Staff Sgt. Lauren Johnson, then an intelligence analyst NCO with the Cyber Mission Unit, 7th Signal Command (Theater), at Fort Gordon, Ga., watches for attacks on the Army's networks in the CMU's Cyber Operations Center last July. (Photo by Michael L. Lewis)

From Weapons Systems to Squad Leaders, Cyber NCOs Protect All That's Connected

By Michael L. Lewis

NCO Journal

In an age where everything is now networked — including weapons systems, squad leaders and desktop computers — the protection of that network and everything connected to it has become a life-or-death mission for the Army. As the Army establishes the organizational structure, educational institutions and doctrine for its cyber force, the way that force fights is changing with astonishing speed, and NCOs are integral to making sure the Army keeps up, said Command Sgt. Maj. Rodney Harris, the senior enlisted advisor of the Army's cyber force headquarters, U.S. Army Cyber Command.

"We have one of the Army's most dynamic missions," Harris said. "We operate in a unique, challenging domain that is changing daily with capable adversaries who are actively engaged in trying to do our Army and our nation harm. … We're actively engaged with an adversarial force across multiple nation-states. We have cyber criminals, 'hacktivists,' terrorist organizations all together affecting what we're doing in cyberspace, and they're actively targeting and actively working in and on our networks with the purpose of doing us harm."

And because just about everything in the Army today is connected — providing a level of communica-

The CMU's Cyber Operations Center at Fort Gordon is home to signal and military intelligence NCOs who watch for and respond to network attacks from adversaries as varied as nation-states, terrorists and "hacktivists." (The center was sanitized of classified information for this photo.) (Photo by Michael L. Lewis)

tion, command and control that was unthinkable a few decades ago — just about everything in the Army today is vulnerable, Harris said.

"In the last 10 years, we've gone from a network that allows us to all communicate on a level plane to, now, our weapons systems are all enabled by that network," he said. "I'm talking about the GMLRS (Guided Multiple Launch Rocket System), our unmanned aerial vehicles, our attack helicopters — I could go on and on and on. If you look at the Network Integration Exercise's Capability Set 14.2 that's being tested out at Fort Bliss (Texas) right now, every squad leader is connected to the Internet. So in our world — in the cyber domain — every connection between one individual or one device and the network is an avenue of approach where our cyber operators as well as our adversaries maneuver."

The cyber organization

To fight and win in this new domain, U.S. Cyber Command, or CYBERCOM, was established in 2009 to unify the U.S. military's cyber operations and network defenses. Army Cyber Command, or ARCYBER, was created in 2010 at Fort Belvoir, Va., to be the Army's component of CYBERCOM. But because CYBERCOM's commander is also the director of the National Security Agency, and ARCYBER's operational units are co-located with the NSA's highly secret facilities across the country, confusion abounds as to what ARCYBER's cyber operators actually do and don't do, Harris said.

"Because the commander of U.S. Cyber Command is also the director of the NSA, people think we do the same thing. Well that's not true," Harris said. "The reason why that commander has to be the same person is because the backbone, the communication infrastructure, that we work on is the same that the NSA works on. But we have two dynamically different missions. The NSA's job is to collect intelligence to support the active defense of the nation. Our job is, first and foremost, to defend all Army networks. Aside from that, we also support combatant commands and their efforts in cyberspace."

To that end, the Army operates 41 of CYBERCOM's 133 military cyber teams — 20 Cyber Protection Teams with defensive capabilities and 21 Cyber Combat Mission Teams and Cyber National Mission Teams with offensive capabilities. They are stationed at joint force headquarters that are co-located with NSA facilities throughout the country: the Navy-run facility is at NSA-Hawaii in Honolulu, the Air Force's is at NSA-Texas in San Antonio, the Marine Corps' is at NSA's headquarters at Fort Meade, Md., and the Army's will be with NSA-Georgia at Fort Gordon.

Fort Gordon will soon become the home of ARCYBER's headquarters and the newly formed Cyber Center of Excellence, a U.S. Army Training and Doctrine Command institution that will write doctrine regarding cyber warfare as well as consolidate the myriad Army, NSA and industry-standard courses that cyber operators must take to be technically and tactically proficient in their field. Someday, cyber will become its own branch, Harris said. But for now, cyber operators come from the Military Intelligence Corps, which focuses on offensive capabilities, and the Signal Corps, which focuses on defensive operations.

On the cyber front lines

A mix of signal and MI Soldiers is what now forms the Cyber Mission Unit at Fort Gordon, a brigade-level headquarters under the 7th Signal Command (Theater) that controls the Army's cyber teams across the country.

"You can't have one without the other," said Command Sgt. Maj. Patrick Brooks, the command sergeant major of the 7th SC(T). "Signal cannot do MI's job and MI cannot do signal's job. But if you combine a group of individuals who specialize in cyber — signal with the defense and MI with the offense — that's your cyber Soldier, that's your cyber warrior."

Those cyber operators are already engaging with adversaries on a daily basis, Brooks said.

"The CMU is such a unique unit, they're on the front lines without needing to deploy," he said. "The rifleman forward downrange is making a difference. But a cyber warrior is also making a difference behind that computer. Because that may be our next war; the next war may be cyber."

Though the exact work cyber operators do is classified, it's mostly NCOs who are doing it, Harris said.

"We say all the time how important the NCO Corps is, and we say all the time that we are the 'backbone of the Army.' But in Army Cyber, our NCOs *are* the technical experts," Harris said. "For the level of education and the level of skill that we need in a standard on-net operator, it takes about three years before we can let them work unsupervised one day."

Even then, however, the battlescape changes almost constantly, Harris said.

"Code changes daily," he said. "Our adversaries change their code and the way they employ malware daily. And the malware we're talking about is not the malware we traditionally think of — stealing our credit card numbers or somehow making our computer not work. The malware that our adversaries are employing against us are tools designed to monitor, retrieve and extract information, like the information we may have that pertains to operations or organizational structures. If we're not careful, the malware that's being employed by our adversaries can give any secrets that we have away."

Finding (and keeping) cyber operators

The Cyber Mission Unit has been recruiting cyber-minded NCOs for more than a year to join the Army's elite cyber teams. Some will attend the new 25D cyber network defender course, which had its first graduation in December, and reclass into that military occupational specialty. Others will remain in signal or MI MOSs, depending on their mission sets. But no matter the MOS, the personnel doing the majority of the work on cyber teams are NCOs, explained Master Sgt. Moises Robles, the CMU's recruiter.

"NCOs are key. They are the ones actually doing the mission," Robles said. "We have officers and civilians, but the officers are managing. The NCOs are the hands-on force that actually gets the mission accomplished."

And it's not just signal and MI NCOs who will excel in cyber units, he said.

"We've had NCOs go through the selection process who didn't necessarily have all the [information technology] experience that you would look for," Robles said. "But they had that aptitude and that motivation to learn. When we put them through the training, they performed extremely well. Those are the individuals who we're looking for."

"We're looking for attitude and aptitude; those are two of our big words," Brooks said. "We're looking for go-getters, self-starters and motivators. We don't want people to come here thinking that this is a 9-to-5 job. This is serious. This is for the Department of Defense, for the [combatant command] commanders and the nation. These are serious threats. It's not to be taken lightly."

For those NCOs who do rise to the challenge, complete the lengthy training process and become successful cyber operators, the challenge is to then keep them as NCOs, Harris said. Once trained, cyber NCOs' education and skills are on par with those of their non-military counterparts in the business world who make three times as much.

"Our challenge is to find those technical operators who have that cognitive capacity to learn the skills that we're giving them and, at the same time, have the institutional drive to want to be a professional noncommissioned officer," Harris said. "Those people are so unique and are so few, we're going to have to think how to manage them differently. Outside industry is after those same people, and they're not asking them to be professional noncommissioned officers; they're just asking them to be really technically savvy operators in order to defend their networks."

Brooks agreed.

"We don't want folks to come in thinking, 'Okay, I'll come in, get all this training and these certifications, and I'll go off and get my big job in the sky.' No, we want folks who are going to hang around and stay in the Army. And it's our mission, once we get these quality individuals we have, to keep them — keep them trained, keep them motivated." ■

NCO JOURNAL
https://www.armyupress.army.mil/Journals/NCO-Journal/
https://www.facebook.com/NCOJournal
https://twitter.com/NCOJournal

NCO Journal provides a forum and publishing opportunity for NCOs, by NCOs, for the open exchange of ideas and information in support of training, education and development.
https://www.armyupress.army.mil/Journals/NCO-Journal/