Guarding

Airman loads security updates for network at Balad Air Base, Iraq

31st Communications Squadron (Michael Holzworth)

Cyberspace
Global Network Operations

By CHARLES E. CROOM, JR.

President George Bush's *National Strategy to Secure Cyberspace* (NSSC) describes cyberspace as the nervous system of our country. The NSSC outlines—for all Federal, state, and local governments, private companies and organizations, and individual Americans—a framework to deter adversaries and assure cyberspace freedoms.

Today, instant cyberspace communication has forever changed and flattened our world. Cyberspace provides unprecedented access to goods, services, and information in a world that is fundamentally more complex than ever before. It drives the global economy and connects people in ever-changing contexts. It also creates *dependencies* in every element of a society's infrastructure: transportation, banking, public utilities, education, governance, diplomacy, and national defense. And no nation is more dependent on cyberspace than ours.

Dependence creates vulnerability, and nothing is more inherently vulnerable than cyberspace. Like previous eras, ours is populated by outlaws and charlatans, thieves and pirates, who threaten the viability of the domain in the name of greed, political or ideological hegemony, or military advantage. What is required is a change in our view of cyberspace: as a matter of national interest and national security, it must be viewed as *battlespace*.

With that operational perspective, cyberspace becomes a warfighting domain—akin to land, sea, and air—where we are engaged in defending our national interests and security. Our society is linked in cyberspace. We are network-centric: network-dependent and network-defined. This "net-centricity" must be defended, just as any other element of our society must be defended.

The weapons system leading the battle is the Department of Defense Global Information Grid (DOD GIG).

Basic to this notion is the integration of cyberspace capabilities across the full range of military operations. The designated military lead for cyberspace operations,

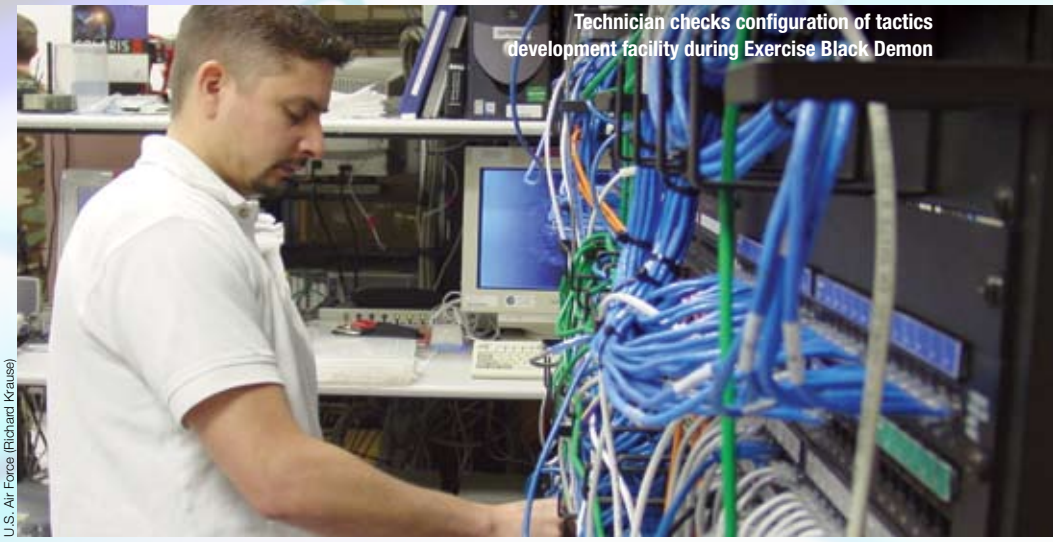
> *as a matter of national interest and national security, cyberspace must be viewed as* battlespace

U.S. Strategic Command (USSTRATCOM), directs the operation and defense of the DOD GIG to assure timely and secure net-centric capabilities in support of the full spectrum of warfighting, intelligence, and business missions. This is the frontline of the new battlespace.

USSTRATCOM's agent for this action is the Joint Task Force–Global Network Operations (JTF–GNO), which was created out of a series of real-world cyber events in 1997 that targeted DOD networks. Those events clearly showed two things: the vulnerability of DOD mission-essential computer assets and the need for a single organization with the appropriate levels of authority to defend these globally interconnected networks, associated information capabilities, processes, and information.

The JTF–GNO manages four overarching concerns: *who* is on the GIG, *what* does the GIG look like, *where* are the vulnerabilities, and *how* can risks be mitigated? The JTF–GNO addresses those concerns by serving as the fusion point for its mission partners and producing alerts, bulletins, assessments, and tasking orders. In addition, it manages the status of Information Condition (INFOCON), the alert system governing the defensive tactics and policies that users of the GIG need to follow.

The GIG is hit with millions of scans every day, and while the vast majority are deflected, each must be treated as a potential intrusion attempt. Complicating this effort



Technician checks configuration of tactics development facility during Exercise Black Demon

U.S. Air Force (Richard Krause)

Lieutenant General Charles E. Croom, Jr., USAF, is Director, Defense Information Systems Agency. He is also Commander, Joint Task Force–Global Network Operations, U.S. Strategic Command.


Airman checks SIPRNET security at Ramstein Air Base, Germany

U.S. Air Force (Latonia Brown)

is the fact that our information management systems are largely based on commercial software—the same software available to adversaries and malicious actors. Advances in computer information technology are available *globally*, making the threat to the GIG extensive, pervasive, and increasingly sophisticated.

This battlespace demands a proactive, preventive capability; a flexible, layered defense; rapid detection; robust response options; shared situational awareness across cyber domains; timely warning of impending attacks; effective defensive tools; and measures to defeat attacks as they occur. Cyberspace is the only domain where all instruments of national power (diplomatic, informational, military, and economic) can be exercised simultaneously, yet it is also the only place where our infrastructures can be attacked from obscure launching sites at the speed of light.

As a consequence, the JTF–GNO must provide guaranteed availability of systems and networks, assured delivery, and protection of information. By bringing this balance of capabilities to the DOD information environment, with potentially vast implications for mission success, the JTF–GNO unites all users of the GIG with common standards and processes through a doctrinal construct known as the Joint Concept of Operations for GIG Network Operations (NetOps CONOPS).

The USSTRATCOM commander articulated the specifics of the CONOPS, which provides the operational framework and command and control structure to combine the disciplines of enterprise systems and network management, network defense, and content management. These three essential tasks, as well as command and control and situational awareness, are the fundamental components of NetOps.

Each essential task has a specific body of objectives. Where network management is concerned, NetOps relies on the understanding, application, and integration of information technology, technology standards, and standard processes that provide traditional systems and network management (fault management, configuration management, accounting management, performance management, and security management). NetOps enterprise management consists of the many elements and processes needed to communicate across the full spectrum of the GIG and includes enterprise services management, systems management, network management, satellite communications management, and electromagnetic spectrum management.

content management seeks to make data visible, discoverable, and understandable

At the same time, network defense includes USSTRATCOM's operational responsibilities for information assurance, computer network defense, critical infrastructure protection, and other GIG defense tasks. NetOps is not intended to replace institutional practices of information assurance and computer network defense but to enhance them through a comprehensive process of protection, monitoring, detection, analysis, and response.

Finally, content management involves the ability to "maneuver information across GIG terrestrial, space, airborne, and wireless environments." It supports the broad DOD data strategy that seeks to make data visible, discoverable, and understandable.

NetOps puts a combatant commander in charge of the GIG end-to-end; it surpasses basic network management and computer network defense practices in net-centric military operations. NetOps includes not only balancing GIG responsibilities between theater and Service components but also establishing and sharing GIG situational awareness across DOD. NetOps does not mean that network providers or frontline defenders relinquish their responsibilities for their respective combatant command, Service, or agency; it does require that all synchronize their efforts to maximize efficiency, ensure data availability, and enhance protection of the network at large.

Operating in this unique and dynamic area of responsibility, the JTF–GNO has command relationships with all DOD commands, Services, and agencies. Its mission partners include allied nations, other U.S. Government departments, the National Cyber Response Coordination Group, the U.S. Computer Emergency Response Team, law enforcement agencies, the Intelligence Community, and the private sector, including telecommunications, banking and finance, transportation, and information technology.

As well as delineating the day-to-day activities of the GIG, the NetOps CONOPS defines the way ahead and establishes a working vocabulary of GIG activities and components. The JTF–GNO vision, according to its strategic plan, is to "lead an adaptive force that assures the availability, delivery, and protection of the GIG."

The JTF–GNO is facilitating the operational environment in which net-centricity can thrive, and it helps guarantee the free and open use of cyberspace for everyone to embrace the opportunities offered by a globally connected world. **JFQ**