Building Teams of Cyber Warriors

By LTC Joseph Doty
and
MAJ T.J. O'Connor

Developing an offensive cyber-warfare capability is one of our nation's goals right now and a key component of our national security strategy. At the heart of this challenge is recruiting and building cyber-warfare teams composed of highly talented and skilled individuals. We cannot simply assemble a group of all-stars and then watch as they "conquer the world."

Rather, we must focus on how to teach and develop these cyber warriors to work as part of a larger team and to begin playing in a team environment. For cyber-warfare teams to succeed (and our adversaries are formidable opponents), we need to examine closely what a cyber warrior looks like, and what we can do to further build successful cyber-warfare teams.

Why do teams of talented and skilled professionals fail where teams of amateurs succeed? The 2004 U.S. Olympic basketball team, composed entirely of professional players, lost three games and finished the tournament with a bronze medal. Four years later, the U.S. Olympic basketball team went undefeated and won the gold medal. The 2008 team's head coach, Mike Krzyzewski, was singularly focused on ensuring that these phenomenally talented professionals were playing as a team. (See *The Gold Standard: Building a World-Class Team* by Mike Krzyzewski and Jamie K. Spatola.) The 1980 U.S. Olympic hockey team, composed mainly of unknown college players, defeated the mighty Soviet Union team in what is widely considered to be one of the biggest upsets in the history of sports. At the very heart of this is the phenomenon that people who place a higher value on the success of the team (not the individual) succeed because of a shared purpose, vision and trust. *A team working together will achieve far more than the sum of the individual team members working alone.*

Is this true, however, with cyber security? Expertise in cyber warfare and security requires knowledge, skills, abilities and talent that necessitate years of study and practice of how different protocols and security mechanisms work. Even having a breadth of knowledge doesn't make an individual talented in cyber warfare.

It requires the ability to take that knowledge and turn it on its head. To be really successful in cyber warfare requires teams that can figure out how to bend and break the mold, to make protocols work in a method for which they were not originally intended, to find weaknesses in proven mechanisms for security—this is the art, instead of the science, of cyber warfare. The practical reality is that in order to be that introspective, a cyber warrior is more likely to be an individual than a member of a team. Yet we need teams to succeed in cyber warfare. A coordinated offensive strike against another nation or decentralized network requires thousands of hackers working

in multiple locations who communicate and build upon each other's strengths.

How is cyber warfare done well? There have been a number of successes in team-organized cyber warfare. In early July, a team attack targeted dozens of government web sites in the United States and South Korea. While suspected to have originated in North Korea, the attack required the ability to work with individuals in the United States, Guatemala, Japan and China. The team effort succeeded in crippling the web sites of 27 different services in the United States and South Korea. Shared communication, shared vision and a cooperative working environment contributed to the unfortunate (for U.S. and South Korean security) success of these attackers.

What does the cyber warrior look like? In 2004, Chinese hackers from the province of Guangdong attacked the U.S. Army Missile Command at Redstone Arsenal, Ala. In an operation called Titan Rain by U.S. authorities, a team of about 20 Chinese hackers grabbed specifications for helicopters and flight planning software. They gained and kept access to several machines at Sandia National Laboratories at Redstone, pillaging secret information from the U.S. government, and were eventually discovered and stopped by a single individual, Shawn Carpenter. An employee at the Department of Energy (DoE), Carpenter performed an unauthorized investigation into the hackers that led to their detection and Carpenter's subsequent dismissal from the DoE.

Carpenter's success in detecting the hackers highlights a challenge with cyber warriors: These talented people have highly specialized skills that the national security community does not necessarily fully understand or comprehend. Essentially, every cyber warrior has the ability to read his boss' e-mail—building teams of such people is a scary thought. We require them to be ethical and maintain professionalism in their craft, but this is often secondary to their ability to strike with technical precision.

In the case of Shawn Carpenter, the DoE missed the opportunity to put a talented professional with a clear professional agenda back into the field defending our nation's secrets. In contrast, the DoE punished Carpenter for violating procedural regulations—the equivalent of firing a bank teller who fought back against a bank robber. Talented cyber warriors often look and act differently from usual society. They are often referred to as nerds or geeks. We should embrace rather than fear the Shawn Carpenters in our organizations because they are vital to the security of our country.

Building cyber-warfare teams is something the U.S. Military Academy at West Point does extremely well. Every year, West Point fields a cyber-warfare team that competes against teams from every other service academy.

For four days in the spring, the National Security Agency's best hackers attack the U.S. Coast Guard Academy, the U.S. Air Force Academy, the U.S. Naval Academy, the U.S. Merchant Marine Academy and the U.S. Military Academy. For the past three years, the

U.S. Military Academy has won decisively. Why? The other schools have equivalent educational programs teaching their students technical expertise. West Point's team is so successful because individuals playing as a team win, while teams playing as individuals lose. West Point's team was led last year by senior Cadet Sal Messina. Halfway through the competition, his second-in-command made a mocking phone call to the NSA deputy director. Cadet Messina chastised the other cadet—not for the phone call, but for putting the team at risk. He told the cadet he did not have the right to sacrifice the work of the other members of the team. This was a clear example of the team's shared vision and effort.

It takes a great deal of resources—time and money—to recruit a talented, ethical cyber warrior, that unique individual who has incredible technical savvy, yet also has a high ethical code and a dedication to a profession. This often means they come from existing professional environments and may have little to no technical expertise.

Clifford Stoll, renowned for detecting the first series of cyber-warfare attacks in the 1980s, was simply an astrophysicist who became upset when he could not perform his research properly on compromised computer machines. Shawn Carpenter was a DoE employee dedicated to protecting his government's secrets. Does this mean that cyber warriors must be drawn exclusively from the professional ranks of our Department of Defense? No. They are most likely, however, to be individuals who have learned to work on teams. As we charge forward into the next cyber-warfare battlefield, we must not forget to tap the Sal Messinas that we have already grown and developed within our ranks. □

***LTC Joseph Doty**, Ph.D., is the deputy director of the Army's Center of Excellence for the Professional Military Ethic. He previously commanded 1st Battalion, 27th Field Artillery Regiment, V Corps Artillery. **MAJ T.J. O'Connor** teaches in the Department of Electrical Engineering and Computer Science at the U.S. Military Academy at West Point, N.Y. He previously served as a signal center director with the 7th Special Forces Group in Afghanistan.* (The views expressed here are those of the authors and do not purport to reflect the position of the U.S. Military Academy, the Department of the Army or the Department of Defense.)