NCO JOURNAL

Modern Leaders: Evolution of today's NCO Corps

By Sgt. 1st Class James Hays
U.S. Army Asymmetric Warfare Group, Fort Meade, Maryland

September 2017

Sgt. Jacob Butcher, a squad leader for Company A, 1st Battalion, 18th Infantry Regiment, 2nd Armored Brigade Combat Team, 1st Infantry Division, troubleshoots the DUKE version 3 system, Sept. 11 during the testing portion of the Counter Radio-Controlled IED Electronic Warfare Specialist Certification, or CREW, training course at the Tactical Support Center on Fort Riley, Kansas. Butcher was one or more than 50 "Dagger" brigade Soldiers to successfully pass the 40-hour, two-week course. (U.S. Army Photo by Staff Sgt. Tamika Dillard)

The nature of war has not changed. The use of, or the threat of, direct hostilities by a nation or state against another is a matter of political policy. The character of warfare, however, continually evolves with emerging technologies, doctrinal advancements, and in response to varying global threats and political situations. As the character of war evolves, so too must those characters who fight.

An NCO's Journey

In 2003 I crossed the border into Iraq for the first time. I was a young infantry fire team leader and while I had no doubt I could lead my team, I had no idea what to expect of combat. I was worried about the things I could touch: how many bullets were in each magazine, were my Soldiers drinking water, how long would my radio batteries last, and was my compass tied down? If I couldn't physically see it, it was of distant concern.

A few years later in 2006, I returned to Iraq as a young platoon sergeant. Again, I was concerned with what I could see and touch. Did we have enough explosives ready, were the machine guns mounted and functioning, was the medic adequately equipped to deal with trauma, did the trucks have gas and were they serviceable, and most importantly, would my platoon leader make good decisions? Issues like the overall scheme of maneuver for the battalion or the brigade's intent for this phase of the operation were good to know, but not things I was overly concerned with.

In 2009, 2011, and 2014 I saw my role as a platoon sergeant and company first sergeant begin to merge towards active participation in operational planning and coordination. Noncommissioned officers over the last decade have become more involved with what we used to consider "officer business." The basic role of an NCO hasn't changed from Soldier welfare

and mission accomplishment, but that second piece has grown in complexity and depth. Where NCOs once forced mission accomplishment through physical and mental toughness, we are now able to insure success through understanding the intent and actively shaping all facets of the mission through our tactical and technical experience.

I returned to Iraq in December 2016 as an operational advisor with the Asymmetric Warfare Group. This gave me a unique opportunity to view the current battlefield from an almost abstract view point. I was able to embed with several units at the battalion and company levels. (I moved to the sound of the guns, on my own initiative, and placed myself at the points of friction to understand why there was friction, and "applied the grease" directly to the wheel.) I was there for the initial assaults into both the west and east sides of Mosul, spending time with seven different maneuver companies and five battalion task forces in ten weeks' time. I received incoming fire with conventional and special operations forces, stood guard on a MK19 40mm grenade machine gun, filled sandbags, got bombed by Islamic State in Iraq and Syria drones, and was at the tip of the spear when building the requirement for offensive and defensive tactical cyber capabilities. As an observer not directly tied to daily requirements of leadership, I began to notice how technically capable today's maneuver formation *could* be.

The fight into Mosul was strange, especially when based on my previous experiences in Iraq and Afghanistan as part of unilateral and partnered operations. The fight into Mosul was about supporting the Iraqi Security Forces, enabling them to attack. This assistance and support came primarily from surface and aerial fires. They provided a link between our intelligence, surveillance, and reconnaissance and full motion video collection assets and the ISF commanders on the ground, and protection from threat systems, like small unmanned aircraft systems. This

support was delivered at multiple echelons, from Special Operations Forces and small company teams, to battalion task forces, brigade headquarters, and multinational corps-level commands.

Today's NCO

At every echelon of the Army there are NCOs partnered with officers. This was done by design to allow for cross talk, a second point of view, a fresh take, and, especially at the lower levels, mentorship from an experienced professional. This was also seen at every level of advisory support provided to the ISF; however, the NCOs are not as effective in this role as they could be. In many cases, NCOs fulfilled the "beans and bullets" stereotype and Soldier welfare, but they have not engaged in advisory support efforts. Why is it that, while they are the number one reason the U.S. Army is the premier fighting force, NCOs are not as involved in supporting the ISF? We succeed as a force *because* of the relationship between our NCOs and officers, not in spite of it. Peeling back the layers on this question identified a real training gap and lack of knowledge in our NCO Corps. Similar to the "beans and bullets" stigma, NCOs are sometimes recognized as the old timer who says, "Well, that's the way we've always done it," and more than a few senior NCOs would rather use a flip phone than an iPhone, myself included.

Noncommissioned officers are sometimes seen as dinosaurs when it comes to emerging technology, especially in the cyber domain. It sometimes seems like we (again, myself included) wish we could just close our eyes and go back to the days of compass-based land navigation and hand-and-arm signals. The Army's role in the cyber domain is here to stay and will only grow in scope and depth as we move forward. And it's time, faced with the risk of becoming marginalized, for the NCO Corps to get deep into this evolving cyber fight.

The Cyber Domain

NCOs are trained to understand the priorities of defense. One of our key responsibilities is force protection, and developing a defense is one of the NCO Corps strongest skills. When looking at the cyber domain, defensive strategy and engagement area development are only slightly tweaked. Using the seven-step engagement area development model found in **FM 3-21.8, Ch 8, Sec. IV**, and can enable a cyber-focused operation in a manner similar to a land-focused one.

1. Identify likely enemy avenues of approach. How is the enemy currently or likely to use the cyber domain? Where, geographically, are their systems and cyber infrastructure? What platforms do they use for communications, propaganda, recruiting, etc.? Do they have ISR or UAS capabilities?

2. Identify the likely enemy scheme of maneuver. How can the enemy use the cyber domain to influence friendly forces? Do they have jamming or denial systems? What is their objective and how can they get there?

3. Determine where to kill the enemy. How can we influence their use of the cyber domain? Can we jam their systems? Can we collect? In what way can we degrade their abilities? Where are the gaps in our "kill" abilities?

4. Plan and integrate obstacles. What can we use to mitigate the gaps from step 3? Where will our systems have the greatest effects? If we jam their use of the internet, will that increase their use of FM push-to-talk radios? Can we collect on FM transmissions? If we jam their UAS abilities, will we see more human spotter use? Can we "over-watch" their reactions?

5. Emplace weapon systems. What systems are organically available? Do we have trained operators for the systems?

6. Plan and integrate indirect fires. What systems can we request as multipliers? What is available through adjacent or higher units? What is the call-for-fire request process?

7. Conduct an engagement area rehearsal. Are all the available systems compatible? Will there be gaps in coverage or fratricide between systems? Are the operators identified and trained?

When looking at the cyber domain through the lens of a ground fighter and seeing the relationships and commonalities, it's evident the standard methods we employ relate. The cyber domain is absolutely an area the NCO Corps can work in and be able to provide experience,

insight, and both tactical and technical knowledge. We can work to advise our officer counterparts in a meaningful and beneficial way.

This fight does not fall solely on our shoulders. There are subject matter experts, electronic warfare NCOs and officers, joint service capabilities, and other avenues available and willing to join the fight. Experience will go a long way, but a big part of being successful with what you don't know, is knowing who does. Understanding the capabilities of sister services, other branches and specialties, and adjacent and higher headquarters will provide coverage to gaps identified in planning and self-reflection. As NCOs we can never settle for "the way things are" or "the way we've always done it." We must challenge those statements with new knowledge, revelations, innovation, and the desire to evolve, learn and succeed.

The Future NCO

Noncommissioned officers will continue to maintain responsibility for welfare and preparedness, training and discipline, but will be called on more and more as planners, leaders, and operators. Fast forward to the future battlefield. Where once battles were decided based on physical terrain, in the mud and dirt, the future will inevitably be fought, at least in part, in the cyber domain. The cyber domain overlaps land, sea, air, space, and the human presence. A future squad leader is equipped with organic vertical take-off and landing ISR platforms, capable of delivering precision air-to-ground fires. He is able to communicate over the horizon to anywhere in the world and is able to shape the cyber domain just as he is able to impact the land domain. In the future, a platoon is equipped with cyber-attack capabilities and the ability to selectively jam Wi-Fi, push-to-talk radios, cellular, and other systems in the electromagnetic spectrum. A company is able to fuse these assets to develop cyber engagement areas based on the available system effects. Future forces will deny an enemy the ability to use FM communications and

force an overreliance on cellular networks. By focusing collection assets on these networks, future leaders will steer an adversary into talking on a system they want them to use, and build actionable intelligence using that communication. Commanders will deny threat UAS flights in certain areas, shaping the airspace to channel threat UAS into developed engagement areas where counter-measures are more effective. Tactical level intelligence analysts will scrape social media platforms and understand the mediums that threat forces use for information operations, intelligence preparation of the battlefield, recruiting, and threat financing in their assigned areas. These actions will enable directed strikes against enemy capabilities. Public affairs and information operations officers will craft messages to directly impact audiences in order to counter threat narratives and propaganda in real time. NCOs will need to understand the full spectrum of electronic warfare systems' capabilities to provide timely and realistic advice to their commanders.

Conclusion

Many of these capabilities exist today, but they are under-utilized at the tactical level. Due in part to a lack of knowledge about available systems and their potential effects and impacts on the battlefield. As the Army continues to innovate and modernize the force, NCOs on the cutting edge of battle need to strive to remain balanced at delivering both lethal and non-lethal effects with new technology as it is introduced to the field. An electronic warfare system is just another indirect fire weapon, capable of reaching through the cyber domain to cause an effect or deny freedom of action. Fully understanding the way the cyber domain overlaps and interfaces with other more well understood domains is a challenge for every leader. NCOs lead from the front and by example. They must collectively get ahead of the curve to embrace and understand friendly and enemy cyber capabilities and limitations.

About the author:
Sgt. 1st Class James Hays is an infantryman with 19 years in the Army. He is currently assigned as an operational advisor with the U.S. Army Asymmetric Warfare Group at Fort Meade, Maryland. Previous assignments include rifle company 1st Sgt. and platoon sergeant with the 10th Mountain Division (Light Infantry) at Fort Drum, New York; field recruiter with the 6th Recruiting Brigade in Wasilla, Alaska; platoon sergeant and squad leader with the 4th Infantry Division (Mechanized) at Fort Carson, Colorado; squad leader and team leader with the Allied Mobile Force (Land) in Mannheim, Germany; and team leader, senior scout, and rifleman with the 172d Infantry Brigade (Separate) at Fort Wainwright, Alaska. His deployments include Operation Iraqi Freedom in 2003, 2005, and 2006, Operation Enduring Freedom in 2009, 2010 and 2013, and Operation Inherent Resolve in 2015 and 2016.