Military grooms new officers for war in cyberspace

April 26 2013, by Brian Witte

In this Feb. 20, 2013 photo, Martin Carlisle, standing, a computer science professor at the Air Force Academy and director of the school's Center for Cyberspace Research, instructs cadets in cyber warfare, at the U.S. Air Force Academy, in Colorado Springs, Colo. The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system. (AP Photo/Brennan Linsley)

The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system.

Students at the Army, Navy and Air Force academies are taking more courses and participating in elaborate cyberwarfare exercises as the military educates a generation of future commanders in the theory and practice of computer warfare.

The academies have been training cadets in cyber for more than a decade. But the effort has taken on new urgency amid warnings that hostile nations or organizations might be capable of crippling attacks on critical networks.

James Clapper, director of national intelligence, called cyberattack the top threat to national security when he presented the annual Worldwide Threat Assessment to Congress this month. "Threats are more diverse, interconnected, and viral than at any time in history," his report stated. "Destruction can be invisible, latent, and progressive."

China-based hackers have long been accused of cyber intrusions, and earlier this year the cybersecurity firm Mandiant released a report with new details allegedly linking a secret Chinese military unit to years of cyberattacks against U.S. companies. This year, The New York Times, The Wall Street Journal and The Washington Post all reported breaches in their computer systems and said they suspected Chinese hackers. China denies carrying out cyberattacks.

On Tuesday, hackers compromised Associated Press Twitter accounts and sent out a false tweet. AP quickly put out word that the report was false and that its accounts had been hacked. AP's accounts were shut down until the problem was corrected.

Once viewed as an obscure and even nerdy pursuit, cyber is now seen as one of the hottest fields in warfare—"a great career field in the future," said Ryan Zacher, a junior at the Air Force Academy outside Colorado Springs who switched from aeronautical engineering to computer science.

Last year the U.S. Naval Academy in Annapolis, Maryland began requiring freshmen to take a semester on cybersecurity, and it is adding a second required cyber course for juniors next year.

In this Feb. 20, 2013 photo, a cadet works at a large computer display inside a classroom at the Center for Cyberspace Research, where cyber warfare is taught, at the U.S. Air Force Academy, in Colorado Springs, Colo. The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system. (AP Photo/Brennan Linsley)

The school offered a major in cyber operations for the first time this year to the freshman class, and 33 midshipmen, or about 3 percent of the freshmen, signed up for it. Another 79 are majoring in computer engineering, information technology or computer science, bringing majors with a computer emphasis to about 10 percent of the class.

"There's a great deal of interest, much more than we could possibly, initially, entertain," said the academy's superintendent, Vice Adm. Michael Miller.

Since 2004, the Air Force Academy has offered a degree in computer science-cyberwarfare—initially called computer science-information assurance—that requires cadets to take courses in cryptology, information warfare and network security in addition to standard computer science. The academy is retooling a freshman computing course so that more than half its content is about cyberspace, and is looking into adding another cyber course.

"All of these cadets know that they are going to be on the front lines defending the nation in cyber," said Martin Carlisle, a computer science professor at the Air Force Academy and director of the school's Center for Cyberspace Research.

In this Feb. 20, 2013 photo, a cadet walks past multiple computer displays inside a classroom at the Center for Cyberspace Research, where cyber warfare is taught, at the U.S. Air Force Academy, in Colorado Springs, Colo. The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system. (AP Photo/Brennan Linsley)

About 25 Air Force cadets will graduate this year with the computer science-cyberwarfare degree, and many will go on to advanced studies and work in their service's cyber headquarters or for U.S. Cyber Command at Fort Meade, Md., the Defense Department command responsible for defensive and offensive cyberwarfare.

Almost every Army cadet at the U.S. Military Academy at West Point, New York, takes two technology courses related to such topics as computer security and privacy. West Point also offers other cyber

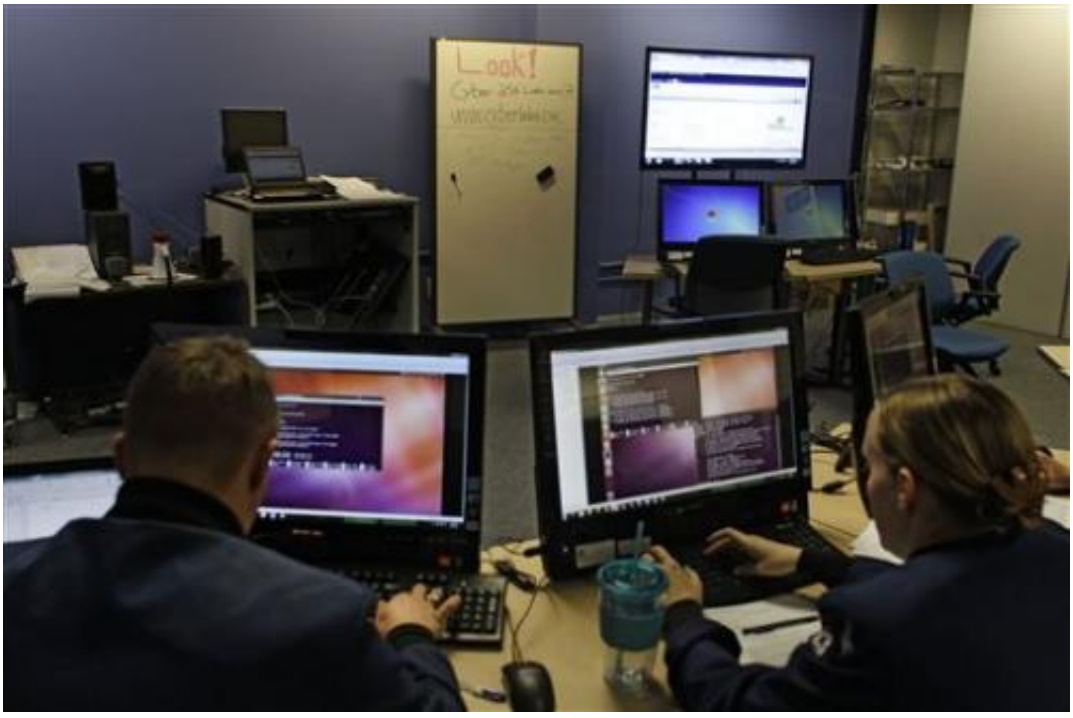
courses, and a computer security group meets weekly. One of the biggest cybersecurity challenges is keeping up with the head-spinning pace of change in the field.

"You know American history is pretty much the same" every year, said Lt. Col. David Raymond, who teaches a cybersecurity course. "In this domain, it's really tough to keep up with how this thing evolves."

In this Feb. 20, 2013 photo, Martin Carlisle, standing, a computer science professor at the Air Force Academy and director of the school's Center for Cyberspace Research, instructs cadets in cyber warfare, at the U.S. Air Force Academy, in Colorado Springs, Colo. The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system. (AP Photo/Brennan Linsley)

In his congressional report, Clapper noted that the chance of a major attack by Russia, China or another nation with advanced cyber skills is remote outside a military conflict—but that other nations or groups could launch less sophisticated cyberattacks in hopes of provoking the United States or in retaliation for U.S. actions or policies overseas. South Korea accused North Korea of mounting a cyberattack in March that shut down thousands of computers at banks and television broadcasters.

Gen. Keith Alexander, head of U.S. Cyber Command, told Congress in March the command is creating teams to carry out both offensive and defensive operations. A spokesman said the command is drawing cyber officers from the service academies, officer schools and Reserve Officer Training Corps programs.



In this Feb. 20, 2013 photo, cadets work at computers inside a classroom at the Center for Cyberspace Research, where cyber warfare is taught, at the U.S. Air Force Academy, in Colorado Springs, Colo. The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront

increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system. (AP Photo/Brennan Linsley)

Teams from the three academies compete in events such as last week's National Security Agency Cyber Defense Exercise, in which they try to keep simulated computer networks running as an NSA "aggressor team" attacks. Teams from the U.S. Coast Guard and Merchant Marine academies also took part, along with graduate students from the U.S. Naval Postgraduate School and Canada's Royal Military College.

Air Force won among undergraduate schools. The Royal Military College won among graduate schools.

That hands-on experience is invaluable, said 2nd Lt. Jordan Keefer, a 2012 Air Force Academy graduate now pursuing a master's degree in cyberoperations at the Air Force Institute of Technology.

"You can't just go out there and start hacking. That's against the law," he said. The competitions, he said, "gave me actual experience defending a network, attacking a network."

In this Feb. 20, 2013 photo, a cadet works at a computer inside a classroom at the Center for Cyberspace Research, where cyber warfare is taught, at the U.S. Air Force Academy, in Colorado Springs, Colo. The U.S. service academies are ramping up efforts to groom a new breed of cyberspace warriors to confront increasing threats to the nation's military and civilian computer networks that control everything from electrical power grids to the banking system. (AP Photo/Brennan Linsley)

Counterterrorism expert Richard Clarke, noting that really high-level computer skills are rare, suggested the military might have to re-examine some of its recruiting standards to attract the most adept cyberwarriors.

"Hackers are the 1 percent, the elite and the creators," said Clarke, who served as White House cybersecurity adviser during the Clinton administration. "I wouldn't worry a whole heck of a lot (about whether they) can they run fast or lift weights."

Cyber's appeal was enough to get Keefer to put aside his dream of becoming a fighter pilot, a job with undeniable swagger. "It's a challenge, and for people who like a challenge, it's the only place to be," Keefer said.