FEATURES

WEST POINT'S CYBER INSTITUTE

BY GLENN RIFKIN

COL. GREGORY CONTI HAS ONE OF THE TOUGHEST JOBS IN THE U.S. ARMY. AS THE DIRECTOR OF THE ARMY CYBER INSTITUTE AT THE U.S. MILITARY ACADEMY AT WEST POINT, CONTI HAS TO PREPARE THE NEXT GENERATION OF OFFICERS TO FIGHT A COMPLETELY NEW KIND OF WAR, A WAR WITHOUT BAYONETS, BULLETS OR BOMBS BUT ONE THAT COULD POTENTIALLY BRING A POWERFUL NATION TO ITS KNEES. A WEST POINT GRADUATE WHO FOUGHT IN THE PERSIAN GULF WAR AND EARNED A PH.D. FROM GEORGIA TECH, CONTI WAS CALLED "THE ULTIMATE CYBERWARRIOR" BY LT. GEN. RHETT HERNANDEZ, WHO WAS HEAD OF THE ARMY CYBER COMMAND WHEN HE APPOINTED CONTI TO HIS CURRENT POST. (HERNANDEZ IS NOW RETIRED.)

THOUGH it hasn't received the kind of press attention that the wars in Afghanistan and Iraq have generated, those at the front lines are clear that a global cyberwar is under way. Though absent an attack on the scale of Pearl Harbor, the cyberwar is being waged on a thousand fronts by aggressive and unconventional enemies.

In 2013, for example, Chinese cyberspies reportedly stole plans for a number of U.S. military weapons and vehicles, including the F-35 Joint Strike Fighter jet, often characterized as the most expensive weapons system in history. Gen. Keith Alexander, the head of the U.S. Cyber Command, said the U.S. military is unprepared for such cyberattacks. "What we're seeing in cyber is going to continue, and it's going to grow and it's going to get worse," Alexander said after the attacks. "The platform we have today is not defensible."

For Conti, being put in charge of the Army's cybereducation effort is a natural evolution. At 46, he has a strong technology background and has spent much of his Army career in signals intelligence, that branch of military intelligence focused on gathering strategic information from signal sources such as the Internet. In 2006, after completing his Ph.D., Conti returned to West Point, where he took over a small cyberwarfare research center. The Army, like other branches of the military, was trying to mount a cohesive effort to address cybersecurity in a time when threats from hackers were growing significantly. Under Conti, the tiny research center with five employees was recently renamed the Army Cyber Institute and is now morphing into a major initiative at West Point with a broad mission of outreach, advice, research and education. Conti said the center needs to be 10 to 25 times bigger to reach maximum effectiveness, and he expects the staff to increase to 75 educators, researchers, scholars and technical professionals within three years.

The Army's cyberwarfare efforts come at an inflection point in world events. The military is in a "draw down" era, with two major wars coming to a close and a mandate to cut military spending. At the same time, cultures are colliding in the Army. The current generation of leaders comes from a time when military strategy and leadership was built upon a deep understanding of conventional warfare and military engagement. Technical types don't have a stellar history of success in the armed forces, generally relegated to a support role without much hope of promotion to the highest levels of leadership.

"Our senior leaders get the importance of this," Conti said. "The news comes up every day, and it gets worse and worse. There is recognition up and down the force of the implications, but the system

is built to grow the best combat Army generals out there. In the Air Force, they create the best pilots; in the Navy, the best ship captains. That is the center of gravity for each of these organizations. So there is a cultural change going on, but things move slowly."

Writing in the *Small Wars Journal* in 2012, Conti, along with two co-authors, said, "There is a reason why we don't place Army officers in charge of aircraft carriers. That being said, you go to war with the Army you have, not the Army you wish you had. We need to fight to understand the domain of cyberspace and learn to effectively lead cyberwarriors."

Conti, who recalled using paper maps as recently as the first gulf war, has bridged the generations enough to have the patient understanding this difficult transition will require.

"We have an inborn ability to understand the laws of the physical world," the journal article stated. "In order to shoot an artillery round farther, just add more powder; to provide cover for protection against bullets, hide behind a rock. The laws of physics however are counterintuitive in cyberspace. In cyberspace, our understanding of the 'laws of physics' is turned on its head.

"Weapons can be reproduced instantly, 'bullets' travel at near the speed of light, destroyed targets can be brought back from the dead, and a seventeen-year-old can command an army. As human beings we are at a distinct disadvantage when thinking intuitively about cyberwarfare."

To that end, Conti wants to build an interdisciplinary approach to the institute at West Point. Rather than focus on technology or policy, he is intent on building "a bench of expertise across the disciplines." Scholars will be joined by cyberoperations analysts, historians of technology and military intelligence, psychologists who specialize in security, social engineers, technologists, experts on policy, law and ethics. "We knew that privacy and civil liberties were important pre-Edward Snowden," Conti said. "We want a democracy, too, a safer and more secure nation, but at the same time preserving our liberties as well."

Conti is also clear that education at West Point will remain ensconced in traditional warfare training and strategy. His job is to incorporate cyberspace capabilities. "There is very rich thought on how to conduct warfare," he said. "Some of these strategies can be applied to cyberoperations to varying degrees." For example, if one considers battlefield terrain—whoever controls that bridge wins the battle—there is an application of such strategy to cyberterrain.

As our world has become intractably dependent on digital systems, the threat of cyberwar has grown more alarming. But unlike conventional warfare, where the defender has a distinct advantage over the attacker, the cyberattacker has all the advantages. The complexity of computer systems offers those with evil intent the ability to identify a single flaw that can be penetrated to bring a system down or infiltrate highly classified data. A certain type of cyberweaponry may be used just once and then never again, leaving a defender helpless in devising a defense.

A CERTAIN TYPE OF CYBERWEAPONRY MAY BE USED JUST ONCE AND THEN NEVER AGAIN, LEAVING A DEFENDER HELPLESS IN DEVISING A DEFENSE.

Conti believes the goal is to grow highly qualified cyberleaders with a solid foundation across technology as well as policy, law, ethics and psychology. "We have to grow agile leaders who can think strategically," he said. "They have to be aware that the implications of their actions can have global consequences. They have to understand that we are building the airplane while flying it. And we have to inspire them to pursue a lifetime of self-education in this area. Because to stand still is to be left behind."

Despite the lure of the riches of Silicon Valley, technology savants are attracted to West Point, Conti said. They tend to be well-rounded, as are most cadets, and looking for a bigger challenge. Conti recalled the awe and admiration with which he held his commanding officer, Gen. Barry McCaffrey, during Operation Desert Storm.

"He knew everything. He was a highly refined person who had grown to the pinnacle of his powers, and he was absolutely the right person to lead that command," Conti said. "I want to do that here. I want to grow that same caliber person. Nothing against the current commanders, but I am trying to grow people better than us, better than me. We owe it to them."