To: Company Commanders
From: Company-grade Cyber Leaders

Leading Teams of Army Cyber Warriors

Our mission is to fight and win our nation's wars across all operational domains: land, sea, air, space and now, cyberspace. Our adversaries' cyber warfare capabilities are growing rapidly; so are ours. In 2010, U.S. Army Cyber Command was established. The following year, the 780th Military Intelligence Brigade was stood up as the first Cyber Brigade Combat Team. This year, Cyber Electromagnetic became a provisional branch, and newly commissioned lieutenants were assigned for the first time directly to cyber assignments.

Cyber is commanders' business. We all must learn how to operate in this new domain, from the basics of defending our local networks to more advanced tasks like integrating cyber offensive operations into our kinetic operations to achieve improved effects. Cyber operations, however, are cloaked in secrecy and remain a mystery to many of us. To help demystify the fastest growing component of our force, several company-grade cyber officers made time to reflect and share some of their experiences and insights.

Capt. Rock Stevens, SC
Cdr., A/781st MI BN
and
Acting Team Leader, National Mission Team
Degree: Computer Science

I remember the first time I saw a computer. I wanted to understand everything about it, to master it, to make it work for me. That set me on this path of a lifelong adventure to learn as much as I can about information technology and our security field. I received my first technical certification—as a certified network administrator—when I was 15 years old. The movie *Office Space* convinced me that I didn't want to spend my life working in a cubicle for a meaningless cause, so I chose to attend West Point. Then, a few weeks into Cadet Basic Training, something happened that changed my life. As I stood in formation one evening, an upper-class cadet pointed to a group of children who were playing lightheartedly on the parade field in front of us and said, "You see that? That's why you're here. You're here to make them safe and to give them an opportunity to grow up in a safe America." I will never forget that moment! Ever since that day, I've been motivated to make a real difference in the world, to do something meaningful—to keep Americans safe.

At West Point, I majored in computer science and was active all four years in SIGSAC, the Special Interest Group for Security, Audit and Control. That group included a bunch of cadets who made use of every opportunity to learn about network operations. We brought in world-renowned security experts and developed close friendships with them. I was able to participate in the ShmooCon every year as a cadet and even as a lieutenant. We brought in companies to run network "capture the flag" contests. The faculty mentored me and permitted me to pursue my passions and take independent study courses on things like network-based forensics and digital forensics. The summer before my senior year, I had the incredible opportunity to intern with the NSA's Red Team. During my senior year, the West Point team won the NSA-sponsored Cyber Defense Exercise over all undergraduate and graduate teams.

> *If you wait for the other side to attack you in cyberspace, you may find that the opponent has, simultaneously with their attack, removed your logic bombs or disconnected the targets from the network paths you expected to use to access them.*
>
> —Richard A. Clarke and Robert K. Knake,
> *Cyber War: The Next Threat to National Security and What to Do About It*

Hoping to be assigned to the NSA after commissioning, I selected Fort Meade as my first post. The Army had other plans, though, and assigned me to a Combat Camera unit, which turned out to be a great experience. That assignment gave me the opportunity to train and operate with a variety of conventional and special operations units. I completed Air Assault, Ranger, SERE and Pathfinder training—defi-

Capt. Rock Stevens, left, competes in CyberCity, a cyber warfare competition at Fort Gordon, Ga.

nitely not *Office Space.* As I developed tactically, I also maintained my technical certifications and attended hacker boot camps and conferences on my own time.

When I was attending the Maneuver Captains Career Course, some faculty members at USMA and the commander of ARCYBER at the time, retired Lt. Gen. Rhett A. Hernandez, reached out to get me assigned to Army Cyber. I am now on my second company command and am dual-hatted as acting team leader on a National Mission Team, which is a major's billet. I am able to lead a great team of soldiers and civilians and be directly involved operationally. I absolutely love it here! Every single day is an opportunity to make a strategic impact on our national security. Every single day is an opportunity to make a lasting impact on a nascent career field and organization. There's a lot of "exploratory learning," yes, but the Army has a long, rich history, and a lot of the Army's concepts and principles bleed into cyber. The Army Joint Planning Process, JOPES, MDMP—all apply in cyber. We have 131As—Field Artillery targeting experts—in our units, because the same principles of targeting apply, regardless of whether the means of attack is firing a cannon or authoring code. So, while in one aspect cyber is brand new, in another aspect it involves the same things we've always been doing.

> *We know that foreign cyberactors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country. We know of specific instances where intruders have successfully gained access to these control systems. We also know they are seeking to create advanced tools to attack these systems and cause panic and destruction and even the loss of life.*
>
> —Then-Secretary of Defense
> Leon E. Panetta, October 2012

What should non-cyber leaders understand about cyber? An emerging field within our force is the use of expeditionary cyber warriors in support of tactical cyber operations, and that capability will be available to leaders at echelons below division. We are trying to integrate that capability into training at the JRTC and NTC to show what cyber brings to the fight. The 1st IO Command has the world-class cyber OPFOR that operates at the combat training centers; they are crushing training units' networks. Most corps and combatant commands have cyber planners on their staffs. Leverage them. We have to train as we fight.

Capt. Sally White, MI

Team Leader, National Support Team

Degree: International Relations

I am currently a National Support Team leader, so I provide support to cyber operations within the Cyber National Mission Force, which operates under CYBERCOM. We focus on "defend the nation" type problem sets; we aren't aligned with combatant commands. My team, currently platoon-sized and a mix of soldiers and civilians, is comprised of incredibly smart people who possess a wide variety of skill sets. As a

CYBERCOM is a sub-unified command under U.S. Strategic Command. CYBERCOM is composed of ARCYBER/Second Army, Fleet Cyber Command/10th Fleet (Navy), Air Forces Cyber/24th Air Force, Marine Forces Cyber Command, and Coast Guard Cyber Command. The services provide National Mission Teams and their support teams, which focus on the strategic defense of the nation; Combat Mission Teams, which assist combatant commands around the world; and Cyber Protection Teams, which defend DoD's networks. ARCYBER's major subordinate units are NETCOM/9th Signal Command and the 1st Information Operations Command. The 780th MI Brigade (Cyber) is an INSCOM unit that directly supports CYBERCOM. The officers who contributed to this article are assigned to the 780th MI Brigade at Fort George G. Meade, Maryland.

humanities/liberal arts kind of person [White was a finalist for a Rhodes Scholarship], I see my role—in addition to providing leadership to my team—as helping to shape the narrative of what we do to audiences both internal and external.

On ethics, we at CYBERCOM work very closely with the NSA, albeit operating under different authorities. The NSA has procedures in place that make ethical decisions nearly automatic. The amount and level of training that cyber soldiers have to go through before they can even touch equipment is incredibly extensive, consistently renewed and endlessly emphasized. The environment is very much based around adherence to legal and ethical norms. The soldiers themselves—the analysts and the operators—have their own battle drills for ethical conduct. For example, "If I encounter U.S.-person information in my search for foreign intelligence, I stop immediately and turn the information over to the proper authority." So, in that sense, there aren't many ethically ambiguous situations at our level.

Ethics gets ambiguous when you try to define cyber actions at the strategic level. There are three primary components to cyberspace operations: ISR, cyber defense and cyber offense. If we ever engage in offensive operations without first being attacked, our actions must be justified as a preemptive strike against imminent aggression because, to the Western mind, war is discreet and binary—we are either at war, or we are at peace. Politics is assumed to be continuous; war is not. Influenced by Clausewitz, we think of war as "politics by other means."

In cyberspace, I wonder about the influence of different cultural norms between Eastern and Western worldviews.

CompanyCommand Glossary

ARCYBER: Army Cyber Command
BDE: Brigade
BN: Battalion
CEM: Cyber Electromagnetic
CYBERCOM: U.S. Cyber Command
INSCOM: U.S. Intelligence and Security Command
IO: Information Operations
ISR: Intelligence, Surveillance and Reconnaissance
JOPES: Joint Operational Planning and Execution System
JRTC: Joint Readiness Training Center
MDMP: Military Decision Making Process
MI: Military Intelligence
NETCOM: U.S. Army Network Enterprise Technology Command
NSA: National Security Agency
NTC: National Training Center
OIC: Officer In Charge
OPFOR: Opposing Forces
S-2: Intelligence Officer
S-3: Operations Officer
S-6: Automation Officer
SERE: Survival, Evasion, Resistance and Escape
ShmooCon: A convention devoted to demonstrating technology exploitation, inventive software and hardware solutions, and open discussions of critical information security issues.
SIGINT: Signals Intelligence
TTPs: Tactics, Techniques and Procedures
USMA: U.S. Military Academy

Capt. Sally White notes, "The amount and level of training that cyber soldiers have to go through before they can even touch equipment is incredibly extensive, consistently renewed and endlessly emphasized."

The Eastern view is less binary: War is cyclic rather than linear, and conflict is the natural state of politics. Thus, politics is war by other means; economics is war by other means; theft of intellectual property is war by other means; etc. This interpretation of conflict, without a rigid distinction between war and peace, is more readily adaptable to the ambiguous medium of cyberspace. We have a ton of lawyers here to think these things through, and they really do a great job. Still, I wonder if our Western worldview doesn't put us at a disadvantage in cyberspace.

1st Lt. Jeff Mullen, MI

OIC, Analysis & Production, National Mission Team

Major: Asian Studies; Minor: Mandarin Chinese

The interesting thing for cyber soldiers is that we are engaging our adversaries every day. It's not like we're sitting back in garrison and training for war. We're in a fight every day; we take some breaks to train, and then we're back in the fight.

Like any Army officer, when I'm in garrison, I get up in the morning, have my cup of coffee and do PT. What's amazing about this work, though, is that within two hours of getting to the office, there's a good chance that my team has done something strategically significant and possibly even something that saved American lives. I joined the Army because I wanted to protect my fellow citizens, and I have an opportunity to do that every day. To an outsider, it may seem like hyperbole to say that our actions can have such a large effect, but if you take 10 minutes to read up on the "doomsday scenarios" that a cyber actor can create, you'll quickly realize the gravity of this threat. In other words, our job is to stop the "Cyber Pearl Harbor" that former Secretary of Defense Leon E. Panetta has often warned of. It's a heavy responsibility and a great honor to engage in this cutting-edge mission at the frontier of military capabilities.

What should all commanders know about cyberspace operations? A senior cyber commander responds: "Cyber is commanders' business. It is not something you delegate to the S-6 and say, 'Hey 6, take care of it. Just show me the chart of green, amber, red.' Fundamentally, your network is key terrain that you have to defend. The network is an intelligence platform, a communications/command-and-control platform and a warfighting platform. So, first and foremost, you have to be in the business of defending it. If you don't defend the network at your level—using things like administrative rights, passwords, training on phishing—then you can become a vector for attack not only against yourself but also against everything you're connected to. At your level, defend your network because you are part of an integrated defense! Then, begin adding effects-based planning. What effects do you want to achieve? Our lessons learned from Iraq and Afghanistan are applicable. If you think about your experiences with expeditionary SIGINT teams, SIGINT terminal-guidance teams and cryptologic-support teams, you'll have a pretty good model for what cyber can do for you. I worked with a lot of BN and BDE commanders who understood those teams' capabilities and employed them effectively. Planning your cyber operations will involve your S-2 (with a good SIGINT section); your S-6, because you are defending the network and using the network; and your S-3, who should be your lead cyber planner and should have someone dedicated to planning electronic warfare/cyber. Increasingly, we demand a level of precision from you—both in the effects you want to achieve and in the language you use to articulate those effects. Commanders cannot get away with saying, 'I want some of that cyber stuff.' Use the language that's prescribed in Joint Publication 3-12 *Joint Cyberspace Operations*. Your usage of the correct doctrinal terms will help us help you achieve your desired effects."

I'm not under personal threat in this job, but I'm still dealing with the weight of my responsibilities and actions. In this field, you can make a mistake that you'll be thinking about for the rest of your life. I've spent time in Afghanistan, and I know what that personal threat feels like. Nevertheless, the responsibility of protecting Americans from our adversaries weighs on me far more than any personal threat did when I was in theater. We partake in a highly technical cat-and-mouse mission in which the terrain we operate on and the targets we prosecute can change at a moment's notice—and they often do. This set of rules (or lack thereof) would be difficult to manage in a vacuum. When you factor in the nature of our threat and the potential costs of failure, it becomes very stressful.

Another unique aspect of our work is that we are very security-conscious. I cannot talk about work or even jot down notes that are on my mind when I'm not at work. After hours, most people can simply send an email or jot down their thoughts if they forget to do so at work. When I wake up in the middle of the night with an idea, I cannot write it down. If someone calls me and has a one-line question that requires a one-line answer, there is a chance that I will have to go all the way back to work to answer it. The advantage here is that I absolutely cannot work from home, a fact that my loved ones seem to appreciate. Of course, the occasional late-night call into the office does earn me some scorn!

On training, cyber soldiers are still soldiers. They need the level of training that any other operational-support soldier needs. They need to know how to work with the line units, how to shoot and how to maneuver. Though the majority of cyber soldiers will spend most of their time in garrison, a number will deploy to combat zones to provide cyber support. However, cyber soldiers are different from many soldiers in their need to acquire master's-level knowledge over cyber concepts and TTPs in order to be effective. As a matter of fact, training a cyber operator can take as long as it takes to train a Special Forces operator.

We progress from training on the theory to actually using

"The interesting thing for cyber soldiers," 1st Lt. Jeff Mullen says, "is that we are engaging our adversaries every day."

practice networks. The nice thing is: While you can't create a physical firing range anywhere you want on a military post when you want to conduct marksmanship training, we can create virtual cyber ranges very quickly. We can quickly create a "range" to look like a specific enemy target, and then we can alter that range to rehearse many different situations and courses of action just as quickly.

On ethics, we take Law of War classes that are geared to the work we're doing, and we always have access to attorneys. In some ways, it's not very different from traditional warfare in that our ultimate job is to create effects—degrade, disrupt or destroy. Like in traditional conflict, when we set out to create an effect, we need to comply with the laws of war. For example, we cannot create an effect against a hospital's computer network, but we can against a full military target. These are the things we look at in our planning cycle to ensure we are well on the ethical side of the argument. Questions do arise, but we're very conservative in our intelligence operations and our application of force.

We also organize operations so we don't have junior soldiers making decisions about whether a strategic effect might be a Law of War violation. Commissioned officers have oversight over all operations, and we are trained to recognize potential issues and to ask the right questions—from planning through every step of an operation. Is this an acceptable target? Will there be secondary effects we ought to consider? If I create an effect on this network, will it propagate to other, unintended networks? While you must consider the secondary and tertiary effects of your actions in traditional combat, the potential for vast undesired consequences is much higher in cyber. After all, when you shoot an artillery round into one grid square, there's no way for its identical effect to replicate three grid squares away. That kind of thing *can* happen in the cyber world of interconnected networks, and it often does! Network administrators create unexpected issues often when they are attempting to fix issues in their networks; imagine what can happen when your goal is to break things. This is why "competence" among the commissioned officers is so critically important. We are making decisions on targets—decisions that depend on deep technical knowledge and understanding—and those decisions can have ethical, and even lethal, implications.

* * *

Cyber today is analogous to air power in the interwar years—fast-developing, not well understood and poised to make a huge impact. It's our duty as professionals of arms to learn about cyber and how to integrate it into our combined-arms operations. *Cyber War: The Next Threat to National Security and What to Do About It*, by Richard A. Clarke and Robert K. Knake, is a great introduction to the topic. This year's May–June issue of *Military Review* includes several good articles on cyber. For more in-depth study, we recommend the Army Cyber Institute's resources.

These contributions are excerpts from interviews of 17 Army officers at Fort George G. Meade, Maryland, conducted by Lt. Col. Pete Kilner, Maj. Jon Silk and Tom Morel in June. The CompanyCommand team is very grateful for the support of the Army Cyber Institute and ARCYBER leaders Col. Jennifer G. Buckner, Lt. Col. John Giordano and Capt. Tyler Jost. Send feedback on this article to Kilner at CoCmd.Team@us.army.mil.

Company commanders: Share your own stories and learn from your peers' experiences in the CompanyCommand professional forum: http://CC.army.mil. Follow us on Twitter: @CoCmd.

Connecting in conversation…
…becoming more effective.
CC.army.mil
Art by Jody Harmon
Have you joined your forum?