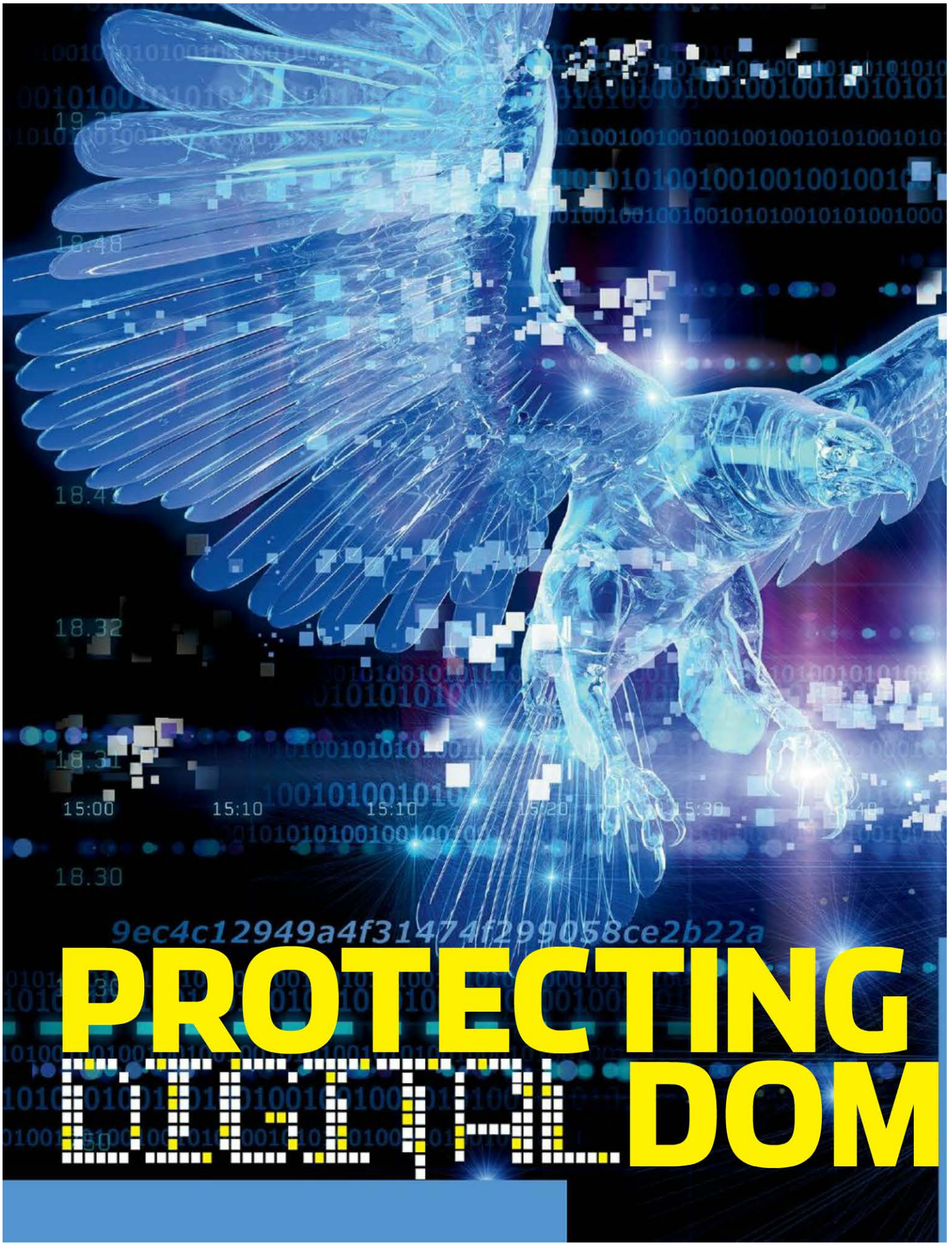
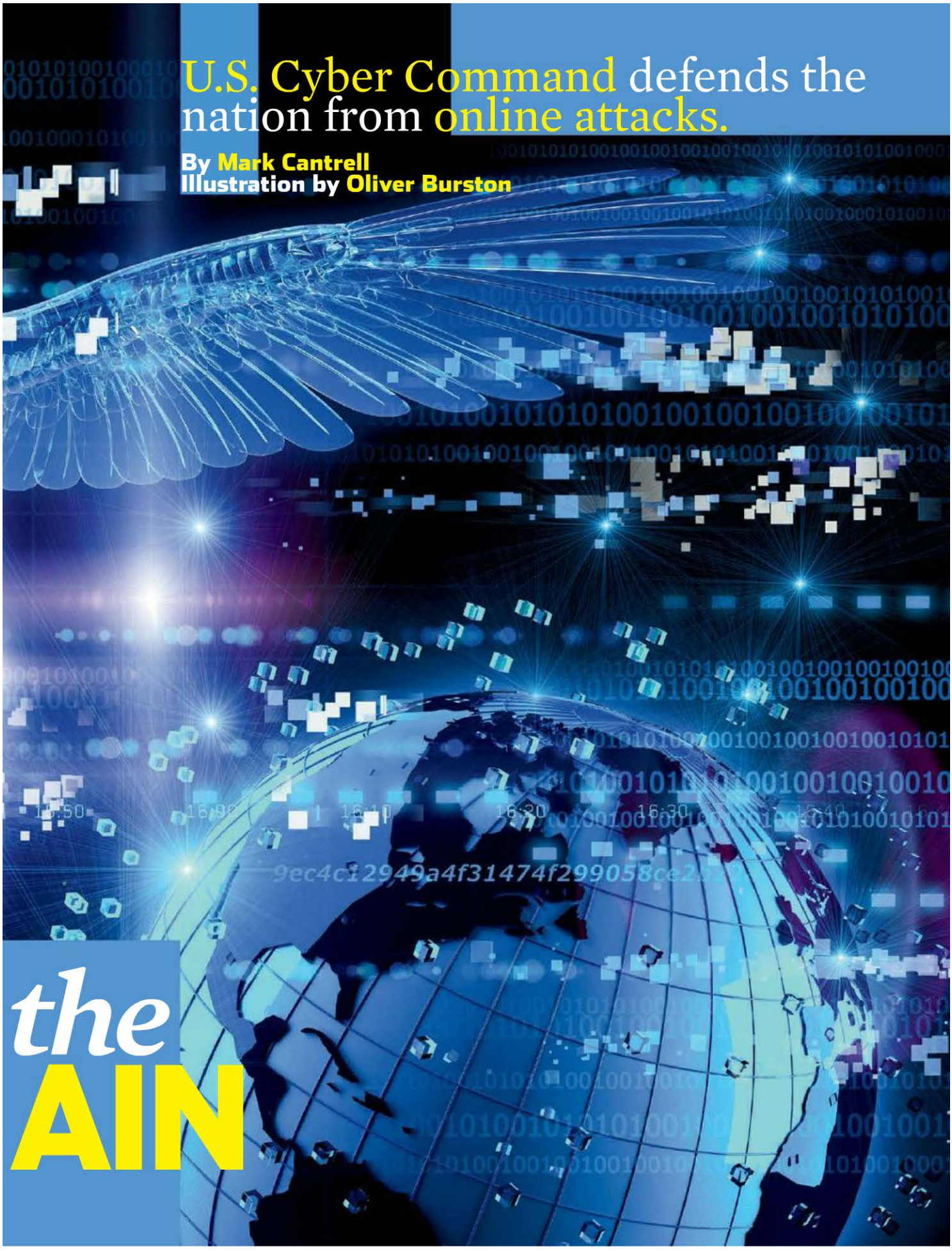


PROTECTING DIGITAL DOM

U.S. Cyber Command defends the nation from online attacks.

By Mark Cantrell
Illustration by Oliver Burston



the AIN

IN THE 1983 FILM *WAR GAMES,* a young hacker breaks into a military supercomputer and, while using it to run a nuclear war simulation, nearly starts World War III. Although entertaining, the plot was extremely far-fetched at the time — but that was before the Internet.

Today, with almost every computing system connected to the World Wide Web, keeping American defense networks safe from intrusion has become a vital part of the military's mission. In addition to the battlefields of land, sea, air, and space, the military now must stand ready to fight in a fifth domain: cyberspace. The Navy was first out of the gate in establishing a computer security wing in 2006, but it never became fully operational. In the face of increasing cyberattacks by China, however, it became obvious a unique type of agency would be required to combat the sophisticated and evolving threats to the military network infrastructure. In 2009, then-Secretary of Defense Robert Gates directed the commander of U.S. Strategic Command to establish U.S. Cyber Command (CYBERCOM). Its mission: to defend DoD's Information Network (DoDIN), provide support to combatant commanders for execution of their missions around the world, and strengthen our nation's ability to withstand and respond to cyberattack.

Gates, in a memo to DoD's top brass, said of the increasing threat, "To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment, as well as providing support to civil authorities and international partners." For the new agency's first director, Gates recommended then-Lt. Gen. Keith Alexander, USA, who was also the director of the National Security Agency (NSA) at the time.

CYBERCOM was stood up at Fort Meade, Md., May 21, 2010, in a small ceremony attended by Gates and Army Gen. David Petraeus, then-

PHOTOS: THIS SPREAD, CLOCKWISE FROM TOP, WILLIAM BELCHER/USAF; DARPA; NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

commander of U.S. Central Command. The new agency absorbed some other commands, including Joint Task Force — Global Network Operations and Joint Functional Component Command — Network Warfare; their staffs relocated to Fort Meade. The Defense Information Systems Agency (DISA) headquarters also moved to the base. In April 2014, Adm. Michael S. Rogers, USN, succeeded Alexander as head of both CYBERCOM and the NSA.

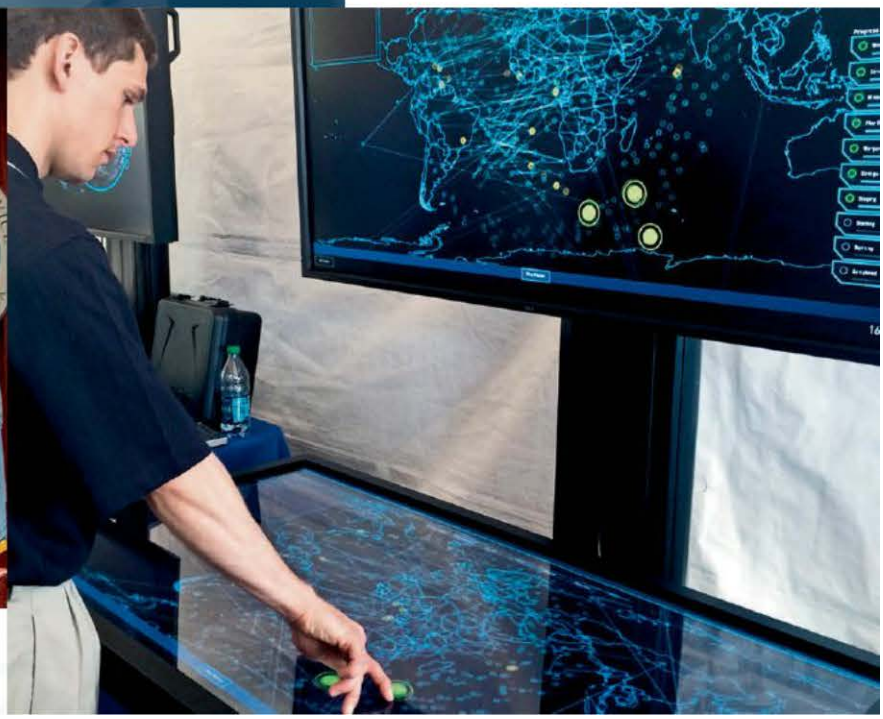
A work in progress

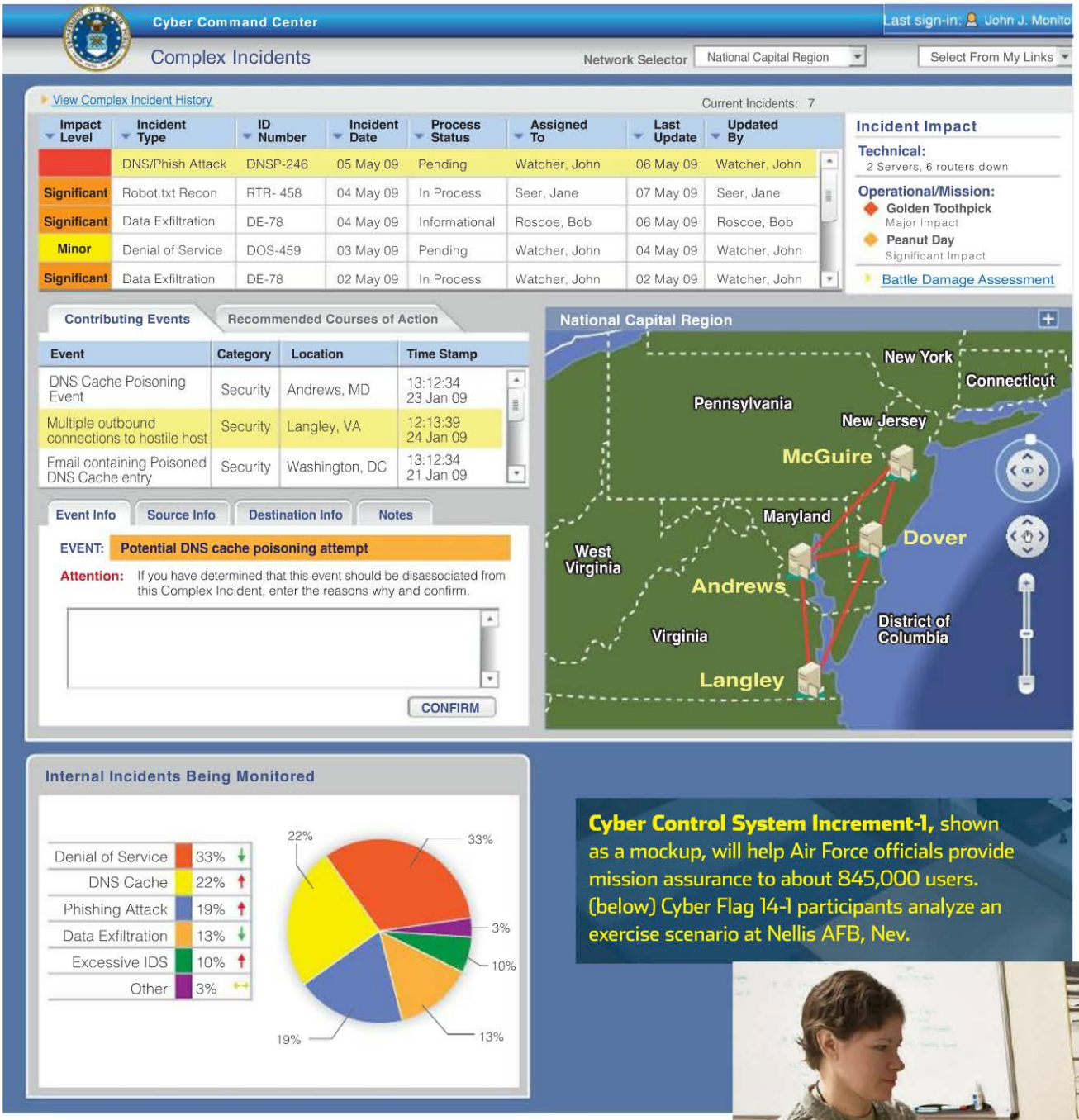
As one of DoD's newest commands, CYBERCOM is still in the process of implementing its Cyber Mission Force (CMF) planning model, which will be built over the next few years, according to a command spokesperson. There are three types of teams that will comprise the CMF to work three main mission areas: Defend the nation, when directed by the president (Cyber National Mission Force); support combatant commanders' priorities (Cyber Combat Mission Force); and defend the DoD information networks (Cyber Protection Teams). While each force has a specific mission area (defend the nation to protect critical infrastructure; support combatant commanders; defend the DoDIN), integrated planning and coordination goes through the CYBERCOM headquarters to identify mission gaps while helping to avoid unnecessary duplication of effort.

The agency has its work cut out for it, as Director of National Intelligence James Clapper told Congress in 2013. Speaking to the House Armed Services Committee, Clapper noted the threat of cyberattacks by foreign nations could be an even greater danger than that posed by global terrorism. It's not only military networks at risk, said Clapper, but also the nation's critical water, energy, financial, and information infrastructure. Such an attack, he said, could cripple our economy in much the same way 9/11 did.

It's hard to imagine a single hacker or team of programmers could wreak that kind of havoc, but it is becoming more likely. In 2007, the Idaho National Laboratory conducted a test to point out weaknesses in America's electrical grid by changing the operating cycle of a power generator remote-

(clockwise from above) Personnel of the 624th Operations Center conduct operations in support of Air Forces Cyber. A program manager uses a touch table designed by Plan X, a Defense Advanced Research Projects Agency cyber warfare program. Adm. Michael Rogers, USN, right, accepts the Cyber Command flag from Adm. Cecil Haney, USN, as Rogers assumes command.





Cyber Control System Increment-1, shown as a mockup, will help Air Force officials provide mission assurance to about 845,000 users. (below) Cyber Flag 14-1 participants analyze an exercise scenario at Nellis AFB, Nev.

ly by computer. The generator caught fire and was destroyed. Although attempts have been made to secure critical elements of government and commercial infrastructure since then, many systems remain vulnerable. In FY 2013, the Government Accountability Office reported 46,160 cyberattacks on federal agencies alone.

Some of the most vulnerable networks are the supervisory control and data acquisition systems that often control water, power, and other infrastructure elements. They can be located in remote areas and accessed by telecommunication links, which some experts think makes them vulnerable to cyberattack. In addition, many use off-the-shelf software that can be modified by intruders.

A covert invasion

While a physical full-scale attack is meant to create as much "shock and

IMAGES: ABOVE, AIRMAN 1ST CLASS CHRISTOPHER TAM, USAF; TOP, COLIN HAYES BASED ON U.S. AIR FORCE PHOTO ILLUSTRATION

awe" as possible, a cyberattack is a silent, insidious process designed to do its work in secret. Often, the damage is done before network administrators realize it took place. And even though computer attacks are becoming more frequent, it's still usually difficult to determine the identity of the attacker. In a recent attack thought to be the work of a Russian hacker group, three industrial control networks were infected with malware that would have allowed them to sabotage the systems had the attack not been identified.

CYBERCOM's job is to prevent these kinds of attacks on DoD networks, but that's only part of its mission; increasingly, its operatives are going on the offensive. The same vulnerabilities that can compromise DoD systems exist on those of our adversaries and can be exploited in the same way. If an enemy's missile control system could be penetrated, for example, the threat could be nullified without firing a shot. To that end, experts in "vulnerability discovery" are currently in high demand at CYBERCOM and the NSA.

A good offense

Their work is evident in initiatives such as Operation Olympic Games, a still-unacknowledged cyberattack that allegedly planted a virus called Stuxnet, which damaged centrifuges in Iran's nuclear enrichment facilities. While defending networks from cyberattack is still important, the concept of "cyberspace superiority," an edge that gives warfighters key advantages in situational awareness and other areas, is rising to the fore. Compromising or destroying an enemy's computer and communication systems before a U.S. offensive would give servicemembers a big tactical advantage, without risking lives.

One of the ways computer systems can be compromised is by using "zero-day" exploits — flaws in a system's software that are as yet undiscovered. Those chinks in a computer's armor allow CYBERCOM operators to implant viruses and other bits of malware that can take over a system or render it inoperative. Understandably, zero-day exploits are highly sought after by DoD, especially when they involve the computer systems of our adversaries.

The Defense Advanced Research Projects Agency (DARPA) is usually on the leading edge of new military technology, and that's true in the case of cyberwar as well. The agency's Plan X, announced in 2012, aims to create revolutionary technologies to enable the military to more fully utilize cyberspace. One part of the program involves creating situational awareness tools integrating physical and cyber elements on the battlefield and making them available to commanders. That way, a warfighter will know not only where the enemy is and what weapons they're using but also whether they're communicating via cellphone or Wi-Fi — virtually "mapping" the digital battlefield in cyberspace. DARPA will begin to implement Plan X at DoD and CYBERCOM in October 2017.

As traditional weapons increase in capability and sophistication, so will the weapons and tactics of cyberwar. CYBERCOM will be at the forefront on this newest battlefield. MO

— **Mark Cantrell** *is a North Carolina-based freelance writer. His last feature article for* Military Officer *was "Camo-flawed," May 2014.*

Hacker Techniques

Hackers can disrupt and control a remote computer system by several methods.

- **Distributed denial of service attack:** over a period of time, infecting a large number of computer systems with a virus that enables them to seize control and turn them into "zombie" systems. At an arranged time, the controllers command the computers to all access the same website at once, making it inaccessible.
- **Semantic attack:** planting inaccurate information into a computer system so it seems to operate normally but produces false results. The Israeli Air Force employed this kind of attack in 2007, disrupting the Syrian air defense system before making an air strike on a Syrian nuclear facility.
- **Syntactic attack:** using malicious software such as viruses, trojans, and worms to infect a computer system. These types of malware replicate themselves inside a system and easily can spread to other computers attached to the network.
- **Social engineering:** tricking people into compromising their system's security — for example, getting them to click on a Web link that loads a virus or divulge personal information through a fraudulent website.