructure means easier information sharing and faster response times, which allows for smarter, better informed decisions at the tactical edge.

In 2011, the deputy secretary of defense signed the IT Enterprise Strategy and Roadmap, which is a set of initiatives that are aimed at achieving two primary goals: to make the department more secure against cyber-attacks and to reduce costs and improve the agility of its information technology and networks by simplifying, standardizing and consolidating infrastructure. The chief information officer is leading efforts to complement this strategy by making improved mission effectiveness and cybersecurity the primary goals of a reengineered information infrastructure, with efficiency through consolidation, simplification, standardization and automation. The result of this new effort will be the joint information environment, or JIE. Experts from throughout the department are now developing milestones and an implementation plan.

One feature of the JIE is the consolidation of essential information capabilities into a small set of core data centers. These computing centers will be managed by the military services and by the Defense Information Systems Agency as joint assets, and will contain information capabilities and services provided by each military service and many other department components.

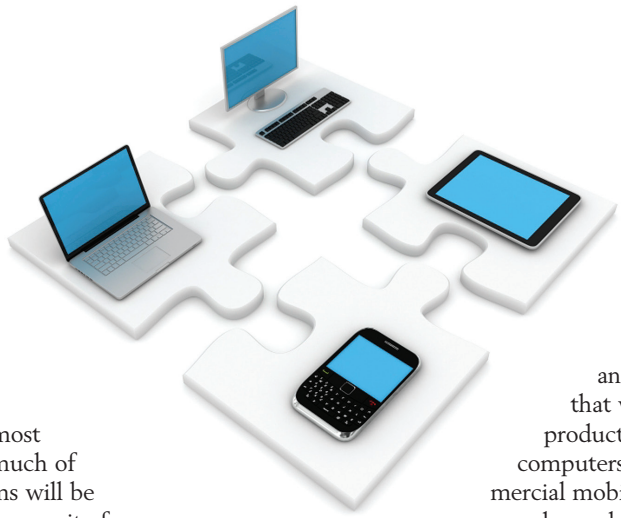
Another key feature of the JIE is the simplification of networks. Today's enterprise consists of many separately designed and managed networks, all sharing a common core. They are built to department standards and are generally operated by a single organization, such as one of the military services, and are cryptographically separate, with a modest number of points at which they connect to other components.

This complex structure makes it difficult to understand the many networks on which a joint mission depends, and makes defending missions — as opposed to defending computers — much more difficult than it needs to be. The program will repurpose many of the defenses the military has already fielded into joint, regional defenses. The separately tunneled networks will be replaced with a single network that makes situational awareness and defense of computer networks — as well as dependability and interoperability — significantly better.

Another key feature of the joint information environment is a set of initiatives aimed at improving information access and protection while simultaneously driving out the anonymity inherent in many of the information technologies on which the department depends. The first part of these identity efforts is the movement to a single, standard cyber-identity credential, issued by the public key infrastructure, for both the unclassified and secret networks. The third part is to use these credentials to allow access to information. This will let the department do away with passwords and their attendant vulnerability, and will simplify information access. Finally, the joint information environment will move to the use of standard labels for information, with access to this information controlled by the labels and the credentials and attributes of the people and systems requesting access.

Though budget cuts have been and will continue to be made, the infrastructure must become more secure.

In addition to benefits for end-users and network security experts, the JIE will speed up capability deployment while making them less expensive and more secure. In today's environment, a typical information technology program must develop and integrate the entire "stack," including the network, the computing, the standard software loads on the computing, global load balancing and the core machine-to-machine services, such as messaging. In addition, the program must integrate cybersecurity across all of this, from operating system configuration, access controls, perimeter defenses, cyber-attack detection and diagnosis. Much of this



effort is similar across almost every information technology program.

In contrast, the JIE will provide program offices an enabling infrastructure of network, computing, core enterprise services and security. Program managers will often be able to build on top of all or most of this standard platform. Since much of the work is already done, programs will be faster, and will inherit better cybersecurity from the start. Through efforts like the forge.mil software development environment and integrated test and security evaluation capabilities that match the production platform, the CIO can also help speed up the development, quality control and cybersecurity evaluations for programs. As a result of the use of this standard platform, both information resources and the network itself will be more easily accessible and better protected.

This standardized IT and network infrastructure will help eliminate barriers to information sharing. The department's new approach to cybersecurity focuses on five goals: to ensure that IT infrastructure is dependable in the face of cyberwarfare; to enable rapid and safe data sharing; to protect sensitive and classified information; to protect mission commanders' access to cyberspace; and to adopt new technology in a fast, efficient manner.

These goals cover all cybersecurity concerns, from removing or shielding network vulnerabilities to detecting, reacting to and deterring intrusions. The Internet and technology landscape is ever changing. This fluid and rapid turnover of new products makes the Defense Department information infrastructure difficult to defend and attacks hard to anticipate.

Creating a leaner, more agile joint force means reducing costs and finding efficiencies concerning overhead and support activities, not just removing personnel or lowering expectations. Though budget cuts have been and will continue to be made, the infrastructure must become more secure.

Networks have to be monitored in order to be protected. This requires visible sight lines, so to speak, through the entire network. Consolidating networks and data centers will, in the long term, both reduce IT costs and create a system that is easier to monitor, and thus easier to defend. Currently, the Defense Department operates more than 770 data centers, which are characterized by underused capacity. The CIO is working with the services and defense agencies to set standards for data center consolidation and the type and design of new centers. This consolidation will result in three types of data centers: core, which will be used for information services and applications used across the department; regional, which will host services beneficial to users in a specific area; and forward deployed or deployable, which will provide regional and enterprise services. By the end of fiscal year 2012, the department will have reduced the number of data centers by more than 115.

Also, consolidating and standardizing top-level architectures, hardware and software purchases and network interconnections will allow the department to support all environments, including work, home, mobile and future devices. One of the goals for the JIE is to reduce reliance on desktop computers and promote use of client-based mobile technology, including smartphones, tablets and laptops. The aim is to deliver highly functional and secure mobile applications and devices that would allow the work force to be as productive on mobile devices as it is on desktop computers. The department is working on a commercial mobile device strategy that will describe how we can keep abreast of new, helpful technology.

The department is going from today's end-user computing to laptops, thin clients, and smartphones. The final product will be a secure, interoperable network that is faster and more responsive to war fighter needs. The emerging joint force — as well as the network that supports it — will be able to adapt to fit any situation. Agile operations will define the force of the future.

Given the fluid parameters of cyberspace and the potentially devastating real-world effects of a network breach, this is a step in the right direction. The joint force will be as effective in cyberspace as it is on land, at sea and in space.

Teri Takai is the Defense Department chief information officer.

ISTOCKPHOTO